МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«НАЦІОНАЛЬНИЙ ГІРНИЧИЙ УНІВЕРСИТЕТ»

Т.В. Бабенко
Г.М. Гулак
С.О. Сушко
Л.Я. Фомичова

КРИПТОЛОГІЯ У ПРИКЛАДАХ, ТЕСТАХ І ЗАДАЧАХ

Навчальний посібник

Дніпропетровськ
НГУ
2013

УДК 21.973-018.2.я7
ББК 004.72.056.55:003.26
К35

Рекомендовано Міністерством освіти і науки України як навчальний посібник для студентів вищих навчальних закладів галузі знань «Інформаційна безпека» (лист №1/11-12176 від 30.07.13).

Рецензенти:

Є.А. Мачуський, д-р техн. наук, проф. (Національний технічний університет України «Київський політехнічний інститут»);

О.Г. Корченко, д-р техн. наук, проф. (Національний авіаційний університет);

В.О. Хорошко, д-р техн. наук, проф. (Державний університет інформаційно-комунікаційних технологій).

К35 **Криптологія** у прикладах, тестах і задачах: навч. посібник / Т.В. Бабенко, Г.М. Гулак, С.О. Сушко, Л.Я. Фомичова. – Д.: Національний гірничий університет, 2013. – 318 с.

ISBN 978-966-350-436-0

Викладено теоретичні і практичні тести, приклади та задачі з криптології. Докладні відповіді, розв'язання типових завдань та достатня кількість тестів для самостійної роботи дозволяють використовувати посібник для всіх видів занять.

Рекомендовано для студентів вищих навчальних закладів, які навчаються за галуззю знань «Інформаційна безпека» за відповідними програми бакалаврської та магістерської підготовки, а також фахівцям у сфері захисту інформації.

УДК 21.973-018.2.я7
ББК 004.72.056.55:003.26

ISBN 978-966-350-436-0

ЗМІСТ

Вступ…… 4

Розділ 1. КЛАСИЧНА КРИПТОГРАФІЯ

Задачі…….. 7
Тести…… 16

Розділ 2. ІНФОРМАЦІЙНО-ТЕОРЕТИЧНА СТІЙКІСТЬ ШИФРІВ

Задачі…….. 37
Тести…… 50

Розділ 3. БЛОКОВЕ ШИФРУВАННЯ

Задачі…….. 56
Тести…… 90

Розділ 4. ПОТОКОВЕ ШИФРУВАННЯ

Задачі…… 116
Тести…… 158

Розділ 5. КРИПТОГРАФІЯ З ВІДКРИТИМ КЛЮЧЕМ

Задачі……184
Тести……225

Розділ 6. ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС. КРИПТОГРАФІЧНІ ПРОТОКОЛИ

Задачі……258
Тести……279

Розділ 7. ПРАВДА ЧИ НЕПРАВДА?..... 310

СПИСОК ЛІТЕРАТУРИ…… 316

ВСТУП

«Теорії з’являються і зникають, а приклади й задачі залишаються», – ці слова приписують відомому математику XX століття, організатору математичної освіти І.М. Гельфанду.

Дійсно, задачі вчать не менше, ніж правила. На жаль, у розмаїтті друкованих видань з криптографії, монографій, вузівських підручників та посібників переважно панують два підходи до викладання предмета. Один з них, так би мовити, фундаментальний, характеризується вкрай «теоретичним» поданням матеріалу та потребує від читача глибокого знання абстрактної алгебри, теорії ймовірностей та математичної статистики, комбінаторного аналізу, алгебри бульових функцій, об’єднані загальним терміном «дискретна математика». Інший підхід орієнтований на широке коло фахівців нетехнічних спеціальностей та спрямований на досить популярне викладення методів криптографічних перетворень інформації та їх властивостей.

І те, і інше не повністю відповідає потребам студента, майбутнього фахівця у сфері захисту інформації, якому розуміння теорії потрібно для її практичного застосування у питаннях менеджменту інформаційної безпеки, побудови та експертизи комплексних систем захисту інформації тощо.

Запропонований посібник – одна з перших вузівських методичних розробок в Україні, в якій акцент робиться на формуванні у майбутнього фахівця навичок практичної оцінки якостей шифрів, умінні використовувати основні методи й способи розв’язання конкретних задач синтезу та аналізу криптографічних систем, що складають сьогодення криптографічного захисту інформації. Зокрема, це стосується забезпечення конфіденційності, цілісності та авторства інформації за допомогою класичних симетричних криптосистем та криптосистем з відкритим ключем.

Головна мета авторів посібника – сформувати навички дослідника, «навчити вчитися» студента на конкретних задачах криптології. При цьому, зважаючи на «неможливість охопити неосяжне» та складність предмета, ми не намагалися запропонувати єдину методику розв’язання задач або подати перелік методичних рекомендацій, придатних для розв’язання будь-якої вправи, а ставили перед собою завдання на прикладі значної кількості розв’язаних задач показати, як досліднику користуватися наявним «інструментарієм», який метод може допомогти у розв’язанні проблеми.

Зміст посібника відповідає вимогам чинних галузевих стандартів з криптології для студентів напрямів підготовки 6.170101 «Безпека інформаційних і комунікаційних систем», 6.170102 «Системи технічного захисту інформації», 6.170103 «Управління інформаційною безпекою».

У посібнику наведено 180 задач з повним їх розв'язанням та 630 тестів, які згруповані таким чином, щоб дати читачеві змогу опанувати на практиці різні підходи, важливі для глибокого розуміння тем. Вправи й завдання досить різняться за складністю – від простих розрахункових до самостійних доведень ключових положень або теорем. Тестові завдання структуровані за типами: це тести з альтернативним або множинним вибором правильної відповіді, тести на встановлення правильних відповідностей за тематичними блоками, які відтворюють змістовні лінії сучасного курсу криптології. Під час розробки тестів ми виходили з принципу, що тестування, крім контролюючої, має й навчальну функцію.

Як традиційно склалося при написанні подібних видань, текст не завжди супроводжується посиланням на літературні джерела, оскільки це часто ускладнює подання матеріалу. За походженням матеріал, що входить до складу збірника, достатньо різноманітний. Подані задачі, що виникли під час обробки журнальних статей, а також запозичені з інших підручників, є задачі, джерела котрих ми не встановили, і такі, що стали частиною «криптографічного фольклору». Основну частину завдань розроблено авторами під час підготовки до практичних та лабораторних занять, проведення екзаменів з криптології, а також у ході роботи над даним збірником. Якщо комусь з читачів відомо походження тієї чи іншої вправи або наше посилання не є точним, ми були б раді дізнатися про це детальніше, щоб у подальшому доповнити список літератури.

Автори з задоволенням об'єднали свої зусилля для роботи над книгою, ґрунтуючись на досвіді читання інформаційних курсів у ДВНЗ «Національний гірничий університет», Державному університеті інформаційно-комунікаційних технологій, Навчально-науковому інституті інформаційної безпеки Національної академії Служби безпеки України. Висока вимогливість студентської аудиторії стала постійним стимулом у пошуку простих і ясних способів викладання матеріалу. Тому сподіваємося, що цей посібник, створений під час живого спілкування із студентами, не буде надзвичайно складною й нудною.

Автори готові надалі працювати над підручником, вдосконалювати його якість. Ми заздалегідь вдячні читачам, які надішлють свої зауваження та побажання за електронною адресою sushkosvet@gmail.com.

ДВНЗ «Національний гірничий університет» надав нам особливі сприятливі умови та фінансову підтримку на всіх стадіях роботи, за що ми висловлюємо щиру подяку ректорові університету, академіку НАН України, професору Півняку Г.Г. Ми глибоко вдячні к.т.н., доценту Державного університету інформаційно-комунікаційних технологій Мухачову Владиславу Андрійовичу, який зробив ряд цінних коментарів, критичних зауважень і пропозицій щодо змісту окремих розділів посібника.

РОЗДІЛ 1. КЛАСИЧНА КРИПТОГРАФІЯ

Задача 1. При шифруванні слова МАЙДАН підстановкою з ключем

А Б В Г Ґ Д Е Є Ж З И І Ї Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ю Я

↓ ↓

У П Ь Х Ж К Г И Ш Я С Н Д Р Ц О Т Б Е Ю Й Ї Ґ Ф А Ч Щ І М З Є Л В

воно змінюється на слово ТУРКУБ. Якщо слово за допомогою цієї підстановки зашифрувати ще раз, то отримаємо слово ҐФЙЦФП, а після третього циклу шифрування – ЖАРЩАЮ. На якому циклі шифрування знову побачимо слово МАЙДАН, якщо кількість виконаних циклів шифрування не обмежити?

Р о з в’ я з а н н я. Кількість різних слів, що можна дістати із початкового слова МАЙДАН, збігається з найменшим номером циклу шифрування, на якому знову виникне початкове слово. Буква М повторюється в кожному циклі, номер якого є кратним 5, буква А – у кожному циклі з номером, що є кратним 3, а букви Й, Д, Н – у циклах з номерами, які є кратними 2; 12; 11 відповідно. Якщо підстановку розкласти в добуток незалежних циклів, то порядок підстановки дорівнюватиме найменшому спільному кратному довжин циклів. Тоді слово МАЙДАН вперше з’явиться в циклі під номером, який дорівнює найменшому спільному кратному НСК(2,3,5,12,11) = 660.

Задача 2. Використання ключового слова (лозунгу) для побудови таблиці шифрозамін у лозунговому шифрі, з одного боку, спрощує запам’ятовування ключа, а з іншого – знижує потужність ключового простору. Скільки різних підстановок можна побудувати за допомогою лозунгів довжиною від 4 до 10 букв (алфавіт український)? Скільки таких лозунгів існує? У скільки разів при цьому звужується потужність ключового простору порівняно з повним ключовим простором для шифру простої моноалфавітної підстановки? Вважаємо, що лозунг необов’язково має бути осмисленим, хоча неосмислені словосполучення важко запам’ятати.

Р о з в’ я з а н н я. Потужність українського алфавіту – 33 букви, а кількість усіх можливих n-буквених слів – 33^n. Тоді кількість слів-лозунгів довжиною від 4 до 10 букв дорівнює $\sum_{n=4}^{10} 33^n \approx 1{,}6 \cdot 10^{15}$.

Нехай, для прикладу, лозунг складається з 10 букв. Тоді решту 23 букви можна упорядкувати 23! способами, що приводить до утворення

$$N_1 = \frac{33!}{23!} = 33 \cdot 32 \cdot \ldots \cdot 24 = 335885501952000$$

різних підстановок. Очевидно, на основі більш коротких ключових слів або ключових слів, що стають коротшими після видалення повторюваних букв, можна побудувати лише підстановку, яка вже врахована у попередньому випадку. Оскільки загальна кількість підстановок для українського алфавіту $N_2 = 33!$, то, порівнюючи потужності ключових просторів, знаходимо

$$\frac{N_1}{N_2} = \frac{1}{23!} \approx 3{,}87 \cdot 10^{-23}.$$

Отже, заміни на основі лозунгових слів складають лише малу частину від кількості усіх замін.

Задача 3. Визначте відстань єдиності шифру за ключем для: а) простої моноалфавітної підстановки; б) m-грамного шифру заміни, вважаючи, що простори відкритих текстів і шифротекстів складаються з усіх можливих m-грам ($m \geq 1$). Алфавіт український. Надлишковість української мови складає 0,72.

Р о з в' я з а н н я. Відстань єдиності шифру за ключем – це мінімальна довжина шифрованого тексту, необхідного для однозначного встановлення істинного ключа шифру (без жодних обмежень на пошук). Ця відстань дорівнює найменшому цілому розв'язку L_0 нерівності

$$L \geq \frac{\log|K|}{D \cdot \log m},$$

Де m – кількість символів українського алфавіту; $|K|$ – потужність ключового простору шифру; D – надлишковість використаної мови.

а) Проста моноалфавітна підстановка: $|K| = m! = 33!$ Значення факторіала $m!$ можливо оцінити за допомогою формули Стірлінга:

$$m! \sim \sqrt{2\pi m}\left(\frac{m}{e}\right)^m.$$

У нашому випадку

$$\log_2 33! \sim \log_2 \sqrt{66 \cdot 3{,}14}\left(\frac{33}{e}\right)^{33} \approx \log_2(8{,}7 \cdot 10^{36}) \approx 122{,}7.$$

$$L \geq \frac{\log_2|K|}{D \cdot \log_2 m} = \frac{\log_2|33!|}{0{,}72 \cdot \log_2 33} = \frac{122{,}7}{0{,}72 \cdot 5{,}04} \approx 33{,}8,$$

тобто $L_0 = 34$ букви.

б) m-грамний шифр заміни: загальна кількість m-грам, утворених з букв українського алфавіту, дорівнює 33^m. Потужність простору ключів

$$|K| = (33^m)!\ ; \qquad L \geq \frac{\log_2 |K|}{D \cdot \log_2 33^m} = \frac{\log_2 |33^m!|}{0,72 \cdot \log_2 33^m}.$$

$$33^m! \sim \sqrt{2\pi \cdot 33^m}\left(\frac{33^m}{e}\right)^{33^m}\ ;\ \log_2 (33^m)! \sim \log_2 \sqrt{2\pi \cdot 33^m} + \log_2 \left(\frac{33^m}{e}\right)^{33^m} =$$

$$= \frac{\log_2 2\pi}{2} + \frac{m \log_2 33}{2} + 33^m (m \log_2 33 - \log_2 e) =$$

$$= 5,04m \cdot 33^m - 1,45 \cdot 33^m + 2,52m + 1,33.$$

$$\log_2 33^m = 5,04m$$

$$L \geq \frac{\log_2 |33^m!|}{0,72 \cdot \log_2 33^m} = \frac{= 5,04m \cdot 33^m - 1,45 \cdot 33^m + 2,52m + 1,33}{0,72 \cdot 5,04m}.$$

$$L_0 \approx \frac{1}{5} \cdot \left(7 - \frac{2}{m}\right) \cdot 33^m + \frac{2}{5} \cdot \left(\frac{1}{m} + \frac{7}{4}\right).$$

При великих значеннях m відстань єдиності $L_0 \approx \frac{7}{5} \cdot 33^m$.

Задача 4. Дешифруйте криптограму

В Д О Щ Т Ф Щ Я И Т Ф Г Я І И С ,

яка отримана в результаті застосування лінійного афінного шифру до тексту українською (розділові знаки і пропуски між словами вилучено), за умови, що біграмі ТФ у криптограмі відповідає біграма ЕР відкритого тексту. Запишіть рівняння зашифрування та розшифрування.

Р о з в’ я з а н н я. Рівняння зашифрування шукатимемо у вигляді $y \equiv kx + t \bmod 33$. Запишемо цифровий еквівалент криптограми

2 5 18 29 22 24 29 32 10 22 24 3 32 11 10 21

та букв у заданих біграмах Е = 6; Р = 20; Т = 22; Ф = 24. Тоді

$$\begin{cases} 22 \equiv 6k + t \bmod 33, \\ 24 \equiv 20k + t \bmod 33. \end{cases}$$

Віднявши порівняння почленно, приходимо до порівняння

$$2 \equiv 14k \bmod 33.$$

Оскільки НСД (2,33) = 1, то $7k \equiv 1 \bmod 33$, звідки $k \equiv 19 \bmod 33$. Тоді з першого порівняння $22 \equiv 6 \cdot 19 + t \bmod 33$ і $t \equiv 7 \bmod 33$. Отже рівняння зашифрування – це $y \equiv 19x + 7 \bmod 33$. Знайдемо рівняння розшифрування:

$$19x \equiv y - 7 \bmod 33 \Rightarrow x \equiv 19^{-1}(y-7) \bmod 33 \equiv 7(y-7) \bmod 33 \Rightarrow$$
$$x \equiv 7y + 17 \bmod 33.$$

Використавши отримане рівняння, розшифровуємо криптограму:

ЮПІТЕР, ТИ СЕРДИШСЯ.

Задача 5. Вважатимемо, що шифрування букви x відкритого тексту українською за допомогою деякого афінного шифру еквівалентне композиції двох шифрів: лінійного шифру $z = ax(\bmod n)$ з ключем a та шифру зсуву $y = z + b(\bmod n)$ з ключем b (n– потужність алфавіту). Опишіть, як за допомогою атаки «зустріч посередині» на основі відомої пари «відкритий текст – відповідний шифротекст» визначити можливі варіанти ключів афінного шифру? Чи буде ця атака менш складною за повний перебір ключів?

Р о з в' я з а н н я. $y = ax + b(\bmod n)$ – рівняння зашифрування афінного шифру, для українського алфавіту $n = 33$. Звідси $y - b \equiv ax(\bmod n) \equiv z$. Складемо списки:

1) $A = \{ax:\ 0 < a < 33;\ \text{НСД}(a,33) = 1\}$;
2) $B = \{y - b:\ 0 \le b < 33\}$.

Якщо списки достатньої довжини, то у цих двох списках має знайтися спільний елемент. Відповідні значення a та b такого елемента – можлива пара для ключа шифру.

Потужність множини ключів афінного шифру дорівнює $n \cdot \varphi(n) - 1$, де $\varphi(n)$ – значення функції Ейлера (виключено пару $a = 1,\ b = 0$, яка при шифруванні не змінить відкритого тексту). Для українського алфавіту $n \cdot \varphi(n) - 1 = 33 \cdot 20 - 1 = 659$. Отже, застосувавши повний перебір ключів, ми маємо обчислити 659 шифротекстів. Атака «зустріч посередині» потребує $\varphi(n) + n = 20 + 33 = 53$ шифрувань, тому така атака менш складна, ніж повний перебір ключів.

Задача 6. Нехай p – просте число. Секретний ключ афінного шифру – пара $a,\ b \in Z_p,\ a \ne 0$. Зашифрування відкритих повідомлень $M \in Z_p$ здійснюється як $C \equiv aM + b \bmod p$. Як, застосувавши метод диференціального криптоаналізу, розкрити шифр?

Р о з в’ я з а н н я. За методом диференціального криптоаналізу атака на шифр будується з використанням лінійної різниці між двома вихідними повідомленнями і двома зашифрованими повідомленнями. Нехай $C_1 \equiv aM_1 + b \bmod p$, $C_2 \equiv aM_2 + b \bmod p$. Тоді

$$C_1 - C_2 \equiv (aM_1 + b) - (aM_2 + b) \equiv a(M_1 - M_2) \bmod p.$$

Якщо зловмисник якось дізнається різницю $M_1 - M_2$, то

$$a \equiv (M_1 - M_2)^{-1}(C_1 - C_2) \bmod p.$$

Тепер простіше відновити другу частину b ключа – для цього потрібна принаймні одна пара «відкритий текст – відповідний шифротекст».

Задача 7. Уявіть, що Ви знайшли старий зашифрований текст, за припущенням, зашифрований з використанням шифру Віженера, а у відкритому повідомленні йшлося про різні стародавні шифри. Ви виявляєте, що рядок РВМФПГІЦЛЬМЩ присутній у шифротексті двічі: вперше він починається з позиції 10-го символу тексту, а вдруге – з позиції 241-го (відлік символів тексту з одиниці, алфавіт український). Ви припускаєте, що цей фрагмент шифротексту відповідатиме у відкритому тексті слову КРИПТОГРАФІЯ. Якщо це припущення правильне, то яким був ключ шифрування?

Р о з в’ я з а н н я. Оцінимо період гами на основі тесту Казіскі. Відстань між двома появами фрагменту 241 – 10 = 231 = 3 · 7 · 11 знаків. Тому можливі значення періоду – 3, 7 або 11. Якщо припущення правильне, то можна знайти відповідний зсув. Так, у позиції 10 зсув ключа на 2 символи дає $T - c = 20 - 2 = 18 =$ «О» і далі за аналогічними розрахунками в інших позиціях виникає ЕЛЕДЬОЖЕЛЕДЬ. При цьому період гами не може бути кратним ані 3, ані 11, бо в цих випадках словоподібні структури не з’являються при будь-якому зсуві. Отже, ключове слово ОЖЕЛЕДЬ має довжину 7 та починається з 15 позиції.

Задача 8. Деяка мова складається з трьох букв А, Б і В, імовірність появи яких у текстах цією мовою 0,7, 0,2 та 0,1 відповідно. Написане цією мовою повідомлення з 1000 букв було зашифровано за допомогою шифру Віженера. Якщо атакувати шифр з використанням індексу збігу у рядку, то на яку кількість збігів букв слід очікувати?

Р о з в’ я з а н н я. На відрізку тексту, довжина якого є кратною довжині ключа, імовірність збігу дорівнює

$$0,7^2 + 0,2^2 + 0,1^2 = 0,54,$$

тому у тексті довжиною 1000 букв слід очікувати приблизно на 540 збігів букв.

Задача 9. Алфавіт деякої мови складається з трьох букв А, Б, В, частота появи яких у відкритих текстах 0,7; 0,2 і 0,1. Результатом шифрування за допомогою криптосистеми Віженера є криптограма АБВБАББАВ (додавання за модулем 3). За умови, що довжина використаного ключа не перевищує 3, знайдіть найбільш імовірний ключ.

Р о з в’ я з а н н я. Спочатку визначимо імовірну довжину ключа.

- Довжина ключа 1.

А|Б|В|Б|А|Б|Б|Б|А|В. Букви А,Б і В зустрічається 3; 5 і 2 рази відповідно;

- Довжина ключа 2.

АБ
ВБ
АБ
ББ
АВ

Збіг букв	I	II
А	3	0
Б	1	4
В	1	1

Найбільш близькі значення до 0,7; 0,2 і 0,1.

- Довжина ключа 3.

АБВ
БАБ
ББА
В

Збіг букв	I	II	III
	1	1	1
Б	2	2	1
В	1	0	1

Отже, довжина ключа 2. При цьому значенні у першому стовпчику частоти 3;1;1, тобто буква А має найбільшу частоту і є першою буквою ключа (зсув 0). У другому стовпчику частоти 0;4;1, а відтак букву Б дістаємо із А зсувом на 1. Таким чином, АБ – ключ шифру. Для перевірки у дешифрованому тексті ААВАААБААБ обчислимо частоти букв: А – 0,7; Б – 0,2; В – 0,1.

Задача 10. Нехай зловмисник проводить атаку на основі вибраного відкритого тексту і може отримати криптограму будь-якого тексту, щоб установити ключ зашифрування. Укажіть найпростіші відкриті тексти, які він має вибрати для атаки на шифр а) зсуву; б) Віженера; в) проста моноалфавітна підстановка; г) перестановки?

Р о з в’ я з а н н я. а) Достатньо зашифрувати будь-яку букву алфавіту, щоб визначити значення зсуву.

б) Для зашифрування потрібно вибрати відкритий текст вигляду АААААААААААА…. Кількість повторень букви має бути не меншою за довжину можливого ключового слова.

в) Відновити ключ моноалфавітної підстановки дозволяє шифрування усього алфавіту АБВГҐД…ЬЮЯ.

г) Якщо ключем шифру є перестановка степеня n, де n менше, ніж кількість букв алфавіту, то знову достатньо подати для зашифрування АБВГҐД…ЬЮЯ. Щодо перестановок більшого степеня, то імовірно потрібно зашифрувати більшу кількість повідомлень.

Задача 11. За допомогою трьох класичних шифрів відкритий текст СВІТ ЛОВИВ МЕНЕ, АЛЕ НЕ ПІЙМАВ було зашифровано та отримано три шифротексти:

1) ЬРРЇЬНІШІЕСМЛОФЩЯДШЩТЕЛБ;
2) ХЕЛЦПТЕКЕРИСИҐПИСИУЛНРҐЕ;
3) ІОЛСТВИВЕАЕВНМЕЛПМЙНІЕВА.

Ваша мета – визначити, які шифри використано, та встановити ключі шифрування. Яку атаку Вам потрібно провести? Перед шифруванням у відомому висловлюванні Г. Сковороди вилучили кому та пропуски між словами.

Р о з в’ я з а н н я. Аналіз пари «відкритий текст – відповідний шифрований текст» виявляє:

1). У першому шифрі шифропозначення букв залежіть від їх положень у відкритому тексті. Так, буква Е переходить у букви С, Л, Щ або Д. Тому моноалфавітна підстановка не використовувалась. Не було задіяно й шифр перестановки, бо у шифрограмі є букви, відсутні у відкритому тексті. Перевіряємо, а чи не був це шифр Віженера. Якщо від букв шифротексту відняти букви відкритого тексту, то отримаємо

ЗОЗУЛЯЗОЗУЛЯЗОЗУЛЯЗОЗУЛЯ.

Отже, це був шифр Віженера із ключем ЗОЗУЛЯ.

2). У другій шифрограмі присутні букви, яких не було у відкритому тексті, але шифропозначення букв не дублюються. Все це свідчить на користь того, що найімовірніше це – проста моноалфавітна підстановка. Зібравши дані у таблицю, приходимо до таких замін:

А Б В Г Ґ Д Е Є Ж З И І Ї Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ю Я

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

Ґ Е И К Л Н П Р С Т У Х Ц

Як бачимо, це може бути шифр зсуву з ключем 4.

3) Третя криптограма отримана шифруванням за допомогою шифру перестановки, бо перші її вісім букв – результат перестановки перших восьми букв відкритого тексту. Тут і далі для 8-буквених блоків відкритого тексту застосована перестановка (3 6 5 1 4 2 8 7).

У всіх випадках проведена атака на основі пари «відкритий текст – шифрований текст».

Задача 12. Припустимо, що ймовірності поява n-грам деякої мови утворюють геометричну прогресію, алфавіт складається з N букв. Покажіть, що якщо шифрування відкритого тексту цією мовою відбувається за допомогою заміни n-грам, то шифр можна розкрити на основі частотного аналізу з поліноміальною складністю.

Р о з в' я з а н н я. Нехай $p-$ максимальна ймовірність появи у тексті однієї букви. Тоді за умовою

$$p + p^2 + ... + p^N = 1.$$

Сума цієї геометричної прогресії $p\dfrac{1-p^N}{1-p} = 1.$

Тому складність дешифрування найбільш імовірної букви є поліноміальною. Повторюємо аналогічні міркування для алфавіту з $(N-1)$ букви. Це означає, що за допомогою частотного аналізу шифр розкривається з поліноміальною складністю.

Задача 13. Для зашифрування використано шифр Хілла з матрицею 2-го порядку (алфавіт український) та отримано криптограму:

Н Р Д П Ф Б У П У Ш Г Ш Щ Ю Ф Ю

Визначте ключ зашифрування за умови, що першій біграмі НР криптограми відповідає біграма ПО відкритого тексту, а останній біграмі ФЮ – біграма ОТ. Дешифруйте текст.

Р о з в' я з а н н я. Ототожнюючи український алфавіт з кільцем лишків Z_{33}, запишемо цифровий еквівалент криптограми

17 20 5 19 24 1 23 19 28 12 3 28 29 31 24 31

та цифрові еквіваленти потрібних біграм:

НР = 17 20; ОТ = 18 22; ПО = 19 18; ФЮ = 24 31.

З рівняння зашифрування $Y = KX$ шифру Хілла дістаємо $K = Y \cdot X^{-1}$, де K – ключ зашифрування, X – матриця відкритого тексту, Y – матриця шифротексту, X^{-1} – обернена матриця до матриці X (у матрицях X та Y букви відповідних текстів записано у стовпці). Отже,

$$K = \begin{pmatrix} 17 & 24 \\ 20 & 31 \end{pmatrix} \begin{pmatrix} 19 & 18 \\ 18 & 22 \end{pmatrix}^{-1} \bmod 33.$$

$$\begin{vmatrix} 19 & 18 \\ 18 & 22 \end{vmatrix} \bmod 33 = 418 - 324 \equiv 28 \bmod 33.$$

НСД (28,33) = 1, тому обернена матриця існує.

$$28^{-1} \bmod 33 \equiv 13, \quad \begin{pmatrix} 19 & 18 \\ 18 & 22 \end{pmatrix}^{-1} \equiv 13 \begin{pmatrix} 22 & 15 \\ 15 & 19 \end{pmatrix} \bmod 33 \equiv \begin{pmatrix} 22 & 30 \\ 30 & 16 \end{pmatrix}.$$

$$K = \begin{pmatrix} 17 & 24 \\ 20 & 31 \end{pmatrix} \begin{pmatrix} 22 & 30 \\ 30 & 16 \end{pmatrix} \bmod 33 \equiv \begin{pmatrix} 1094 & 894 \\ 1370 & 1096 \end{pmatrix} \equiv \begin{pmatrix} 5 & 3 \\ 17 & 7 \end{pmatrix}.$$

Ключ дешифрування $K^{-1} \equiv \begin{pmatrix} 5 & 3 \\ 17 & 7 \end{pmatrix}^{-1} \bmod 33;$

$$|K| \equiv \begin{vmatrix} 5 & 3 \\ 17 & 7 \end{vmatrix} \bmod 33 \equiv 17; \; 17^{-1} \bmod 33 \equiv 2; \; K^{-1} \equiv \begin{pmatrix} 14 & 27 \\ 32 & 10 \end{pmatrix} \bmod 33.$$

$$X = K^{-1}Y = \begin{pmatrix} 14 & 27 \\ 32 & 10 \end{pmatrix} \begin{pmatrix} 17 & 5 & 24 & 23 & 28 & 3 & 29 & 24 \\ 20 & 19 & 1 & 19 & 12 & 28 & 31 & 31 \end{pmatrix} \bmod 33 \equiv$$

$$\equiv \begin{pmatrix} 19 & 22 & 0 & 10 & 23 & 6 & 22 & 18 \\ 18 & 20 & 19 & 2 & 26 & 13 & 17 & 22 \end{pmatrix} \bmod 33.$$

Відкритий текст 19 18 22 20 0 19 10 2 23 26 6 13 22 17 18 22.

Повернувшись до буквених позначень, дістаємо повідомлення ПОТРАПИВ У ЦЕЙТНОТ.

Задача 14. Визначте кількість ключів шифру Хілла для зашифрування m-грам $(m \geq 2)$ відкритого тексту за умови, що алфавіт використаної мови містить p букв, де p – просте число.

Р о з в’ я з а н н я. В якості ключа шифру Хілла можна вибирати лише квадратні матриці m-го порядку, що будуть оборотними у кільці Z_p, бо у цьому випадку можлива операція розшифрування. З лінійної алгебри відомо, що матриця є оборотною тоді і тільки тоді, коли її рядки лінійно незалежні. Далі розглядатимемо лише ненульові рядки. Очевидно, перший рядок може бути будь-яким і для його вибору існує $p^m - 1$ способів (віднімання відображає заборону ненульових рядків). Єдина вимога для вибору другого рядка – він не може утворюватися з першого вже обраного рядка множенням на константу. Цій вимозі задовольняє $p^m - p$ різних рядків. Як третій рядок також можна обрати будь-який, аби він не дорівнював лінійній комбінації перших двох. Таких рядків існує $p^m - p^2$. Загалом, k-им ненульовим рядком може бути лише такий, що не виражатиметься через лінійну комбінацію перших $k-1$ рядків. Варіантів вибору таких рядків $p^m - p^{k-1}$. Тоді загальна кількість оборотних матриць m-го порядку у кільці Z_p дорівнює добутку

$$\prod_{i=0}^{m-1}(p^m - p^i).$$

Задача 15. Припустимо, відкритому тексту АГРЕСІЯЛЯКАЄ (алфавіт український) відповідає шифротекст ЕИМФТЮУІЙВЗР, отриманий за допомогою шифру Хілла над кільцем Z_{33}, але розмір матриці-ключа невідомий (тобто невідома кількість букв у блоках, що шифрувалися). Визначте мінімально можливу розмірність m ключа зашифрування, який міг би давати такий шифротекст. Скільки різних матриць могли б претендувати на роль ключа?

Р о з в' я з а н н я.

АГРЕСІЯЛЯКАЄ $\to$ 0 3 20 6 21 11 32 15 32 14 0 7;
ЕИМФТЮУІЙВЗР $\to$ 6 10 16 24 22 31 23 11 13 2 9 20.

- $m=1$: неможливо, бо аналіз текстів вказує, що тоді А$\to$Е і А$\to$З;
- $m=2$: $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\cdot\begin{pmatrix} 0 \\ 3 \end{pmatrix}=\begin{pmatrix} 6 \\ 10 \end{pmatrix} \Rightarrow \begin{cases} 3b = 6 \bmod 33, \\ 3d = 10 \bmod 33 \end{cases}.$

Останнє порівняння не має розв'язків, оскільки число 10 не ділиться націло на НСД (33,3)=3;

- $m=3$: $\underbrace{\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}}_{K}\cdot\begin{pmatrix} 0 & 6 & 32 & 14 \\ 3 & 21 & 15 & 0 \\ 20 & 11 & 32 & 7 \end{pmatrix}=\begin{pmatrix} 6 & 24 & 23 & 2 \\ 10 & 22 & 11 & 9 \\ 16 & 31 & 13 & 20 \end{pmatrix}$, звідки

$$K=\begin{pmatrix} 1 & 11x+4 & 3 \\ 2 & 11y+1 & 2 \\ 0 & 11z+2 & 17 \end{pmatrix}, \text{ де } 11x+4, 11y+1, 11z+2 \in Z_{33}.$$

1). При $x, y, z = 3t$, де $t \in Z$, $11x = 11y = 11z = 33t \equiv 0 \bmod 33$;

2). При $x, y, z = 3t+1$, $11x = 11y = 11z = 33t + 11 \equiv 11 \bmod 33$;

3). При $x, y, z = 3t+2$, $11x = 11y = 11z = 33t + 22 \equiv 22 \bmod 33$.

Отже, усього існує 27 можливих матриць для ключа.

ТЕСТИ

1. У яких з наведених нижче випадків використовується криптографічний захист інформації?

   а) на грошовій купюрі національний банк наносить водяні знаки, що повторюють основний малюнок банкноти;

б) у програмі-архіваторі комбінації символів, які зустрічаються багато разів, подаються у вигляді певного запису, який має меншу довжину;
в) шпигун передає у «центр» повідомлення, у яких замінює кожну букву іншими заздалегідь узгодженими символами;
г) у комп'ютері кожен символ подається у двійковому коді ASCII, що доповнюється додатковим бітом таким чином, щоб загальна кількість бітів була непарною.

2. З преси відомо, що під час підготовки терористичного акту 9 вересня 2001 року члени радикальної ісламської організації аль-Каїда приховували передачу своєї секретної інформації всередині графічних комп'ютерних об'єктів. Як називається такий метод захисту інформації?

а) криптографія; б) криптоаналіз;
в) стеганографія; г) тунелювання;
д) інформаційне перенаправлення.

3. Що є метою криптоаналізу?

а) визначення рівня стійкості алгоритму шифрування або знаходження методу відновлення початкового тексту без знання секретного ключа;
б) розроблення методів синтезу функцій шифрування у криптографічних алгоритмах;
в) зменшення кількості функцій шифрування у криптографічному алгоритмі;
г) реалізація практичних способів обміну інформацією.

4. Цілісність інформації – це неможливість

а) її несанкціонованого перегляду;
б) її несанкціонованої зміни;
в) несанкціонованого доступу до неї;
г) відмови від авторства.

5. Забезпечення конфіденційності даних означає

а) їх захист від несанкціонованого перегляду;
б) їх захист від модифікації, зміни, видалення та повторної передачі;
в) встановлення справжності інформаційних об'єктів;
г) неможливість відмови від авторства.

6. Який метод гарантує, що передана інформація отримана від легального джерела і надійшла належному абонентові?

а) забезпечення конфіденційності;
б) збереження цілісності;

в) автентифікація;
г) гарантія доступності.

7. Які властивості інформації розуміють під терміном автентичність?

а) її цілісність ;
б) її конфіденційність;
в) неможливість відмови від авторства;
г) її доступність;
д) справжність авторства.

8. Поставте у відповідність послуги із захисту інформації, що записані у нумерованому списку, та задачі, розв'язувані системами захисту інформації із списку, позначеному буквами.

1) конфіденційність;	а) встановлення джерела інформації і її автора;
2) автентифікація;	
3) неможливість відмови;	б) шифрування інформації;
4) цілісність	в) розмежування доступу до ресурсів автоматизованої системи;
	г) електронний цифровий підпис.

9. В алгоритмі симетричного шифрування секретним має бути

а) алгоритм шифрування; б) ключ;
в) окремі частини алгоритму шифрування; г) криптограма.

10. Криптосистема називається симетричною, якщо при шифруванні

а) відкритий текст розбивається на блоки однакової довжини;
б) ключі зашифрування та розшифрування збігаються або легко обчислюються один з одного;
в) використовуються циклічно повторювальні операції (раунди);
г) перший та останній символи криптограми однакові.

11. Криптографія з симетричними ключами застосовує

а) секретний ключ тільки з боку отримувача криптограми;
б) відкритий ключ з боку отримувача криптограми;
в) секретний ключ тільки з боку відправника криптограми;
г) секретний ключ у відправника та у отримувача криптограми.

12. У симетричній криптографічній системі обов'язково

а) процес шифрування має вигляд $ab...yz$ (відкритий текст) $zy...ba$;
б) ключ шифрування у два рази коротший, ніж ключ розшифрування;
в) ключі зашифрування і розшифрування є секретними;
г) відкритий текст шифрується посимвольно.

13. У чому переваги симетричних криптосистем над асиметричними?

а) висока швидкість шифрування для однотипних реалізацій;
б) менша довжина ключа для забезпечення порівняної стійкості;
в) стійкість у разі компрометації одного з ключів;
г) простота реалізації для будь-яких операційних систем;
д) простота розподілу ключів у мережі, що зазнає постійних змін.

14. Які основні проблеми застосування симетричних криптоалгоритмів?

а) складність реалізації на ЕОМ;
б) за допомогою ЕОМ такі шифри легко розкриваються;
в) ускладненість доставки ключів шифру;
г) шифрування за їх допомогою потребує великих обчислювальних ресурсів.

15. Які з наведених властивостей симетричних шифрів не відповідають дійсності?

а) складність розподілу ключів;
б) масштабованість (легкість підключення до мережі додаткових користувачів та ресурсів);
в) неможливість забезпечити теоретичну стійкість;
г) повільніше виконання операцій зашифрування/дешифрування порівняно з асиметричними шифрами.

16. Якщо n – кількість абонентів у мережі, то за формулою $N = \frac{n(n-1)}{2}$ розраховується

а) мінімальна кількість різних ключів, що необхідні для забезпечення попарних шифрованих з'єднань у мережі у разі застосування симетричної криптосистеми;
б) середня кількість ключів, що необхідна кожному абоненту мережі для відправлення криптограм будь-якому іншому абоненту;
в) кількість ключів, необхідних для запобігання колізій;
г) загальна кількість секретних ключів, що необхідні для забезпечення асиметричного шифрування даних в мережі.

17. Які з наведених видів криптосистем є симетричними?

а) криптосистеми з відкритим ключем;
б) потокові шифри;
в) блокові шифри;
г) системи ЕЦП.

18. За принципом Керкгоффса криптографічна стійкість шифру повинна визначатися тільки

а) його складністю; б) часом шифрування;

в) довжиною ключа шифру; г) секретністю ключа.
д) секретністю алгоритму шифрування;

19. Археологи знайшли манускрипт, написаний невідомою мовою. Пізніше до них потрапила маленька табличка, яка містила пропозицію, записану тією самою мовою з перекладом на грецьку. Використавши табличку, вони прочитали манускрипт. Яку атаку здійснили археологи?

а) атаку за методом «людина всередині»;
б) атаку на основі відомої пари «відкритий – шифрований текст»;
в) атаку на основі вибраного відкритого тексту;
г) атаку на основі вибраної криптограми.

20. Студент читає книгу з криптографії. На сторінці 112 автор книги наводить шифрований текст, а на сторінці 113 повідомляє, який було використано шифр, і який відкритий текст відповідає криптограмі. Пізніше на сторінці 133 наведена інша криптограма. Студент миттєво дешифрував криптограму, оскільки ключ не змінився. Про який тип атаки йдеться?

а) атаку на основі криптограми;
б) атаку на основі відомого відкритого тексту;
в) атаку на основі вибраного відкритого тексту;
г) атаку на основі вибраної криптограми.

21. Щоб дістати ключ шифру, криптоаналітик таємно отримав доступ до чужого комп'ютера та, використавши шифр законного користувача, записав у вікно для вводу тексту слово СВІТЛО. На екрані з'явився шифротекст ПРЕШНА. Яку атаку здійснив криптоаналітик?

а) атаку на основі криптограми;
б) атаку на основі відомого відкритого тексту;
в) атаку на основі вибраного відкритого тексту;
г) атаку на основі вибраної криптограми.

22. Криптоаналітик перехопив електронний лист з невідомим для нього кодуванням. Перевіривши всі кодування (Windows Cyrillic, юнікод тощо), він прочитав відкритий текст. Це була атака

а) на основі шифрованого тексту;
б) на основі вибраного шифрованого тексту;
в) на основі вибраного відкритого тексту;
г) за допомогою грубої сили;
д) статистична.

23. Агент, який здійснював у компанії економічну розвідку, умовив її президента підписати діловий лист щодо продажу продукції словами ПРЕЗИДЕНТ КОМПАНІЇ ВОЛОШИН, зашифрувати його та надіслати

дочірньому підприємству. Перехопивши криптограму, він розкрив увесь текст і завдяки значному часу життя ключа отримав можливість читати пошту компанії. Це була атака

а) на основі шифрованого тексту;
б) на основі вибраного шифрованого тексту;
в) на основі відкритого тексту;
г) за допомогою грубої сили;
д) на основі вибраного відкритого тексту.

24. Криптоаналітик виявив, що багато шифрованих листів, які фірма-виробник надсилає замовникам, починаються зі слів «У відповідь на ваше прохання…». Це дало йому змогу, перехопивши шифрований текст, відновити ключ шифру та прочитати все повідомлення. Яку атаку здійснив криптоаналітик?

а) на основі шифрованого тексту;
б) статистичну;
в) на основі відкритого тексту;
г) за допомогою грубої сили;
д) на основі вибраного відкритого тексту.

25. Криптоаналітик, спостерігаючи за діяльністю торгівельного кооперативу, встановив, що більшість шифрованих ділових листів, надісланих партнерам, містили слова ТОРГІВЕЛЬНА МАРКА, ЛОГОТИП, ДИЗАЙН. Перехопивши шифрограму, він підрахував частоту вживання однакових слів та розкрив ключ. Це була атака

а) на основі шифрованого тексту;
б) статистична;
в) на основі відкритого тексту;
г) за допомогою грубої сили;
д) на основі вибраного відкритого тексту.

26. abStwdRd; pVtrKRLp; iryzhToz; URbhhbEH; JEXHZmJ; zTDXJrZ – попередні паролі доступу до серверу (усі букви латинського алфавіту). Яку кількість паролів слід перебрати за методом «грубої сили» (у найгіршому випадку), щоб отримати доступ до серверу за новим паролем?

а) 2^8; б) 52^8; в) 8^8; г) 8^{26}; д) 8^{52}; е) $8!$ є) $26!$

27. Атаки за часом базуються на можливості високоточного вимірювання часу

а) передачі шифрованого повідомлення;
б) дешифрування шифротексту;
в) виконання алгоритмом шифрування операції піднесення до степеня;

г) виконання алгоритмом шифрування логічних операцій.

28. Припустимо, зловмисник може виконувати 2^{20} розшифрувань за секунду, а розмір ключа шифру 40 бітів. Як довго триватиме атака за допомогою грубої сили?

а) близько 25 діб; б) близько 20 діб; в) близько 18 діб;
г) близько 12 діб; д) близько 3 діб; е) близько 2 діб.

29. Припустимо, зловмисник може виконувати 2^{20} розшифрувань за секунду, а розмір ключа шифру 80 бітів. Як довго триватиме атака за допомогою грубої сили?

а) $3{,}8 \cdot 10^{16}$ років ; б) $2{,}8 \cdot 10^{10}$ років; в) близько 25 років;
г) близько 2 років; д) близько 3 діб.

30. Припустимо, зловмисник може виконувати 2^{20} розшифрувань за секунду, а розмір ключа шифру 40 бітів. В якій ситуації припустимо використання шифру з такою довжиною ключа?

а) для зашифрування повідомлень електронних переказів, за умов що доставка цих повідомлень відбувається не більш однієї доби;
б) для зашифрування запитів у технічному комплексі системи протиповітряної оборони, який забезпечує автоматичну ідентифікацію своїх літаків, у випадку коли єдиний ключ використовується протягом місяця;
в) для зашифрування повідомлень електронної пошти за умов щоквартальної зміни ключу;
г) жоден з наведених сценаріїв не є припустимим.

31. Яке твердження *неправильне*?

а) криптографічний алгоритм, для якого не знайдено методу дешифрування, буде обов'язково більш стійким до криптоатак ніж той, для якого такий метод вже розроблено;
б) розробник шифру має оцінювати криптографічні властивості криптосистеми, припускаючи, що зловмиснику відомі зміст криптограм та усі елементи криптосистеми, окрім ключа шифру;
в) одна з вимог до сучасних криптоалгоритмів – це зміна принаймні 50 % бітів криптограми у разі зміни біта ключа шифрування;
г) алгоритм повного перебору ключів шифрування може бути розпаралелений.

32. Корпоративна мережа банку об'єднує 100 відділень. Скільки необхідно мати ключів для шифрування за допомогою симетричного криптоалгоритму, якщо всі відділення банку повинні мати можливість передавати конфіденційні повідомлення один одному?

а) 4950; б) 99; в) 50; г) 495.

33. Яку умовну назву мала шифрувальна машина японського дипломатичного відомства, що була успішно дешифрована американською спецслужбою на початку Другої світової війни?

а) «Енігма»; б) М-209;
в) шифр «Сцітала»; г) «Пурпурний код»;
д) шифр Ямамото.

34. Шифрувальна машина «Енігма», що використовувалася у нацистській Німеччині у часи Другої світової війни реалізовувала

а) потоковий шифр; б) блоковий шифр;
в) шифр перестановки; г) шифр моноалфавітної заміни;
д) асиметричний шифр.

35. Нехай M_i і C_i – символи відкритого та шифрованого текстів відповідно; $M_i \in Z_{10}$, $C_i \in Z_{10}$, де $Z_{10} = \{0,1,2,3,4,5,6,7,8,9\}$; $C_i = E_K(M_i)$ – рівняння шифрування. Котру з наведених функцій можна застосувати як функцію шифрування E_K?

а) $E_K(M) = M(\mathrm{mod}10)$; б) $E_K(M) = K(\mathrm{mod}10)$;
в) $E_K(M) = M + K(\mathrm{mod}10)$; г) $E_K(M) = M \cdot K(\mathrm{mod}10)$;
д) $E_K(M) = M^{K+1}(\mathrm{mod}10)$.

36. Яким буде результат шифрування слова КУТ шифром Цезаря з ключем 2?

а) ЛФУ; б) НФХ ; в) МХФ; г) ХМФ.

37. Яка потужність ключового простору у шифрі Цезаря, якщо для запису текстів використано алфавіт з n символів?

а) $\varphi(n)$, де φ – функція Ейлера; б) $n-1$; в) $n!$; г) 2^n, д) n.

38. За допомогою простої моноалфавітної підстановки зашифрували слова ГОРН, АРГО та НЕРО і отримали криптограми АБЦЛ, ГЦВЛ і ВЛЦА (відповідність між словами та криптограмами невідома). Словам РОГА і ГАНГРЕНА при такому шифруванні відповідають криптограми

а) ВЛАЦ, ВГЦБААВГ; б) ЦАЛВ, ГАБЦВАГВ;
в) ЦВГЛ, БАГЦВАГВ; г) ЦЛВГ, ВГАВЦБАГ.

39. Використавши ключову фразу БУТИ ЧИ НЕ БУТИ? ОСЬ В ЧОМУ ПИТАННЯ як лозунг, сформйте ключ простої моноалфавітної підстановки. У відповідь записати другий рядок підстановки.

а) БУТИЧНЕОСЬВМПАЯЖЗГҐДЄІРФЇЙКЛХЦЮШЩ;
б) БУТИЧНЕОСЬВМПАЯГҐДЄЖЗІЇЙКЛРФХЦШЩЮ;
в) АБВЕИМНОПСТУЧЬЯГҐДЄЖЗІЇЙКЛРФХЦШЩЮ;
г) ГҐДЄЖЗІЇЙКЛРФХЦШЩЮБУТИЧНЕОСЬВМПАЯ.

40. У чому полягає основна слабкість простої моноалфавітної підстановки?

а) невелика потужність простору ключів;
б) шифрований текст зберігає статистичні властивості відкритого тексту;
в) якщо два тексти зашифровані за допомогою одного ключа, то шифр розкривається автоматично шляхом додавання двох криптограм;
г) супротивник може легко знайти ключ, отримавши пару «відкритий текст – відповідний шифрований текст».

41. Яка потужність ключового простору шифру простої заміни, якщо використаний алфавіт нараховує n букв?

а) n^n; б) $n \cdot \varphi(n)$, де φ – функція Ейлера; в) $n!$; г) n.

42. При шифруванні текстів за допомогою простої заміни як шифропозначення для букв задіяно двоцифрові числа. Один з наведених шифрованих текстів відповідає повідомленню українською, а інший – англійською (пропуски між словами і розділові знаки виключено). Який з шифрованих текстів відповідає повідомленню українською?

Перший текст:

95 96 96 92 73 79 92 33 98 95 32 92 90 93 38 92 96 73 94 90 91
75 73 77 96 92 98 74 92 79 96 90 79 92 96 98 94 90 76 98 74 92
77 98 95 90 38 77 70 70 90 98 74 92 96 98 96 77 72 92 34 77 96
79 92 38 98 95 91 34 95 73 77 96 92 78 95 73 98 92 96 92 72 98
96 91 73 92 98 74 95 73 33 72 96 90 34 95 73 73 97 36 71 92 33
98 98 90 77 38 92 38 72 91 73 92 96 70 95 33 92 38 33 92 90 96
77 96 72 92 34 77 96 75 90 76 95 38 98 92 70 33 90 96 79.

Другий текст:

38 94 70 73 79 77 79 78 39 94 75 94 70 73 75 74 76 94 39 74 96
29 78 74 96 74 92 30 38 79 70 72 94 78 79 22 92 92 79 98 37 70
92 74 94 77 74 93 31 78 74 70 39 39 71 75 94 98 70 39 97 92 72
71 75 74 39 74 73 74 72 30 73 74 78 33 79 98 94 78 36 79 97 72
22 23 39 78 94 70 74 76 78 94 78 78 30 77 39 94 74 75 94 39 79
74 72 74 92 71 75 94 98 35 22 92 72 22 23 39 71 75 74 39 74 73
74 76 78 74 96 79 94 39 79 71 30 27 39 79 32.

а) перший; б) другий;

в) недостатньо інформації; г) питання некоректне.

43. Текст українською шифрують за допомогою шифру простої заміни (пропуски між словами і розділові знаки виключено). Шифропозначення букв – двоцифрові числа. Визначити, скільки існує можливих місць, на яких у відкритому тексті могло б бути записано слово СТАРИНА, якщо тексту відповідає криптограма:

92 97 36 72 97 92 70 73 97 90 97 72 38 39 74 76
97 34 79 78 97 70 76 74 72 74 73 74 76 70 70 97
76 74 96 74 37 39 75 97 70 39 74 79 39 37 71 74
98 35 94 90 98 97 94 96 74 98 74 76 97.

а) 5; б) 4; в) 3; г) 2; д) на жодному.

44. При шифруванні слова ШИФР підстановкою з ключем

А Б В Г Ґ Д Е Є Ж З И І Ї Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ю Я _
↓ ↓
Я М Д Ж Е Ь З Р Ф І К Л І Й Т Ї Г У Б А В Х И Ц О Ю Щ_ П Ц С Є Ш Ч

воно змінюється на слово ПКОВ. Якщо слово за допомогою цієї підстановки зашифрувати ще раз, то отримаємо слово АТБД, а після третього циклу шифрування – ЯИМЬ. На якому циклі шифрування знову побачимо слово ПКОВ, якщо кількість виконаних циклів шифрування не обмежити?

а) 16; б) 24; в) 64; г) 576; д) 2040.

45. Рівняння шифрування має вигляд $y_i = x_i + k(\mathrm{mod}\, m)$, де x_i, y_i – цифрові еквіваленти букв відкритого та шифрованого текстів відповідно, k – ключ зашифрування, m – потужність використаного алфавіту. У цьому разі відкритий текст відновлюється за допомогою рівняння $x_i = y_i + k'(\mathrm{mod}\, m)$, де ключ розшифрування k' пов'язаний з ключем k формулою

а) $k' = m - k$; б) $k' = k - 1$; в) $k' = k^{-1}(\mathrm{mod}\, m)$;
г) $k' = k + 1$; д) $k' = k + 1(\mathrm{mod}\, m)$.

46. Відкритий текст українською (алфавіт з 33 букв) спочатку шифрують за допомогою шифру зсуву з ключем $k_1 = 17$, а далі до отриманої криптограми знову застосовують той самий шифр, але з ключем $k_2 = 23$. Такі послідовні шифрувальні операції еквівалентні одноразовому застосуванню шифру зсуву з ключем

а) $k = 40$; б) $k = 23$; в) $k = 6$; г) $k = 7$.

47. Які умови накладаються на ключ шифрування k лінійного шифру з рівнянням шифрування $y_i = (kx_i) \bmod m$, де x_i, y_i – цифрові еквіваленти букв відкритого та закритого текстів відповідно, m – потужність використаного алфавіту?

а) НСД$(k,m) \neq 1$; б) НСК$(k,m) = km$;
в) $m \le k < 2m$, НСК$(k,m) > m$; г) $0 \le k < m$; НСД$(k,m) = 1$.

48. Потужність алфавіту відкритого тексту становить 36. Якщо текст шифрувати за допомогою афінного шифру, то в якості ключа k можна вибрати числа

а) 41; б) 20; в) 17; г) 15; д) жодне з наведених.

49. Якщо m – потужність алфавіту відкритого тексту, то ключ шифрування k і ключ розшифрування k' в афінному шифрі при НСД$(k,m) = 1$ зв'язані формулою

а) $k' = k^{-1} + 1 \bmod m$; б) $k' = -k \bmod m$;
в) $k' = -k^{-1} \bmod m$; г) $k' = k^{-1} \bmod m$.

50. Нерухомою буквою відносно афінного шифру з рівнянням шифрування $y = (kx + t) \bmod m$ називають таку букву x, для якої $x = (kx + t) \bmod m$. Скільки нерухомих букв існує для афінного шифру з ключем $k = 10, t = 15$?

а)1; б) 2; в) 3; г) 4; д) таких букв не існує.

51. Яка потужність ключового простору афінного шифру, якщо використаний алфавіт нараховує n букв?

а) n^n; б) $n \cdot \varphi(n) - 1$, де φ – функція Ейлера; в) $n!$; г) 2^n.

52. Знайти можливі ключі k і t афінного шифру, якщо за допомогою рівняння шифрування $y = kx + t (\bmod 33)$ біграма ОИ відкритого тексту перетворюються на біграму ТЧ у шифрованому тексті?

а) $\begin{cases} k = 20 \\ t = 25 \end{cases}$; б) $\begin{cases} k = 24 \\ t = 29 \end{cases}$; в) $\begin{cases} k = 10 \\ t = 17 \end{cases}$; г) $\begin{cases} k = 11 \\ t = 19 \end{cases}$.

53. Відкритий текст спочатку шифрують за допомогою афінного шифру $y = ax + b (\bmod n)$, а далі до отриманої криптограми застосовують

інший афінний шифр $y = kx + t(\mathrm{mod}\, n)$. Така композиція шифрів еквівалентна афінному шифру $y = px + q(\mathrm{mod}\, n)$, де

а) $p = bk;\ q = ak + t$;
б) $p = ak;\ q = tk + b$;
в) $p = tk;\ q = ab + t$;
г) $p = tk;\ q = at + b$;
д) $p = ak;\ q = bk + t$;
е) $p = ak;\ q = at + b$.

54. Що допомагає при шифруванні за допомогою омофонної підстановки приховати частоту появи символів алфавіту відкритого тексту?

а) те, що для шифропозначень букв алфавіту вибирають числа;
б) те, що для заміни букв відкритого тексту використовують не одну, а кілька алфавітів;
в) те, що для букв з великою частотою вживання в даній мові пропонується кілька різних шифропозначень, а для рідко вживаних букв – одне шифропозначення;
г) те, що для букв з низькою частотою вживання в даній мові, пропонується декілька різних шифропозначень, а для часто вживаних букв – одне шифропозначення.

55. У часи Другої світової війни для шифрування даних широко використовувся шифр

а) шифр Сцітала;
б) DES;
в) схема Фейстеля;
г) одноразовий блокнот.

56. Коли у шифрі перестановки ключем зашифрування є (7 3 2 1 4 5 6), то ключем розшифрування буде

а) (7 3 2 1 4 5 6);
б) (6 5 4 1 2 3 7);
в) (3 4 7 1 6 5 2);
г) (4 3 2 5 6 7 1).

57. Якщо фразу ОДНА ЛАСТІВКА ВЕСНИ НЕ РОБИТЬ зашифрувати за допомогою шифру перестановки з ключем (3 1 4 5 2), то отримаємо

а) НОАЛД ТАІВС ВКЕСА ННЕРИ ИОТЬБ;
б) ТАІВС НОАЛД ВКЕСА ННЕРИ ИОТЬБ;
в) ВКЕСА НОАЛД ННЕРИ ИОТЬБ ТАІВС;
г) ННЕРИ ИОТЬБ НОАЛД ТАІВС ВКЕСА.

58. Що допомагає при шифруванні за допомогою поліалфавітних шифрів приховати частоту появи символів абетки, якою записано відкритий текст?

а) те, що на початку шифрування потрібно перевести відкритий текст у цифрову форму, а це змінює частоту появи букв абетки;

б) те, що у процесі шифрування абетка шифротексту змінюється залежно від номера букви у відкритому тексті;
в) те, що для букв, що мають велику частоту вживання в даній мові, пропонується декілька різних шифропозначень, а для рідко вживаних букв – одне шифропозначення;
г) те, що для букв, що мають низьку частоту вживання в даній мові, пропонується декілька різних шифропозначень, а для часто вживаних букв – одне шифропозначення.

59. Застосування тесту Казіскі до криптограми, отриманої за допомогою шифру Віженера, дозволяє

а) знайти довжину ключа;
б) провести частотний аналіз;
в) провести атаку за допомогою грубої сили;
г) відразу дістати відкритий текст.

60. Якщо слово ШПИГУН зашифрувати за допомогою шифру Віженера (алфавіт український з 33 букв без пропуску між словами) на ключі РОМБ, то отримаємо шифротекст

а) Л Ґ Ц Ґ И В; б) А П Р Н О А; в) В Ч С Ь Б З; г) Ф Р А Ф П Н.

61. Шифротекст ОТПБХ отримано зі слова МІДЯК за допомогою шифру Віженера (алфавіт український з 33 букв без пропуску між словами) з секретним ключем

а) МІНОР; б) НІС; в) ВІК; г) КРИК; д)ДІМ.

62. Скільки можливих ключів довжиною l існує для шифру Віженера, якщо використаний алфавіт нараховує n букв?

а) $(n-l)!$; б) $n!$; в) l^n; г) n^l.

63. За якої умови при шифруванні за допомогою шифру Віженера слова x з ключем y і слова y з ключем x в обох випадках виникають дві однакові криптограми?

а) до складу слова та ключа мають входити однакові букви, але порядок їх може бути різним;
б) довжина слова та ключа має бути однаковою;
в) слова обов’язково не можуть мати однакових букв;
г) однакові криптограми не можуть виникнути у жодному випадку, що забезпечує ін’єктивність функції шифрування.

64. При якому ключовому слові γ у шифрі Віженера результат шифрування тексту українською буде таким самим, як і під час застосування до тексту шифру Цезаря?

а) $\gamma =$Г; б) $\gamma =$АБВ; в) $\gamma =$ЬЮЯ; г) $\gamma =$Я.

65. Відкритий текст українською (алфавіт з 33 букв) спочатку шифрують за допомогою шифру Віженера з ключем γ_1 довжиною 8, а далі до отриманої криптограми знову застосовують той самий шифр, але з ключем γ_2 довжиною 4. Такі послідовні шифрувальні операції еквівалентні одноразовому застосуванню шифру Віженера з ключем мінімальної довжини

а) 32; б) 16; в) 12; г) 8; д) 6; е) 4.

66. Відкритий текст спочатку шифрують за допомогою шифру Віженера з ключем довжиною l_1, а далі до отриманої криптограми знову застосовують той самий шифр, але з іншим ключем довжиною l_2. Така композиція двох шифрів Віженера породжує еквівалентний шифр Віженера з деяким іншим ключем довжиною l_3. Укажіть випадки, коли для наведених значень l_1 і l_2 значення l_3 обчислене *правильно*.

а) $l_1 = 4,\ l_2 = 5,\ l_3 = 4$; б) $l_1 = 4,\ l_2 = 5,\ l_3 = 5$;

в) $l_1 = 4,\ l_2 = 5,\ l_3 = 20$; г) $l_1 = 12,\ l_2 = 4,\ l_3 = 4$;

д) $l_1 = 12,\ l_2 = 4,\ l_3 = 12$; е) $l_1 = 12,\ l_2 = 4, l_3 = 48$.

67. Що називають індексом збігу у текстовому рядку?

а) імовірність того, що дві навмання вибрані букви алфавіту стоятимуть поруч у даному рядку;
б) імовірність того, що навмання вибрана буква рядка збігається з навмання вибраною буковою алфавіту;
в) імовірність того, що дві навмання вибрані букви цього рядка збігаються;
г) різницю $(x_i - x_j)(\mathrm{mod}\, n)$, де x_i, x_j – номери двох букв, розташованих поруч у даному рядку, n – потужність алфавіту.

У тестах №68-70 f_i – частота появи у рядку $x = (x_1, x_2, ..., x_m)$ букви під номером i у алфавіті; p_i – імовірність появи букви алфавіту в осмисленому тексті даною мовою, n – потужність використаного алфавіту.

68. За якою формулою обчислюється індекс збігу текстового рядка $x = (x_1, x_2, ..., x_m)$?

а) $I_c(x) = \dfrac{\sum_{i=0}^{m-1} f_i(f_i - 1)}{n(n-1)}$; б) $I_c(x) = \dfrac{\sum_{i=0}^{n-1} f_i(f_i - 1)}{m(m-1)}$;

в) $I_c(x) = \sum_{i=0}^{n-1} f_i(f_i - 1)$; г) $I_c(x) = \sum_{i=0}^{m-1} f_i(f_i - 1)$.

69. Для рядка довжиною m осмисленого тексту індекс збігу $I_c(x)$ дорівнює

а) $I_c(x) = \sum_{i=0}^{n-1} p_i^2$; б) $I_c(x) = \dfrac{1}{m}$;

в) $I_c(x) = \dfrac{\sum_{i=0}^{n-1} f_i(f_i - 1)}{m(m-1)}$; г) $I_c(x) = \dfrac{\sum_{i=0}^{m-1} f_i(f_i - 1)}{n(n-1)}$.

70. Для рядка довжиною m неосмисленого тексту індекс збігу $I_c(x)$ дорівнює

а) $I_c(x) = \sum_{i=0}^{n-1} p_i^2$; б) $I_c(x) = \dfrac{1}{m}$;

в) $I_c(x) = \dfrac{\sum_{i=0}^{n-1} f_i(f_i - 1)}{m(m-1)}$; г) $I_c(x) = \dfrac{\sum_{i=0}^{m-1} f_i(f_i - 1)}{n(n-1)}$.

71. Що називають взаємним індексом збігу двох текстових рядків?

а) імовірність того, що дві навмання вибрані букви стоятимуть у рядках на одних й тих самих позиціях;
б) імовірність того, що навмання вибрана буква першого рядка збігається з навмання вибраною буковою другого рядка;
в) імовірність того, що дві сусідні букви з першого рядка стоятимуть у другому рядку у зворотному порядку;
г) різницю $(x_i - x_j) \pmod n$, де x_i, x_j – номери двох букв, розташованих у позиціях з номерами i та j у першому та другому рядках відповідно.

72. $f_0, f_1, ..., f_{n-1}$ і $f'_0, f'_1, ..., f'_{n-1}$ – відповідно частоти появи букв у рядках $x = (x_1, x_2, ..., x_m)$ та $y = (y_1, y_2, ..., y_M)$ відкритого тексту. За якою формулою обчислюється взаємний індекс рядків?

а) $M I_c(x, y) = \frac{n}{f_i f'_i}$;

б) $M I_c(x, y) = \frac{mM}{f_i f'_i}$;

в) $M I_c(x, y) = \frac{\sum_{i=0}^{m-1} f_i \cdot f'_i}{n \cdot N}$;

г) $M I_c(x, y) = \frac{\sum_{i=0}^{n-1} f_i \cdot f'_i}{m \cdot M}$.

73. Джерело відкритих текстів породжує текст із використанням алфавіту *a*; *b*; *c*; *d*; *e*, імовірність появи букв якої p(*a*)=0,2; p(*b*)=0,1; p(*c*)=0,3; p(*d*)=0,3; p(*e*)=0,1. Обчислити індекс збігу для тексту, генерованого цим джерелом.

а) 1,0; б) 0,45; в) 0,24; г) 0, 48; д) 0,12; е) 0,54.

74. Три різних відкритих тексти складені з букв українського алфавіту та записані у три рядки, індекси збігу яких дорівнюють відповідно 0,0575; 0,0057; 0,0157. Який з рядків може бути осмисленим текстом?

а) перший; б) другий; в) третій;
г) усі три; д) жоден не є осмисленим текстом.

75. Щоб провести криптоаналіз шифру Віженера методом імовірних слів (потужність використаного алфавіту $n > 2$), необхідно

а) відняти від криптограми ймовірне слово за модулем n у всіх можливих позиціях;
б) додати до криптограми ймовірне слово за модулем n у всіх можливих позиціях;
в) обчислити взаємний індекс збігу у криптограмі та ймовірному слові;
г) обчислити індекс збігу для ймовірного слова.

76. Виберіть *неправильне* твердження.

а) шифр Віженера – поліалфавітний;
б) довжину ключа шифру Віженера можна знайти за допомогою тесту Казіскі;
в) при шифруванні за допомогою шифру Віженера частоти букв криптограми збігаються з середньостатистичними частотами появи букв у мові, якою написано відкритий текст;
г) індекс збігу для рядків осмисленого тексту завжди більший, ніж для рядків неосмисленого тексту.

77. При шифруванні за допомогою поліалфавітного шифру

а) букви відкритого тексту міняються місцями;
б) змінюються ключі залежно від номеру букви у відкритому тексті;
в) змінюються слова відповідно до кодової книги;
г) змінюється алфавіт шифротексту залежно від місця букви у відкритому тексті.

78. Скільки можливих ключів існує для шифру перестановки, якщо використаний алфавіт нараховує 15 букв, а текст містить 10 букв?

а) $10!$; б) $15!$; в) 10^{15}; г) 15^{10}; д) 2^{10}; е) 2^{15}.

79. У шифрі одноразового блокноту ключ вибирають

а) за номером першої букви відкритого тексту;
б) з урахуванням шифрування попереднього блоку відкритого тексту;
в) відповідно до ключового розкладу;
г) рівноймовірно та випадково.

80. ДШОХ – це шифротекст, отриманий за допомогою шифру Хілла при шифруванні слова КІНЬ з секретним ключем

а) $\begin{pmatrix} 3 & 2 \\ 1 & 9 \end{pmatrix}$; б) $\begin{pmatrix} 12 & 11 \\ 2 & 9 \end{pmatrix}$; в) $\begin{pmatrix} 9 & 1 \\ 2 & 3 \end{pmatrix}$; г) $\begin{pmatrix} 11 & 9 \\ 2 & 3 \end{pmatrix}$.

81. Якій криптоаналітичній атаці піддається шифр Хілла?

а) атака тільки на основі криптограми;
б) атака на основі відомого невибраного відкритого тексту;
в) атака на основі вибраного відкритого тексту;
г) атака на основі вибраної криптограми.

82. Відкритий текст українською (абетка з 33 букв) спочатку шифрують за допомогою шифру Хілла з ключем $K_1 = \begin{pmatrix} 4 & 8 \\ 3 & 1 \end{pmatrix}$, а далі до отриманої криптограми знову застосовують той самий шифр, але з ключем $K_2 = \begin{pmatrix} 15 & 1 \\ 10 & 2 \end{pmatrix}$. Такі послідовні шифрувальні операції еквівалентні одноразовому застосуванню шифру Хілла з ключем

а) $\begin{pmatrix} 9 & 4 \\ 1 & 2 \end{pmatrix}$; б) $\begin{pmatrix} 21 & 10 \\ 2 & 5 \end{pmatrix}$; в) $\begin{pmatrix} 8 & 20 \\ 22 & 5 \end{pmatrix}$; г) $\begin{pmatrix} 30 & 22 \\ 13 & 16 \end{pmatrix}$.

83. Який з нижченаведених шифрів має інформаційно-теоретичну стійкість?

а) RSA; б) шифр Віженера; в) DES;
г) одноразовий шифрувальний блокнот; д) шифр Хілла.

84. Які умови має задовольняти матриця K, щоб її можна було вибрати як ключ шифру Хілла для шифрування відкритого тексту, написаного з використанням алфавіт з n букв?

а) усі елементи матриці K мають бути взаємно простими з n;
б) визначник матриці K має бути взаємно простим з n;
в) має існувати обернена матриця K^{-1} у полі цілих чисел;
г) визначник матриці K має ділитися на n.

85. Яке твердження *неправильне*?

а) шифр Віженера відноситься до поліалфавітних шифрів;
б) якщо ключ шифру Хілла є квадратна матриця другого порядку, то одиницею шифрування буде біграма відкритого тексту;
в) шифр Хілла вразливий до методу повного перебору ключів;
г) афінні шифри відносяться до перестановочних.

86. Дехто, ігноруючи принципи Керкгоффса, приховує тип шифру, який використовує. Як, перехопивши шифрограму, з'ясувати, чи використовувався шифр перестановки або шифр простої заміни?

а) при застосуванні шифру перестановки частоти повторюваності букв у шифрограмах близькі до середньостатистичних частот букв мови, а при застосуванні шифру простої заміни, частоти букв у шифрограмах практично збігаються з середньостатистичними частотами букв відкритого тексту з точністю до їх перестановки.
б) шифрограми, отримані за допомогою шифрів перестановки, мають лінійну структуру, шифрограми, здобуті при шифруванні заміною, такої структури не мають;
в) провести атаку «зустріч посередині», до якою вразливими є тільки шифри простої заміни, а шифри перестановки – ні;
г) якщо змінити принаймні одну букву відкритого тексту, то у шифрограмі, отриманій за допомогою шифру перестановки, частоти букв значно збільшаться, а у шифрограмі, отриманій при шифруванні підстановкою, частоти майже не зміняться.

87. Яке твердження *неправильне*?

а) небезпечно шифрувати двічі за допомогою одного й того самого одноразового блокноту;

б) гама для шифрувального блокноту має бути згенерована випадково;
в) після шифрування одноразовий блокнот має бути знищеним;
г) блокнот, так саме, як і відкритий ключ у асиметричній криптографії, не потребує захисту від фізичного розкриття.

88. Поставте у відповідність поняття: пароль (I); вектор ініціалізації (II); сіль (III); ключ криптосистеми (IV) та їх визначення.
    а) випадкове число, що регулярно обновлюється, передається каналом керування та використовується для початку роботи алгоритму шифрування;
    б) рядок випадкових даних, що подається на вхід однобічної функції разом з паролем, причому обчислене значення функції зберігається для наступної автентифікації;
    в) змінний параметр, кожному значенню якого відповідає одне з можливих відображень, які можна здійснити за допомогою криптосистеми;
    г) послідовність символів, що задає ключ або надає доступ до криптографічних або обчислювальних засобів.

89. Розташуйте наступні чотири шифри за зростанням розсіювання інформації при шифруванні: шифр Цезаря (1), шифр Віженера (2), одноразовий шифрувальний блокнот (3), моноалфавітна підстановка (4).

    а) 1, 2, 4, 3; б) 2, 1, 4, 3; в) 3, 1, 2, 4; г) 4, 2, 3, 1.

Для розв'язання тестів № 90 – 92, за необхідністю, можна використати гістограму зустрічаємості букв стандартної української мови, наведену на рис. 1.1. Алфавіт український: 33 букви і пропуск між словами.

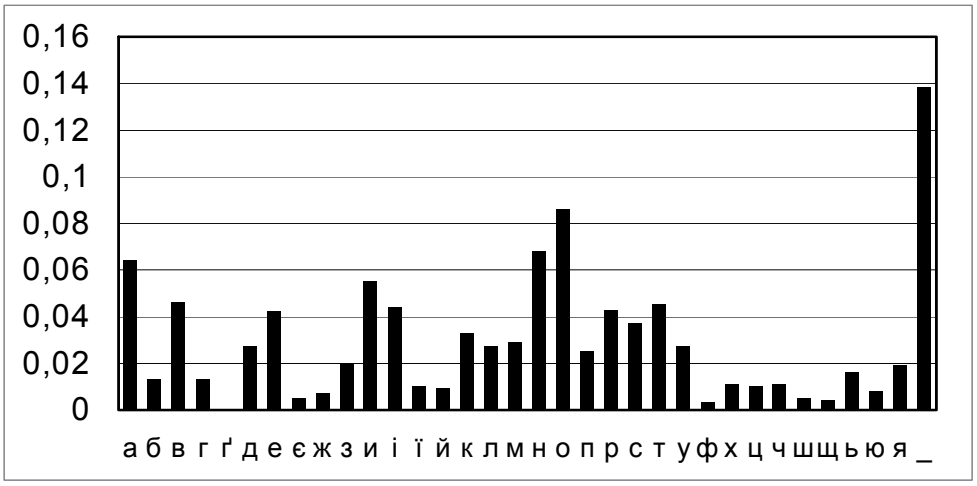


Рис. 1.1

90. Гістограма частот букв деякого зашифрованого тексту, подана на рис.1.2, ймовірно відповідає зашифруванню відкритого тексту, написаного українською, за допомогою

а) афінного шифру з ключами $a = 1,\ b = 2$;
б) шифру Віженера з довжиною гами $d = 2$;
в) одноразового блокноту;
г) шифру зсуву з ключем $k = 2$;
д) моноалфавітної заміни.

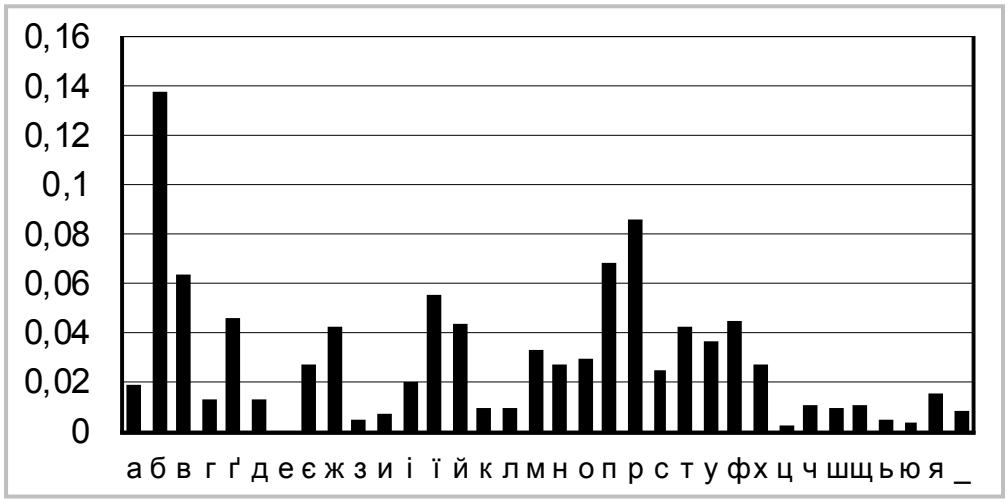


Рис. 1.2

91. Гістограма частот букв деякого зашифрованого тексту, подана на рис.1.3, ймовірно відповідає зашифруванню відкритого тексту, написаного українською, за допомогою

а) афінного шифру з ключами $a = 1,\ b = 0$;
б) шифру Віженера з довжиною гами $d = 1$;
в) шифру Плейфера з ключем
АБВГҐДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ;
г) шифру зсуву з ключем $k = 2$;
д) моноалфавітної заміни.

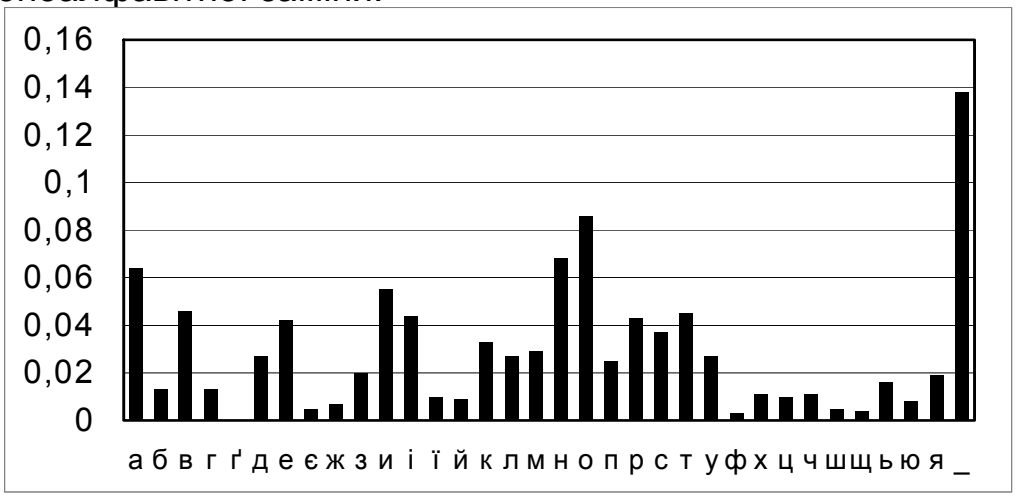


Рис. 1.3

92. Гістограма частот букв деякого зашифрованого тексту, подана на рис.1.4, ймовірно відповідає зашифруванню відкритого тексту, написаного українською, за допомогою

а) моноалфавітної заміни;
б) шифру Віженера з гамою, що складається з однієї букви Д;
в) шифру Вернама за модулем 34 з гамою, що є істинно випадковою послідовністю;
г) шифру зсуву з ключем $k = 5$;
д) афінного шифру з ключами $a = 1,\ b = 1$.

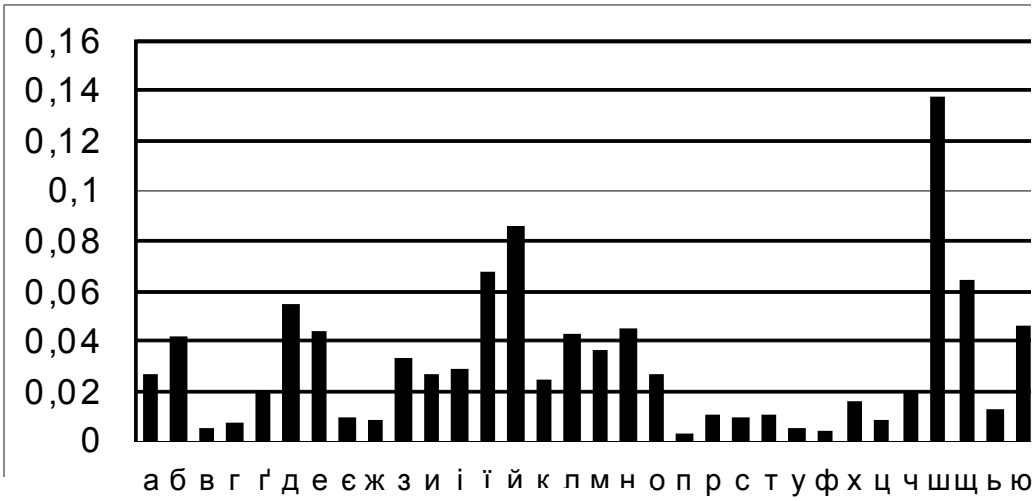


Рис. 1.4

РОЗДІЛ 2. ІНФОРМАЦІЙНО-ТЕОРЕТИЧНА СТІЙКІСТЬ ШИФРІВ

Задача 1. PIN-код – число $x_1x_2x_3x_4$, де чотири десяткові знаки $x_i\,(i=1,2,3,4)$ утворюються з бітових послідовностей $b_1,b_2,...,b_{16}$ за допомогою рівняння

$$x_i = b_{4i-3} + b_{4i-2}\cdot 2 + b_{4i-1}\cdot 2^2 + b_{4i}\cdot 2^3 \bmod 10.$$

Обчисліть ентропію PIN-коду за умови, що розподіл імовірностей бітів $b_1,b_2,...,b_{16}$ є рівномірним, а знаки x_1,x_2,x_3,x_4 незалежні у сукупності. Порівняйте отримане значення з максимально можливим значенням ентропії рядка з чотирьох десяткових випадкових знаків.

Р о з в' я з а н н я. Десяткові знаки для PIN-коду обчислюються незалежно один від одного, тому ентропія PIN-коду $H(PIN)=4H(x_i)$. Визначимо множину X, елементами якої будуть знаки x_i для PIN-коду:

$$X=\{0,1,2,3,4,5,6,7,8,9,\ \ 10\equiv 0\bmod 10,\ 11\equiv 1\bmod 10,\ 12\equiv 2\bmod 10,$$
$$13\equiv 3\bmod 10,\ 14\equiv 4\bmod 10,\ 15\equiv 5\bmod 10\}.$$

Отже,

$$P\{x_i=0\}=P\{x_i=1\}=P\{x_i=2\}=P\{x_i=3\}=P\{x_i=4\}=P\{x_i=5\}=\frac{2}{16};$$

$$P\{x_i=6\}=P\{x_i=7\}=P\{x_i=8\}=P\{x_i=9\}=\frac{1}{16}.$$

Тоді

$$H(PIN)=4H(x_i)=4\left(-6\cdot\frac{2}{16}\log_2\frac{2}{16}-4\cdot\frac{1}{16}\log_2\frac{1}{16}\right)=13\,\text{(бітів)}.$$

Максимальне можливе значення ентропії рядка з чотирьох десяткових випадкових знаків дорівнює $H_0=4\cdot\log_2 10\approx 13,29$ (бітів), що більше, ніж $H(PIN)$.

Задача 2. X_1,X_2,X_3 – три випадкові дискретні величини, яким притаманна така властивість:

$$P\{X_1=x_1\}=P\{X_2=x_2\}=P\{X_3=x_3\}=\frac{1}{4},$$

якщо триграма $x_1x_2x_3$ належить множині $\{(000),(011),(101),(110)\}$, інакше ці ймовірності дорівнюють нулю. Обчисліть ентропії $H(X_1)$, $H(X_3)$, $H(X_1X_2)$, $H(X_2|X_1)$, $H(X_1X_2X_3)$, $H(X_3|X_1X_2)$ та інформацію $I(X_1,X_3)$, $I(X_1X_2,X_3)$.

Р о з в' я з а н н я.

$$P\{X_1=0\}=P\{x_1x_2x_3=000\}+P\{x_1x_2x_3=011\}=\frac{1}{4}+\frac{1}{4}=\frac{1}{2};$$

$$P\{X_1=1\}=P\{x_1x_2x_3=101\}+P\{x_1x_2x_3=110\}=\frac{1}{4}+\frac{1}{4}=\frac{1}{2}.$$

Аналогічно отримаємо

$$P\{X_2=0\}=P\{X_2=1\}=P\{X_3=0\}=P\{X_3=1\}=\frac{1}{2};$$

$$P\{X_1X_2=00\}=P\{X_1X_2=01\}=P\{X_1X_2=10\}=P\{X_1X_2=11\}=\frac{1}{4};$$

$$P\{X_1X_3=00\}=P\{X_1X_3=01\}=P\{X_1X_3=10\}=P\{X_1X_3=11\}=\frac{1}{4};$$

$$P\{X_2X_3=00\}=P\{X_2X_3=01\}=P\{X_2X_3=10\}=P\{X_2X_3=11\}=\frac{1}{4}.$$

$$H(X_1)=-P\{X_1=0\}\log_2 P\{X_1=0\}-P\{X_1=1\}\log_2 P\{X_1=1\}=\frac{1}{2}+\frac{1}{2}=1\,(\text{біт});$$

$$H(X_3)=-P\{X_3=0\}\log_2 P\{X_3=0\}-P\{X_3=1\}\log_2 P\{X_3=1\}=\frac{1}{2}+\frac{1}{2}=1\,(\text{біт});$$

$$H(X_1X_2)=-P\{X_1X_2=00\}\log_2 P\{X_1X_2=00\}-$$

$$-P\{X_1X_2=01\}\log_2 P\{X_1X_2=01\}-P\{X_1X_2=10\}\log_2 P\{X_1X_2=10\}-$$

$$-P\{X_1X_2=11\}\log_2 P\{X_1X_2=11\}=-4\cdot\frac{1}{4}\log_2\frac{1}{4}=2\,(\text{біти});$$

$$H(X_2|X_1)=H(X_1X_2)-H(X_1)=2-1=1\,(\text{біт});$$

$H(X_3|X_1X_2)=0$, оскільки за відомими значеннями X_1 і X_2 однозначно встановлюється значення X_3;

$$H(X_1X_2X_3)=H(X_1X_2)+H(X_3|X_1X_2)=2+0=2\,(\text{біти});$$

$$H(X_1|X_3)=H(X_1X_3)-H(X_3)=2-1=1\,(\text{біт}),\ \text{бо}\ H(X_1X_3)=2\,(\text{біти});$$

$$I(X_1,X_3)=H(X_1)-H(X_1|X_3)=1-1=0\,(\text{біт});$$

$$I(X_1X_2,X_3)=H(X_3)-H(X_3|X_1X_2)=1-0=1\,(\text{біт}).$$

Знак відкритого тексту

Знак гами	А	Б	В	Г
А	Г	Б	В	А
Б	Б	Г	А	В
В	Г	Б	А	В
Г	Б	Г	А	В

Задача 3. Нехай в деякій шифросистемі алфавіт відкритих текстів, шифротекстів і знаки гами складаються з чотирьох букв А, Б, В, Г. Довжина повідомлень – 5 знаків. Для зашифрування знаки відкритого тексту додаються до знаків випадкової гами у відповідності з наведеною таблицею замін. Знаки гами розподілені рівноймовірно, відкриті тексти, що підлягають шифруванню, з'являються з імовірностями:

$$P\{\text{ВБГБВ}\}=\frac{1}{5};\quad P\{\text{ВАГБА}\}=\frac{3}{10};\quad P\{\text{ГАГБВ}\}=\frac{1}{2},$$

при цьому ймовірність зашифрування будь-якого іншого тексту дорівнює нулю. Якщо Ви перехопили шифротекст ВГАГА, то які умовні ймовірності того, що це був відкритий текст ВБГБВ, ВАГБА, ГАГБВ?

Р о з в' я з а н н я. Нехай шифротекст $c=$ВГАГА виникає при зашифруванні відкритого тексту m. За умовою задачі потрібно обчислити для всіх можливих відкритих текстів M_0 умовну ймовірність

$$P\{m=M_0|c=\text{ВГАГА}\}.$$

Загальна кількість ключів – 4^5. За умови, що вибрано повідомлення M_0 обчислимо ймовірність створення шифротексту $c=\text{ВГАГА}$, яка дорівнює сумі ймовірностей усіх тих ключів, за допомогою яких текст M_0 переводиться у даний шифротекст:

$$P\{c=\text{ВГАГА}\,|\,m=\text{ ВББГББВ}\}=\frac{1\cdot 2\cdot 1\cdot 2\cdot 3}{4^5}=\frac{3}{256};$$

$$P\{c=\text{ВГАГА}\,|\,m=\text{ ВАГБА }\}=\frac{1\cdot 2\cdot 1\cdot 2\cdot 0}{4^5}=0;$$

$$P\{c=\text{ВГАГА}\,|\,m=\text{ ГАГББВ }\}=\frac{3\cdot 2\cdot 1\cdot 2\cdot 3}{4^5}=\frac{9}{256}.$$

Тоді

$$P\{c=\text{ВГАГА}\}=\sum_{M_0}P\{c=\text{ВГАГА}\,|\,m=M_0)\cdot P(m=M_0)=$$

$$=\frac{3}{256}\cdot\frac{1}{5}+0\cdot\frac{3}{10}+\frac{9}{256}\cdot\frac{1}{2}=\frac{51}{2560}.$$

За теоремою Байеса отримуємо

$$P\{m=M_0\,|\,c=\text{ВГАГА}\}=\frac{P\{c=\text{ВГАГА}\,|\,m=M_0\}\cdot P\{m=M_0\}}{P\{c=\text{ВГАГА}\}},$$

звідки

$$P\{m=\text{ВББГББВ}\,|\,c=\text{ВГАГА}\}=\frac{P\{c=\text{ВГАГА}\,|\,m=\text{ВББГББВ}\}\cdot P\{\text{ВББГББВ}\}}{P\{c=\text{ВГАГА}\}}=\frac{2}{17};$$

$$P\{m=\text{ВАГБА}\,|\,c=\text{ВГАГА}\}=\frac{P\{c=\text{ВГАГА}\,|\,m=\text{ВАГБА}\}\cdot P\{\text{ВАГБА}\}}{P\{c=\text{ВГАГА}\}}=0;$$

$$P\{m=\text{ГАГББВ}\,|\,c=\text{ВГАГА}\}=\frac{P\{c=\text{ВГАГА}\,|\,m=\text{ГАГББВ}\}\cdot P\{\text{ГАГББВ}\}}{P\{c=\text{ВГАГА}\}}=\frac{15}{17}.$$

Задача 4. Чи буде досконало стійкою симетрична схема шифрування, в якій множина відкритих текстів, ключів і шифротекстів – кільце лишків Z_6, а рівняння зашифрування:

а) $E_K(M)=C=M+K \bmod 6$;

б) $E_K(M)=C=M+2K \bmod 6$?

Р о з в’ я з а н н я. Задамо функції шифрування відповідними матрицями:

а) $C = M + K \bmod 6$ б) $C = M + 2K \bmod 6$

M

K	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

M

K	0	1	2	3	4	5
0	0	1	2	3	4	5
1	2	3	4	5	0	1
2	4	5	0	1	2	3
3	0	1	2	3	4	5
4	2	3	4	5	0	1
5	4	5	0	1	2	3

Імовірність $P\{E_K(M) = C\}$ – це кількість випадків отримання шифротексту C при зашифруванні відкритого тексту M, ділена на потужність ключового простору. Так, у випадку а) маємо: $P\{E_K(M) = 4\} = \frac{1}{6}$, бо шифротекст 4 однократно з’являється під час шифрування кожного відкритого тексту при застосуванні кожного з ключів. Узагальнивши результат, визначимо, що

$$P\{E_K(M) = C\} = \frac{\left|\{K \in Z_6 :\ K + M \bmod 6 = C\}\right|}{\left|Z_6\right|} = \frac{1}{6}.$$

Отже, такий шифр досконало стійкий.

Для випадку б) аналогічно обчислимо

$$P\{E_K(0) = 4\} = \frac{2}{6} = \frac{1}{3}; \quad P\{E_K(1) = 4\} = \frac{0}{6} = 0,$$

тобто ми знайшли такі відкриті тексти $M_1 = 0$, $M_2 = 1$ і шифротекст $C = 4$, що $P\{E_K(M_1) = C\} \neq P\{E_K(M_2) = C\}$. Тому така криптосистема не може бути досконалою.

Задача 5. Простір відкритих текстів складається з двох текстів $M = \{M_1, M_2\}$ із розподілом імовірностей: $p(M_1) = 1/4$; $p(M_2) = 3/4$. Простір ключів містить три ключі $K = \{k_1, k_2, k_3\}$, імовірності вибору ключів $p(k_1) = 1/2$, $p(k_2) = 1/4$, $p(k_3) = 1/4$. Простір шифротекстів являє собою множину $C = \{C_1, C_2, C_3, C_4\}$, а функція зашифрування задана таблицею

		M	
		M_1	M_2
K	k_1	C_1	C_2
	k_2	C_2	C_3
	k_3	C_3	C_4

Обчисліть невизначеність шифру за ключем.

Р о з в’ я з а н н я. Імовірності виникнення шифротекстів:

$$p(C_1) = p(M_1) \cdot p(k_1) = \frac{1}{4} \cdot \frac{1}{2} = \frac{1}{8};$$

$$p(C_2) = p(M_1) \cdot p(k_2) + p(M_2) \cdot p(k_1) = \frac{1}{4} \cdot \frac{1}{4} + \frac{3}{4} \cdot \frac{1}{2} = \frac{7}{16};$$

$$p(C_3) = p(M_1) \cdot p(k_3) + p(M_2) \cdot p(k_2) = \frac{1}{4} \cdot \frac{1}{4} + \frac{3}{4} \cdot \frac{1}{4} = \frac{1}{4};$$

$$p(C_4) = p(M_2) \cdot p(k_3) = \frac{3}{4} \cdot \frac{1}{4} = \frac{3}{16}.$$

Обчислюємо ентропію розподілу відкритих текстів, ключів та шифротекстів:

$$H(M) = -\frac{1}{4}\log_2\frac{1}{4} - \frac{3}{4}\log_2\frac{3}{4} \approx 0{,}81;$$

$$H(K) = -\frac{1}{2}\log_2\frac{1}{2} - 2 \cdot \frac{1}{4}\log_2\frac{1}{4} \approx 1{,}5;$$

$$H(C) = -\frac{1}{8}\log_2\frac{1}{8} - \frac{7}{16}\log_2\frac{7}{16} - \frac{1}{4}\log_2\frac{1}{4} - \frac{3}{16}\log_2\frac{3}{16} \approx 1{,}85;$$

Тепер можна знайти невизначеність шифру за ключем:

$H(K \mid C) = H(K) + H(M) - H(C) \approx 1{,}5 + 0{,}81 - 1{,}85 = 0{,}46$ (бітів).

Задача 6. Простір відкритих текстів складається з двох текстів $M = \{A; B\}$ із розподілом імовірностей: $p(A) = 2/3;\ p(B) = 1/3$. Простір

ключів містить чотири ключі $K=\{1;2;3;4\}$, імовірність вибору яких однакова. Простір криптограм являє собою множину $C=\{a;b;c\}$, а функція шифрування задана матрицею

K	$E_k(A)$	$E_k(B)$
1	a	b
2	b	c
3	b	a
4	c	a

,

причому ключі для шифрування дібрані незалежно від вибору відкритого тексту. Покажіть, що апостеріорна умовна ймовірність

$$P\{M=A\big|C=a\}=\frac{P\{M=A\}}{2-P\{M=A\}}.$$

Чи матиме такий шифр досконалу стійкість? Обчисліть невизначеність шифру за ключем.

Р о з в’ я з а н н я. За умовою $P\{K=i\}=\frac{1}{4}$, $i=1,2,3,4$. За теоремою Байеса дістаємо

$$P\{M=A\big|C=a\}=\frac{P\{M=A\}\cdot P\{C=a\big|M=A\}}{P\{C=a\}}.$$

Оскільки вибір відкритого тексту не залежіть від вибору ключа для зашифрування, то

$$P\{C{=}a\}=P\{K{=}1\}\cdot P\{M{=}A\}+P\{K{=}3\}\cdot P\{M{=}B\}+P\{K{=}4\}\cdot P\{M{=}B\}=$$

$$=\frac{1}{4}\cdot P\{M{=}A\}+\frac{1}{4}\cdot P\{M{=}B\}+\frac{1}{4}\cdot P\{M{=}B\}=\frac{1}{4}\cdot P\{M{=}A\}+\frac{1}{2}\cdot\big(1-P\{M{=}A\}\big)=$$

$$=\frac{1}{2}-\frac{1}{4}P\{M{=}A\}.$$

Крім того,

$$P\{C=a\big|M=A\}=P\{K=1\}=\frac{1}{4}.$$

Тоді

$$P\{M=A\,|\,C=a\}=\frac{\frac{1}{4}\cdot P\{M=A\}}{\frac{1}{2}-\frac{1}{4}P\{M=A\}}=\frac{P\{M=A\}}{2-P\{M=A\}}.$$

Щоб шифр відносився до досконало стійких, потрібно виконання умови $P\{M=j\,|\,C=i\}=P\{M=j\}$ для всіх пар (i,j) «відкритий текст – відповідний шифротекст». Як вже доведено $P\{M=A\,|\,C=a\}\neq P\{M=A\}$ (крім випадку, коли $P\{M=A\}=0$ і $P\{M=A\}=1$), тому даний шифр не має досконалої стійкості.

Далі обчислимо невизначеність шифру за ключем

$$H(K\,|\,C)=H(K)+H(M)-H(C).$$

Необхідні значення ентропії ключа, відкритих текстів складають:

$$H(K)=4\left(-\frac{1}{4}\log_2\frac{1}{4}\right)=2\,(\text{біти});$$

$$H(M)=-P\{M=A\}\log_2 P\{M=A\}-P\{M=B\}\log_2 P\{M=B\}=$$

$$=-\frac{2}{3}\log_2\frac{2}{3}--\frac{1}{3}\log_2\frac{1}{3}\approx 0{,}92\,(\text{біти});$$

Для визначення ентропії шифротекстів спочатку знайдемо ймовірності їх появ при зашифруванні:

$$P\{C=a\}=P\{K=1\}\cdot P\{M=A\}+P\{K=3\}\cdot P\{M=B\}+P\{K=4\}\cdot P\{M=B\}=$$

$$=\frac{1}{4}\left(\frac{2}{3}+\frac{1}{3}+\frac{1}{3}\right)=\frac{1}{3};$$

$$P\{C=b\}=P\{K=2\}\cdot P\{M=A\}+P\{K=3\}\cdot P\{M=A\}+P\{K=1\}\cdot P\{M=B\}=$$

$$=\frac{1}{4}\left(\frac{2}{3}+\frac{2}{3}+\frac{1}{3}\right)=\frac{5}{12};$$

$$P\{C=c\}=P\{K=4\}\cdot P\{M=A\}+P\{K=2\}\cdot P\{M=B\}=\frac{1}{4}\left(\frac{2}{3}+\frac{1}{3}\right)=\frac{1}{4}.$$

$$H(C) = -\frac{1}{3}\log_2\frac{1}{3} - \frac{5}{12}\log_2\frac{5}{12} - \frac{1}{4}\log_2\frac{1}{4} \approx 1{,}55 \text{ (бітів);}$$

$$H(K \mid C) = 2 + 0{,}92 - 1{,}55 \approx 1{,}36 \text{ (бітів).}$$

Задача 7. Розглянемо джерело повідомлень M, що генерує два символи у відповідності з законом розподілу: $P(m=0)=p$; $P(m=1)=q$; $p+q=1$, і одноразовий блокнот з рівномірним розподілом ймовірностей знаків гами: $P(k=0)=1/2$; $P(k=1)=1/2$. Рівняння шифрування $c_i = m_i \oplus k_i$, де m_i, k_i, c_i – біти відкритого тексту, гами та шифротексту. Яким є розподіл імовірностей шифротекстів? Визначте ентропію $H(M)$ відкритих текстів, ентропію $H(K)$ ключів, ентропію $H(C)$ шифротекстів та взаємну інформацію $I(M,C)$ відкритих текстів і шифротекстів. Якщо знаки гами шифру нерівноймовірні, наприклад, $P(k=0)=3/4$, $P(k=1)=1/4$, то як зміняться значення $H(C)$, $H(K)$ та $I(M \mid C)$?

Р о з в’ я з а н н я.

$$P\{c=0\} = P\{m=0\}P\{k=0\} + P\{m=1\}P\{k=1\} = \frac{1}{2}p + \frac{1}{2}q = \frac{p+q}{2} = \frac{1}{2};$$

$$P\{c=1\} = P\{m=1\}P\{k=0\} + P\{m=0\}P\{k=1\} = \frac{1}{2}p + \frac{1}{2}q = \frac{q+p}{2} = \frac{1}{2};$$

$$H(M) = -p\log_2 p - q\log_2 q; \quad H(K) = -\frac{1}{2}\log_2\frac{1}{2} - \frac{1}{2}\log_2\frac{1}{2} = 1 \text{ (біт);}$$

$$H(C) = 1 \text{ (біт).}$$

Сумісний розподіл ймовірностей відкритих тестів і шифротекстів є рівномірним:

$$P\{m=0, c=0\} = P\{m=0, c=1\} = \frac{p}{2}; \quad P\{m=1, c=0\} = P\{m=1, c=1\} = \frac{q}{2}.$$

Взаємну інформацію $I(M \mid C)$ відкритих текстів і шифротекстів обчислимо за допомогою сумісної ентропії $H(M,C)$:

$$I(M,C) = H(M) - H(M \mid C) = H(M) + H(C) - H(M,C),$$

$$H(M,C) = -P\{m=0, c=0\}\log_2 P\{m=0, c=0\} - P\{m=0, c=1\}\log_2 P\{m=0, c=1\} -$$

$$-P\{m=1, c=0\}\log_2 P\{m=1, c=0\} - P\{m=1, c=1\}\log_2 P\{m=1, c=1\}.$$

$$I(M|C)=-p\log_2 p-q\log_2 q+1+\frac{p}{2}\log_2\frac{p}{2}+\frac{p}{2}\log_2\frac{p}{2}+\frac{q}{2}\log_2\frac{q}{2}+\frac{q}{2}\log_2\frac{q}{2}=$$

$$=-p\log_2 p-q\log_2 q+1+p\cdot\log_2\frac{p}{2}+q\cdot\log_2\frac{q}{2}=$$

$$=-p\log_2 p-q\log_2 q+1+p\cdot\log_2 p-p+q\cdot\log_2 q-q=0,$$

бо за умовою $p+q=1$.

У випадку $P\{k=0\}=3/4$, $P\{k=1\}=1/4$ маємо

$$P\{c=0\}=P\{m=0\}P\{k=0\}+P\{m=1\}P\{k=1\}=\frac{3}{4}p+\frac{1}{4}q=\frac{3p+q}{4};$$

$$P\{c=1\}=P\{m=1\}P\{k=0\}+P\{m=0\}P\{k=1\}=\frac{1}{4}p+\frac{3}{4}q=\frac{3q+p}{4};$$

$$H(M)=-p\log_2 p-q\log_2 q;\ \ H(K)=-\frac{3}{4}\log_2\frac{3}{4}-\frac{1}{4}\log_2\frac{1}{4}\approx 0,81\,(\text{біт});$$

$$H(C)=-\frac{3p+q}{4}\log_2\frac{3p+q}{4}-\frac{3q+p}{4}\log_2\frac{3q+p}{4}.$$

Сумісний розподіл імовірностей відкритих тестів і шифротекстів змінюється:

$$P\{m=0,c=0\}=\frac{3p}{4};\ P\{m=0,c=1\}=\frac{p}{4};\ P\{m=1,c=0\}=\frac{3q}{4};\ P\{m=1,c=1\}=\frac{q}{4}.$$

Тоді взаємна інформація відкритих текстів і шифротекстів

$$I(M\mid C)=H(M)-H(M\mid C)=H(M)+H(C)-H(M,C)=$$

$$=-p\log_2 p-q\log_2 q-\frac{3p+q}{4}\log_2\frac{3p+q}{4}-\frac{3q+p}{4}\log_2\frac{3q+p}{4}+$$

$$+\frac{3p}{4}\log_2\frac{3p}{4}+\frac{p}{4}\log_2\frac{p}{4}+\frac{3q}{4}\log_2\frac{3q}{4}+\frac{q}{4}\log_2\frac{q}{4}=$$

$$=-\frac{3p+q}{4}\log_2\frac{3p+q}{4}-\frac{3q+p}{4}\log_2\frac{3q+p}{4}+\frac{3}{4}\log_2\frac{3}{4}+\frac{1}{4}\log_2\frac{1}{4}\approx$$

$$\approx-\frac{3p+q}{4}\log_2\frac{3p+q}{4}-\frac{3q+p}{4}\log_2\frac{3q+p}{4}-0,8.$$

Задача 8. Знайдіть відстань єдиності шифру Віженера при шифруванні українського тексту. Вважайте, що надлишковість української мови складає 0,75.

Р о з в' я з а н н я. Нехай гама шифру нараховує n знаків і має вигляд $k_0k_1...k_{n-1}$. Обчислимо ентропію ключового простору

$$H(K) = H(k_0) + H(k_1|k_0) + H(k_2|k_0k_1) + ... + H(k_{n-1}|k_0k_1...k_{n-2}).$$

Прийнявши, що поява знаку k_i гами не залежіть від появи попереднього її знаку і всі знаки рівноймовірні, маємо

$$H(K) = H(k_0) + H(k_1) + ... + H(k_{n-1}) = n \cdot H(k) = n \cdot \log_2 m,$$

де m – потужність використаного алфавіту. За цих умов визначимо відстань єдиності шифру Віженера

$$L = \frac{\log_2 |K|}{D \cdot \log_2 m} = \frac{H(K)}{D \cdot \log_2 m} = \frac{n \cdot \log_2 m}{0,75 \cdot \log_2 m} = \frac{4}{3}n.$$

Задача 9. Нехай $M_1, M_2, ..., M_n$– послідовність незалежних десяткових знаків, що перетворюється за допомогою шифру простої заміни у послідовність $C_1, C_2, ..., C_n$, де $C_i \in Z_{10} = \{0,1,2,3,4,5,6,7,8,9\}$. Визначте відстань єдиності шифру за умови, що $P\{M=0\} = P\{M=1\} = 4 \cdot P\{M=2\}$, а $P\{M=2\} = P\{M=3\} = ... = P\{M=9\}$.

Р о з в' я з а н н я. Загальна кількість ключів – $10!$, потужність алфавіту $m = 10$. За умовою розподіл імовірностей десяткових знаків у відкритих текстах має вигляд:

M_0	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9
$4p$	$4p$	p	p	p	p	p	p	p	p

Звідси $4p + 4p + 8p = 1 \Rightarrow p = 1/16$. Обчислимо ентропію мови

$$H(M) = -2 \cdot \frac{1}{4}\log_2 \frac{1}{4} - 8 \cdot \frac{1}{16}\log_2 \frac{1}{16} = 3 \text{ (біти)},$$

і її надлишковість $D = 1 - \frac{H(M)}{\log_2 m} = 1 - \frac{3}{\log_2 10} = \frac{\log_2 10 - 3}{\log_2 10}$. Тоді відстань єдиності шифру

$$L = \frac{\log_2 |K|}{D \cdot \log_2 m} = \frac{\log_2 10!}{\frac{\log_2 10 - 3}{\log_2 10} \cdot \log_2 10} = \frac{\log_2 10!}{\log_2 10 - 3} \approx 68 \text{(знаків)}.$$

Задача 10. У криптосистемі простір M відкритих текстів, простір C криптограм і простір K ключів являють собою рядки з m бітів, а ключі вибираються випадково й рівноймовірно. Криптосистема використовується для зашифрування повідомлень, створених з m-бітових відрізків, кожен з яких містить лише один біт «1», а решта бітів – «0». Поява блоків у відкритих текстах незалежна і рівноймовірна. Доведіть, що відстань єдиності такого шифру не більше за 2 при всіх значеннях m, крім $m = 3$.

Р о з в' я з а н н я. Усього існує m різних m-бітових відрізків, до складу якого входить лише один біт «1». Оскільки вони всі рівноймовірні, то ентропія одного відрізка $H(P) = \log_2 m$. Оскільки вибір блоків незалежний, то ентропія мови дорівнюватиме

$$H = \lim_{n \to \infty} \frac{H(P^n)}{n} = \lim_{n \to \infty} \frac{nH(P)}{n} = H(P) = \log_2 m.$$

Тепер знайдемо надлишковість мови

$$D = 1 - \frac{H}{\log_2 2^m} = 1 - \frac{\log_2 m}{m} = \frac{m - \log_2 m}{m}.$$

Тоді відстань єдиності шифру становить

$$L = \frac{\log_2 |K|}{D \cdot \log_2 m} = \frac{\log_2 m}{\frac{m - \log_2 m}{m} \cdot \log_2 m} = \frac{m}{m - \log_2 m}.$$

Очевидно, що $L \le 2$ тільки тоді, коли $\log_2 m \le \frac{m}{2}$. Остання рівність виконується при всіх додатних цілих значеннях m, крім $m = 3$, бо $\log_2 3 \approx 1{,}585$.

Задача 11. У деякій криптосистемі для кожної пари (m, c), де m – відкритий текст з множини M відкритих текстів, c – шифрований текст з множини C шифротекстів, існує лише один ключ k з множини ключів K, за допомогою якого виконується перетворення $E_k(m) = c$. Довести, що така криптосистема матиме досконалу стійкість тоді і тільки тоді, коли ентропія ключів дорівнює ентропії шифротекстів, тобто $H(K) = H(C)$.

Р о з в’ я з а н н я. Оскільки у множині ключів K існує лише один ключ k, при якому $E_k(m) = c$, то умовна ентропія $H(K|MC) = 0$. Тоді

$$H(MKC) = H(MC) + H(K|MC) = H(MC).$$

Крім того для будь-якої криптосистеми справедливо

$$H(MKC) = H(MK) = H(M) + H(K).$$

Тоді

$$H(MC) = H(M) + H(K);$$

$$H(C) + H(M|C) = H(MC) = H(M) + H(K).$$

Коли ентропія $H(K)$ ключів дорівнює ентропії $H(C)$ шифротекстів, то з останнього виразу випливає, що $H(M|C) = H(M)$, що збігається з визначенням досконало стійкої криптосистеми за Шенноном.

Задача 12. Чи буде шифр досконало стійким, якщо при будь-якому розподілі над простором M відкритих текстів для будь-яких повідомлень m і $m' \in M$ і для будь-якого шифротексту c із простору C шифротекстів виконується рівність

$$P\{m_0 = m \mid c_0 = c\} = P\{m_0 = m' \mid c_0 = c\}?$$

Р о з в’ я з а н н я. Нехай деякий шифр є досконало стійким. Це означає, що при будь-якому розподілі над простором M відкритих текстів для будь-якого повідомлення $m \in M$ і для будь-якого шифротексту $c \in C$ справджується рівність

$$P\{m_0 = m \mid c_0 = c\} = P\{m_0 = m\}.$$

Тепер розглянемо розподіл імовірностей відкритих текстів, де для текстів m і $m' \in M$

$$P(m_0 = m) \neq P(m_0 = m').$$

Наприклад, нехай множина $M = \{0,1\}$, $P(0) = 0,75$, $P(1) = 0,25$. Тоді для будь-якого шифротексту $c \in C$

$$P\{m_0 = m \mid c_0 = c\} = P\{m_0 = m\} \neq P\{m_0 = m'\} = P\{m_0 = m' \mid c_0 = c\}.$$

Тому у загальному випадку шифр із зазначеною умовою не буде досконало стійким.

Задача 13. Доведіть, що $I(M;C) \geq H(M) - H(K)$, тобто якщо ключовий простір K криптосистеми має невелику потужність, то спостерігатиметься значний витік інформації про відкритий текст.

Р о з в’ я з а н н я. Для будь-якої нетривіальної криптосистеми виконуються нерівності між ентропіями

$$H(M|C) \le H(K|C) \le H(K).$$

Тоді, $I(M;C) = H(M) - H(M|C) \ge H(M) - H(K).$

ТЕСТИ

1. Шифр має теоретико-інформаційну стійкість, якщо
   а) розкриття шифру найкращим з існуючих криптоаналітичних алгоритмів потребує невиправдано великих витрат обчислювальних ресурсів;
   б) отримання інформації про шифротекст C не змінює інформацію про відповідний вихідний текст M: $P(M \mid C) = P(M)$;
   в) розкриття шифру можна звести до розв’язання деякої важкорозв’язувальної математичної проблеми, покладеної в основу криптоалгоритму;
   г) розкриття шифру можливо тільки за умови, що криптоаналітик має нескінченно великі обчислювальні ресурси та необмежений час;

2. Щоб шифр мав довідну стійкість, потрібно
   а) довести, що шифр неможливо зламати за допомогою всіх існуючих криптоаналітичних алгоритмів;
   б) довести стійкість шифру за допомогою теорії інформації;
   в) звести розкриття шифру до розв’язання важкої математичної проблеми, що лежить в основі шифру;
   г) показати, що розкриття шифру можливо тільки, коли криптоаналітик має нескінченно великі обчислювальні ресурси.

3. Якщо шифр має гарантовану обчислювальну стійкість, то
   а) алгоритм, що реалізує процес шифрування, потребує невиправдано великих витрат обчислювальних ресурсів;
   б) розкрити шифр неможливо будь-яким криптоаналітичним алгоритмом, навіть маючи необмежені обчислювальні ресурси та час;
   в) найкращий з існуючих критоаналітичних алгоритмів потребує невиправдано великих витрат обчислювальних ресурсів;
   г) в основу криптоалгоритму шифрування покладено розв’язання деякої важкообчислювальної проблеми.

4. Який з нижченаведених шифрів має теоретико-інформаційну стійкість?

а) RSA; б) шифр Віженера; в) DES;
г) одноразовий шифрувальний блокнот; д) шифр Хілла.

5. Які з нижченаведених шифрів не мають гарантованої обчислювальної стійкості?

а) RSA; б) шифр Віженера; в) AES;
г) DES; д) шифр Хілла.

6. Які з нижченаведених шифрів відносяться до шифрів з довідною стійкістю?

а) RSA; б) шифр Віженера; в) AES;
г) одноразовий шифрувальний блокнот; д) шифр Ель-Гамаля.

7. x – відкритий текст, y – його криптограма, k – ключ шифру. Яка ймовірність цікавіша для криптоаналітика?

а) $p_{відкр./кр.}(x \mid y)$; б) $p_{кр./відкр.}(y \mid x)$;
в) $p_{відкр./кл.}(x \mid k)$; г) $p_{кр.}(y)$.

8. Нехай x – відкритий текст, y – його криптограма, отримана за допомогою шифру з ключем k. За якої умови шифр буде досконало стійким?

а) $p_{відкр./кр.}(x \mid y) = p_{кр.}(y)$; б) $p_{відкр./кр.}(x \mid y) = p_{відкр.}(x)$;
в) $p_{відкр./кр.}(x \mid y) = p_{кл.}(k)$; г) $p_{відкр./кл.}(x \mid k) = p_{кр.}(y)$.

9. Для шифру з ентропіями ключів $H(K)$, криптограм $H(Y)$ та відкритих текстів $H(X)$ у будь-якому випадку *не* може виконуватися співвідношення

а) $H(Y \mid X,K) = 0$; б) $H(X \mid K,Y) = 0$;
в) $H(K \mid Y) = H(K) + H(X) - H(Y)$; г) $H(K,Y) = H(X) - H(K)$.

10. Якими нерівностями зв'язані потужності просторів відкритих текстів $|X|$, шифрованих текстів $|Y|$ та ключів $|K|$ досконало стійкого шифру?

а) $|X| \ge |Y| \ge |K|$; б) $|X| \ge |Y|$, $|Y| \le |K|$;
в) $|X| \le |Y| \le |K|$; г) $|X| \le |Y|$, $|Y| \ge |K|$.

11. $|K|$ – потужність простору ключів деякого шифру. З цього простору обирається навмання сукупність з n ключів. Яка ймовірність того, що потрібний ключ буде відсутній у цій сукупності (у відповіді ця ймовірність апроксимується за допомогою числа e)?

а) $e^{-|K|/n}$;
б) $e^{-\sqrt{|K|}/n}$;
в) $e^{-n/\sqrt{|K|}}$;
г) $e^{-|K|/n^2}$.

12. Шифр називається ендоморфним, якщо

а) простір відкритих текстів збігається з простором криптограм;
б) для букв (або їх сукупностей) з великою частотою вживання в даній мові пропонується кілька різних шифропозначень;
в) його стійкість можна довести за допомогою теорії інформації;
г) у криптоалгоритмі для зашифрування і розшифрування використовують різні ключі.

13. Яке з нижченаведених положень не має відношення до шифрування за допомогою одноразового шифрувального блокноту?

а) шифрувальна гама має бути істинно випадковою числовою послідовністю;
б) шифрувальна гама може використовуватися лише один раз;
в) довжини використаної шифрувальної гами та відкритого тексту однакові;
г) відкритий текст розбивається на блоки, до кожного з яких додається однаковий блок шифрувальної гами.

14. Джерело відкритих текстів породжує текст посимвольно із використанням алфавіту {a,b,c,d,e}. При якому з нижченаведених розподілів імовірностей символів алфавіту ентропія згенерованого тексту буде максимальною?

а) p(a) = p(b) = 0,3; p(c) = p(d) = 0,2; p(e) = 0;
б) p(a) = p(b) = p(c) = p(d) = p(e) = 0,2;
в) p(a) = p(b) = p(c) = p(d) =0; p(e) = 1;
г) p(a) = 0,2; p(b) = 0,1; p(c) = 0,3; p(d) = 0,3; p(e) = 0,1.

15. Джерело відкритих текстів породжує текст посимвольно із використанням алфавіту {a,b,c,d,e}. При якому з нижченаведених розподілів імовірностей символів алфавіту ентропія згенерованого тексту буде мінімальною?

а) p(a) = p(b)=0,3; p(c) = p (d) = 0,2; p(e) = 0;
б) p(a) = p(b) = p(c) = p(d) = p(e) = 0,2;
в) p(a) = p(b) = p(c) = p(d) = 0; p(e) = 1;
г) p(a) = 0,1; p(b) = 0,2; p(c) = 0,3; p(d) = 0,3; p(e) = 0,1.

16. Ентропія мови – це

а) різниця між кількостями інформації, що містяться у відкритому та шифрованому текстах;
б) міра кількості інформації, що припадає на одну букву відкритого тексту даною мовою;
в) міра кількості інформації, що припадає на всі букви відкритого тексту даною мовою;
г) міра кількості інформації, яка залишається у шифрованому тексті.

17. Якщо H_r – ентропія ймовірнісного розподілу r-грам відкритого тексту деякою мовою, то чому дорівнює границя $\lim\limits_{r\to\infty}\frac{H_r}{r}$?

а) надлишковості мови; б) відстані єдиності шифру;
в) абсолютній ентропії мови; г) ентропії мови.

18. За якою формулою визначається надлишковість мови з ентропією *H*, якщо для запису відкритих текстів цією мовою використовується алфавіт з m букв?

а) $D=\frac{H}{\log_2 m}$; б) $D=\frac{H}{\log_2 m}$;

в) $D=\frac{\log_2 m}{H}-1$; г) $D=1-\frac{H}{\log_2 m}$.

19. Якщо у комп'ютері стискання тексту, поданого у коді ASCII, відбувається за допомогою ідеально архівуючого алгоритму, то надлишковість стиснутого тексту

а) зростає; б) дорівнює надлишковості мови;
в) не змінюється; г) наближається до нуля.

20. Нехай надлишковість деякої мови становить 75 %. Тоді без втрати інформації

а) у відкритому тексті цією мовою можна викреслити будь-які три з чотирьох букв;
б) у відкритому тексті цією мовою можна викреслити не більше, ніж одну з чотирьох букв;
в) при оптимальному кодуванні відкритий текст можна стиснути на 3/4 довжини;
г) при оптимальному кодуванні відкритий текст можна стиснути не більше, ніж на чверть довжини.

21. Відстань єдиності (унікальності) шифру за ключем – це

а) мінімальна довжина шифрованого тексту, необхідного для однозначного визначення істинного ключа шифру;

б) максимальна довжина шифрованого тексту, що можна отримати при шифруванні одного блока інформації;
в) довжина істинного ключа шифру;
г) кількість фальшивих ключів шифру.

22. Відстані єдиності (унікальності) двох шифрів дорівнюють L_{01} і L_{02} відповідно. Якому з них слід віддати перевагу при шифруванні, якщо $L_{01} > L_{02}$?

а) першому; б) другому;
в) жоден з шифрів не має переваг; г) інша відповідь.

23. За якою формулою визначається відстань єдиності шифру за ключем для потокового шифру з рівноймовірним вибором ключів, якщо потужність ключового простору $|K|$, надлишковість мови D, ентропія мови H_0, а алфавіт відкритих текстів складається з m букв?

а) $L_0 = \dfrac{\log_2 |K|}{D \cdot \log_2 H}$; б) $L_0 = \dfrac{\log_2 m}{D \cdot \log_2 |K|}$;

в) $L_0 = \dfrac{\log_2 |K|}{D \cdot \log_2 m}$; г) $L_0 = \dfrac{\log_2 |K|}{m \cdot \log_2 H}$.

24. Обчислити відстань єдиності шифру за ключем для потокового шифру з рівноймовірними ключами, якщо потужність ключового простору дорівнює 2^{60}, надлишковість мови 75 %, а абетка налічує 32 букви?

а) 48 букв; б) 25 букв;
в) 64 букви; г) 16 букв.

25. Формула для невизначеності шифру за ключем має вигляд

а) $H(K|Y) = H(K) - H(X) - H(Y)$;
б) $H(K|Y) = H(K) - H(X) + H(Y)$;
в) $H(K|Y) = H(K) + H(X) - H(Y)$;
г) $H(K|Y) = H(K) - H(X) + H(Y)$.

26. Скільки бітів інформації залишається знайти про істинний ключ шифрування після перехоплення криптограми, якщо ентропія відкритих текстів $H(X) = 2$ біта, ентропія ключів $H(K) = 1,5$ біта, ентропія шифрованих текстів $H(Y) = 2,7$ біта? Скільки при цьому бітів інформації про ключ «повідомляє» криптограма?

а) $0,4$ бітів; $1,1$ біта; б) $0,8$ бітів; $0,7$ біта;
в) $2,2$ бітів; $0,7$ біта; г) $3,2$ бітів; $1,7$ біта.

27. Завдяки надлишковості мови

а) усі відкриті тексти є рівноймовірними;
б) невизначеність відкритого тексту зменшується у разі зростання кількості відомих символів шифрованого тексту;
в) середня ентропія букви у відкритому тексті значно більша, ніж $\log_2 m$ (m – потужність використаної абетки);
г) ентропія мови менша, ніж її абсолютна ентропія.

РОЗДІЛ 3. БЛОКОВЕ ШИФРУВАННЯ

Задача 1. Для криптоалгоритму DES визначте, які з операцій IP, E, додавання раундового ключа $(+K)$, підстановка за допомогою S-боксів, підстановка за допомогою P-боксу відповідають вимозі лінійності: $f(X_1 \oplus X_2) = f(X_1) \oplus f(X_2)$?

Р о з в' я з а н н я. Нехай $(s_1, s_2, ..., s_{64})$, $(t_1, t_2, ..., t_{64})$ – два 64-бітових вектори.

- $IP(s_1, s_2, ..., s_{64}) = (s_{58}, s_{50}, ..., s_7)$; $IP(t_1, t_2, ..., t_{64}) = (t_{58}, t_{50}, ..., t_7)$

$IP(s_1, s_2, ..., s_{64}) \oplus IP(t_1, t_2, ..., t_{64}) = (s_{58} \oplus t_{58}, s_{50} \oplus t_{50}, ..., s_7 \oplus t_7) =$

$= IP(s_{58} \oplus t_{58}, s_{50} \oplus t_{50}, ..., s_7 \oplus t_7)$– лінійна операція.

- Якщо R_s і L_s – ліва та права половини вектора $IP(s_1, s_2, ..., s_{64})$, R_t і L_t – ліва та права половини вектора $IP(t_1, t_2, ..., t_{64})$, то за цих позначень $R_s = (r_{s_1}, r_{s_2}, ..., r_{s_{32}})$ і т.д. Тоді

$E(r_{s_1}, r_{s_2}, ..., r_{s_{32}}) = (r_{s_{32}}, r_{s_1}, r_{s_2}, r_{s_3}, ..., r_{s_1})$;

$E(r_{t_1}, r_{t_2}, ..., r_{t_{32}}) = (r_{t_{32}}, r_{t_1}, r_{t_2}, r_{t_3}, ..., r_{t_1})$.

$E(r_{s_1}, ..., r_{s_{32}}) \oplus E(r_{t_1}, ..., r_{t_{32}}) = (r_{s_{32}}, r_{s_1}, r_{s_2}, r_{s_3}, ..., r_{s_1}) \oplus$

$\oplus (r_{t_{32}}, r_{t_1}, r_{t_2}, r_{t_3}, ..., r_{t_1}) = E(r_{s_1} \oplus r_{t_1}, r_{s_2} \oplus r_{t_2}, ..., r_{s_{32}} \oplus r_{t_{32}})$ –

лінійна операція.

- $+K$ – додавання раундового ключа.

$(a \oplus K) \oplus (b \oplus K) = (a \oplus b) \oplus (K \oplus K) = a \oplus b \neq (a \oplus b) \oplus K$ –

нелінійна операція.

- Підстановки, що реалізуються за допомогою S-боксів.

$S_1(000000) \oplus S_1(111111) = 1110 \oplus 1101 = 0011$;

$S_1(000000 \oplus 111111) = S_1(111111) = 1101$;

$S_1(000000) \oplus S_1(111111) \neq S_1(000000 \oplus 111111)$ –

нелінійна операція.

- Перестановки, що реалізуються за допомогою P-боксів.

Нехай (x_N), (y_N) – блоки з N бітів.

$$P(x_1,...,x_N) \oplus P(y_1,...,y_N) = (x_{P(1)},...,x_{P(N)}) \oplus (y_{P(1)},...,y_{P(N)}) =$$
$$= (x_{P(1)} \oplus y_{P(1)},...,x_{P(N)} \oplus y_{P(N)}) = P(x_{P(1)} \oplus y_{P(1)},...,x_{P(N)} \oplus y_{P(N)}) -$$

лінійна операція.

Задача 2. Покажіть, що другий рядок четвертого S-боксу DES можна дістати з його першого рядку за допомогою перетворення

$$x_1x_2x_3x_4 = x_2x_1x_4x_3 \oplus 0110.$$

Р о з в’ я з а н н я. За таблицею замін у S_4-боксі DES

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

дістаємо

$$7_{10} = 0111_2 \to 1011_2 \oplus 0110_2 = 1101_2 = 13_{10};$$

$$13_{10} = 1101_2 \to 1110_2 \oplus 0110_2 = 1000_2 = 8_{10};$$

$$14_{10} = 1110_2 \to 1101_2 \oplus 0110_2 = 1011_2 = 11_{10};$$

$$3_{10} = 0011_2 \to 0011_2 \oplus 0110_2 = 0101_2 = 5_{10}$$ і т.д.

Задача 3. Якщо замінити перший біт b_1 у лівому півблоці L_0 вхідних даних, що шифрують за допомогою алгоритму DES, то яка максимальна кількість бітів може змінитися у шифротексті (L_1, R_1) на виході після першого раунду порівняно з аналогічним результатом для незмінених даних? Ключ шифрування однаковий в обох випадках, процесс раундового перетворення $L_i = R_{i-1};\ R_i = L_{i-1} \oplus f(R_{i-1}; K_i)$.

Р о з в’ я з а н н я. Процес перетворення першого раунду алгоритму DES виглядає так:

$$\begin{cases} L_1 = R_0; \\ R_1 = L_0 \oplus f(R_0; K_1), \end{cases}$$

де K_1 – ключ першого раунду. Отже, при заміні першого біта b_1 у лівому півблоці L_0 лівий півблок L_1 залишиться без змін, а у півблоці R_1 може змінитися тільки один біт.

Задача 4. Якщо усі перші старші 44 біти 64-бітового ключа криптоалгоритму DES дорівнюють нулю, то яка ефективна довжина такого ключа?

Р о з в' я з а н н я. Згідно з алгоритмом генерації раундових ключів 64-бітовий ключ криптоалгоритму DES скорочують до 56 бітів вилученням кожного восьмого біта у позиціях з номерами 8, 16, 24, 32, 40, 48, 56 і 64. Схематично цей процес проілюстровано на рис. 3.1.

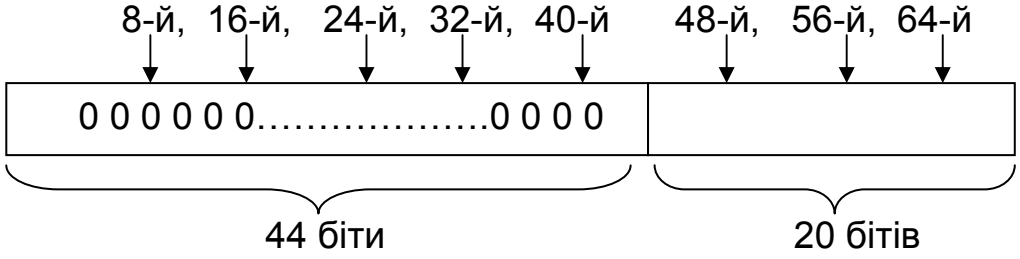


Рис. 3.1

Ефективна довжина ключа шифру: 20 бітів – 3 біти = 17 бітів.

Задача 5. У DES-подібному криптоалгоритмі (рис. 3.2) на вхід подається блок довжини $2n$ бітів, який ділиться на два блоки M_0, M_1 довжини n. Ключ раунду K складається з n бітів і не змінюється. Раундова функція $f(K,M) = K \oplus M$ отримує на вхід n бітів і видає на виході також n бітів. Шифрування складається з трьох раундів. Якщо на вхід раунду подається пара півблоків M_j, M_{j+1}, то на виході раунду отримаємо пару M_{j+1}, M_{j+2}, де $M_{j+2} = M_j \oplus f(k, M_{j+1})$. Якщо ви знаєте тільки результат $M_3 M_4$ шифрування трьох раундів, то чи можна відновити відкритий текст?

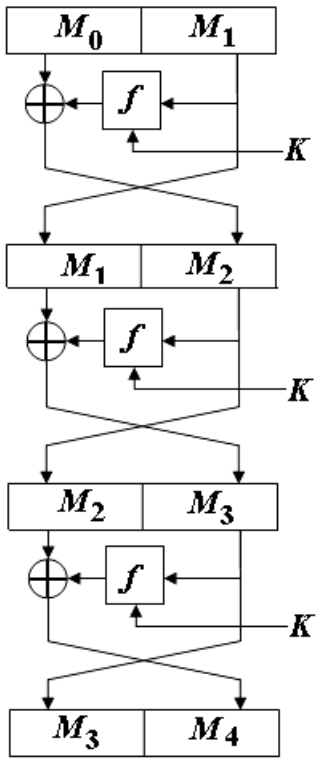


Рис. 3.2

Р о з в' я з а н н я.

$$M_4 = M_2 \oplus M_3 \oplus K; \quad (1)$$

$$M_3 = M_1 \oplus M_2 \oplus K; \quad (2)$$

$$M_2 = M_0 \oplus M_1 \oplus K; \quad (3)$$

Підставимо третє рівняння у друге

$$M_3 = M_1 \oplus M_0 \oplus M_1 \oplus K \oplus K = M_0. \qquad (4)$$

Тепер можна підставити вирази для M_3 и M_2 у перше рівняння

$$M_4 = M_0 \oplus M_1 \oplus K \oplus M_0 \oplus K = M_1.$$

Таким чином, система небезпечна, бо $M_0 = M_3$, $M_1 = M_4$.

Задача 6. Нехай через $\overline{x}$ позначено побітове доповнення, дія якого еквівалентна застосуванню логічного заперечення до кожного біта вектора x (тобто $\overline{0} = 1$, $\overline{1} = 0$). Доведіть, що алгоритму DES притаманна властивість додатковості: якщо $C = DES_K(M)$, то $\overline{C} = DES_{\overline{K}}(\overline{M})$.

Р о з в' я з а н н я. Нагадаємо, що $\overline{x \oplus y} = \overline{x} \oplus y = x \oplus \overline{y}$ і $\overline{x} \oplus \overline{y} = x \oplus y$.

Упевнимось, що коли на вхід раунду DES подати блок даних $\overline{L}, \overline{R}$ та раундовий ключ $\overline{k}$, то шифротекст на виході раунду збігатиметься з побітовим доповненням результату шифрування в одному раунді блока L, R з ключем k. Дійсно,

- розширювальна перестановка E лише розширює правий півблок даних та змінює послідовність його бітів, тому $E(\overline{R}) = \overline{E(R)}$;
- побітове доповнення ключа k хоч і змінить його біти, але після їх покоординатного підсумовування за модулем 2 з виходом розширювальної підстановки в обох випадках результат буде однаковий;
- це спричиняє подачу на вхід S-боксів однакових вхідних векторів, тому й вихідні вектори із S-боксів збігатимуться. Аналогічний висновок матимемо й стосовно P-боксів.

Отже, $f_{DES}(\overline{R}, \overline{k}) = f_{DES}(R, k)$. А відтак, отримаємо

$$\overline{L} \oplus f_{DES}(\overline{R}, \overline{k}) = \overline{L} \oplus f_{DES}(R, k) = \overline{L \oplus f_{DES}(R, k)}.$$

Таким чином, одному раунду DES притаманна властивість додатковості, тому це буде справедливим і для всього шифру.

Задача 7. Доведіть, що властивість додатковості алгоритму DES зберігається для алгоритму 3DES.

Р о з в' я з а н н я. Зашифрування за допомогою 3DES з двома ключами виконується за схемою:

$$3DES_{K_1,K_2}(M) = DES_{K_1}(DES^{-1}_{K_2}(DES_{K_1}(M))).$$

$$3DES_{\overline{K_1},\overline{K_2}}(\overline{M}) = DES_{\overline{K_1}}(DES^{-1}_{\overline{K_2}}(DES_{\overline{K_1}}(\overline{M}))) =$$

$$= DES_{\overline{K_1}}(DES^{-1}_{\overline{K_2}}(\overline{DES_{K_1}(M)})) = DES_{\overline{K_1}}(\overline{DES^{-1}_{K_2}(DES_{K_1}(M))}) =$$

$$= \overline{3DES_{K_1,K_2}(M)}.$$

Задача 8. Одним з варіантів підвищення криптостійкості алгоритму DES є відбілювання, реалізоване в алгоритмі DESX. Крім звичайного для DES 56-бітового ключа k_1, у криптосистемі DESX використовується додатково 64-бітовий ключ k_2, а шифрування одного блока M повідомлення виконується за схемою

$$C = DES_{(k_1,k_2)}(M) = DES_{k_1}(M \oplus k_2) \oplus k_2.$$

Як у такому разі здійснити розшифрування? Яку небезпеку Ви бачите при використанні цього шифру?

Р о з в’ я з а н н я. Розшифрування у криптосистемі DESX:

$$C \oplus k_2 = DES_{k_1}(M \oplus k_2) \Rightarrow DES_{k_1}{}^{-1}(C \oplus k_2) = M \oplus k_2 \Rightarrow$$

$$M = k_2 \oplus DES_{k_1}{}^{-1}(C \oplus k_2),$$

де через $DES_{k_1}{}^{-1}$ позначено звичайне розшифрування за допомогою алгоритму DES. Хоча загальна довжина використаних ключів 120 бітів, але шифр не має стійкості, що мала б відповідати 120-бітовому ключу, бо алгоритм піддається атаці «зустріч посередині». Якщо зловмисник має декілька пар (M, C) – «відкритий текст – відповідний шифротекст», то він зможе провести повний перебір ключів, обчисливши $x = DES_{k_1}(M)$ для кожного можливого ключа k_1 і отримані пари (x, k_1) зберегти у пам’яті. Далі він для всіх ключів k_2 обчислює $C \oplus k_2$ і порівнює цю суму із значеннями, збереженими у пам’яті. У разі збігу $C \oplus k_2$ і x він встановлює потенціальну пару ключів (k_1, k_2). Загальна складність атаки – $2^{64} < 2^{120}$.

Задача 9. Припустимо, що розподіл імовірностей ключів у ключовому просторі криптосистеми є рівномірним. Оцініть відстань

єдиності криптосистеми DES за ключем, прийнявши, що надлишковість мови дорівнює $0,75$.

Р о з в' я з а н н я. Очевидно, потужність ключового простору криптоалгоритму DES складає $|K| = 2^{56}$, а використаний алфавіт $\{0,1\}$ містить два знаки, тобто $|m| = 2$. Тоді відстань єдиності алгоритму DES за ключем становить

$$L = \frac{\log_2 |K|}{D \cdot \log_2 m} = \frac{\log_2 2^{56}}{0,75 \cdot \log_2 2} = \frac{56}{0,75} \approx 75 \text{ (бітів).}$$

Задача 10. Відкритий текст складається з чотирибітових відрізків, кожен з яких містить три біти «0» та один біт «1». Для зашифрування цього тексту використовується криптоалгоритм DES. Визначте відстань єдиності шифру (у бітах), коли: а) відкритий текст зашифровується безпосередньо; б) перед зашифруванням після кожного чотирибітового відрізка вставляються випадкові чотири біти.

Р о з в' я з а н н я. а) Усього існує чотири чотирибітових відрізки, що задовольняють умові – 0001, 0010, 0100, 1000, тому надлишковість відкритого тексту $D = 1 - \frac{\log_2 4}{\log_2 2^4} = \frac{1}{2}$. Відстань єдиності шифру

$$L = \frac{\log_2 |K|}{D \cdot \log_2 m} = \frac{\log_2 2^{56}}{0,5 \cdot \log_2 2^{64}} = 1,75 \text{ блоків DES} = 112 \text{ (бітів).}$$

б) Розглядатимемо кожні вісім бітів як єдиний відрізок. Кількість таких відрізків $4 \cdot 2^4 = 2^6$. Отже, надлишковість відкритого тексту зменшиться

$$D = 1 - \frac{\log_2 2^6}{\log_2 2^8} = \frac{1}{4},$$

а відстань єдиності шифру, навпаки, збільшиться

$$L = \frac{\log_2 |K|}{D \cdot \log_2 m} = \frac{\log_2 2^{56}}{0,25 \cdot \log_2 2^{64}} = 3,5 \text{ блоків DES} = 224 \text{ (бітів).}$$

Задача 11. Абоненти мережі використовують для шифрування алгоритм DES з ключами, які для них генерує центр керування ключами. Для шифрування абонентських ключів центр також застосовує алгоритм DES і деякий майстер-ключ. Вважаючи, що кожен блок шифротексту – це один зашифрований ключ DES, оцініть відстань єдиності криптосистеми,

тобто визначте середню кількість зашифрованих кінцевих абонентських ключів DES, які потрібно отримати, щоб на їх основі визначити єдиний можливий майстер-ключ. Час розшифрування необмежений.

Р о з в я' з а н н я. У криптоалгоритмы DES довжина вхідних та вихідних блоків дорівнює 64 біти, тому при шифруванні ключів DES потужність просторів відкритих текстів і шифротекстів $|M|=|C|=2^{64}$. Довжина ключа DES також складає 64 біти, але вибір кожного восьмого біта ключа залежить від семи попередніх його бітів. Тому потужність простору ключів $|K|=2^{56}$. Крім того, коли DES-ключі абонентів є об'єктами шифрування, то надлишковість «мови» відкритих текстів буде $D=1/8$ (через біт парності). Тоді

$$L_0=\frac{\log_2|K|}{D\cdot\log_2|P|}=\frac{\log_2 2^{56}}{(1/8)\cdot\log_2 2^{64}}=\frac{56}{(1/8)\cdot 64}=7.$$

Задача 12. Спрощений шифр Фейстеля має 2 раунди шифрування та працює з 8-бітовим ключем та 16-бітовими блоками даних. Раундовий ключ K_i для i-го раунду утворюється як $K_i=K+87i \bmod 256$, де $K-$ ключ шифру у десятковій системі числення. Функція шифрування

$$f(K_i,R_{i-1})=127\cdot(K_i+R_{i-1})(\bmod 256),$$

де $R_{i-1}-$ запис у десятковій системі числення правих восьми бітів вхідного блока. Зашифруйте за допомогою такого шифру блок відкритого тексту $M=(86,83)$ з ключем $K=89$.

Р о з в' я з а н н я. Раундові ключі:

$$K_1\equiv K+87 \bmod 256\equiv 89+87 \bmod 256\equiv 176 \bmod 256;$$

$$K_2\equiv K+87\cdot 2 \bmod 256\equiv 89+87\cdot 2 \bmod 256\equiv 7 \bmod 256.$$

$$L_0\,||\,R_0=86\,||\,83.$$

Раунд 1: $f(K_1,R_0)=127\cdot(K_1+R_0)=127(176+83)\equiv 125 \bmod 256;$

$$L_0+f(K_1,R_0)=86+125=1010110\oplus 1111101=0101011=43.$$

$$L_1\,||\,R_1=83\,||\,43.$$

Раунд 2: $f(K_2,R_1)=127\cdot(K_2+R_1)=127(7+43)\equiv 206 \bmod 256;$

$$L_1 + f(K_2, R_1) = 83 + 206 = 01010011 \oplus 11001110 = 10011101 = 157.$$

$$L_2 \,||\, R_2 = 157 \,||\, 43.$$

Шифротекст $(157, 43)$.

Задача 13. 6-бітові блоки відкритого тексту шифрують за допомогою деякої SP-мережі (рис.3.3), поданої на рисунку. Щоб отримати вихідні біти із S-боксів, потрібно помножити три відповідні вхідні біти (як вектор-рядок) справа на матриці

$$S_1 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \text{ та } S_2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

(обидва S-бокси лінійні).

Дія P-боксу описується матрицею

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 3 & 1 & 4 \end{pmatrix}.$$

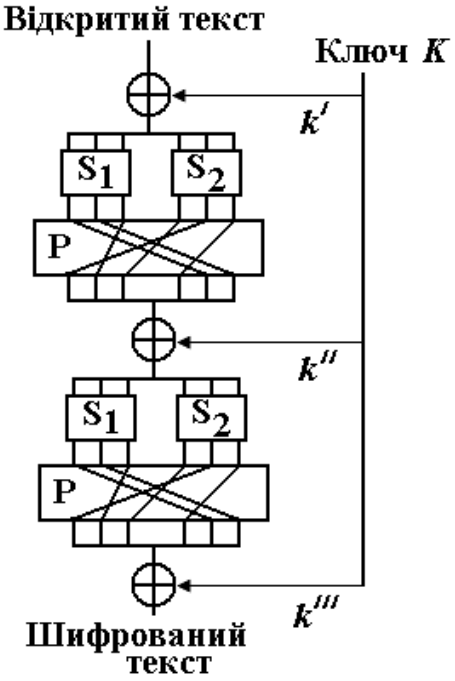


Рис. 3.3

Три раундових ключі $k' = k_1 k_3 k_5 k_2 k_4 k_6$, $k'' = k_5 k_6 k_3 k_4 k_1 k_2$ і $k''' = k_6 k_1 k_4 k_3 k_2 k_5$ утворюються з 6-бітового ключа шифру $K = k_1 k_2 k_3 k_4 k_5 k_6$. Знайдіть ключ K, при якому шифропозначенням блока $\overline{x} = 100111$ буде $\overline{y} = 010100$.

Р о з в’ я з а н н я. Оскільки за умовою обидва S-бокси лінійні, то у мережі всі криптоперетворення лінійні. Для зручності запишемо лінійні рівняння з шістьма невідомими бітами ключа K у матричній формі. Комбінуємо матриці S_1 і S_2 в одну і записуємо матрицю для P-боксу:

$$S = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}; \qquad P = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Аналогічно подамо раундові ключі як

$$k' = K \cdot K',\ k'' = K \cdot K''\ \text{і}\ k''' = K \cdot K''',$$

де

$$K' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix};\ K'' = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix};\ K''' = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Тоді

$$\overline{y} = ((\overline{x} \oplus KK')SP \oplus KK'')SP \oplus KK'''$$

або

$$\overline{y} = \overline{x}(SP)^2 \oplus KK'(SP)^2 \oplus KK''SP \oplus KK'''.$$

Звідси $\overline{y} = \overline{x}(SP)^2 \oplus K(K'(SP)^2 \oplus K''SP \oplus K''');$

$$K(K'(SP)^2 \oplus K''SP \oplus K''') = \overline{y} \oplus \overline{x}(SP)^2;$$

$$K = (\overline{y} \oplus \overline{x}(SP)^2) \cdot (K'(SP)^2 \oplus K''SP \oplus K''')^{-1}.$$

Обчислимо

$$SP = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \end{pmatrix};\quad (SP)^2 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix};$$

$$K'(SP)^2 \oplus K''SP \oplus K''' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} \oplus$$

$$\oplus\begin{pmatrix}0&0&0&0&1&0\\0&0&0&0&0&1\\0&0&1&0&0&0\\0&0&0&1&0&0\\1&0&0&0&0&0\\0&1&0&0&0&0\end{pmatrix}\begin{pmatrix}0&0&0&0&1&1\\0&0&0&0&0&1\\0&1&0&0&0&1\\1&0&1&1&0&0\\1&0&0&1&0&0\\1&0&1&0&0&0\end{pmatrix}\oplus\begin{pmatrix}0&1&0&0&0&0\\0&0&0&0&1&0\\0&0&0&1&0&0\\0&0&1&0&0&0\\0&0&0&0&0&1\\1&0&0&0&0&0\end{pmatrix}=$$

$$=\begin{pmatrix}1&1&1&0&0&0\\0&0&1&1&0&1\\1&1&1&1&0&1\\0&1&1&0&1&0\\1&0&1&0&1&1\\1&1&0&0&1&1\end{pmatrix}\bmod 2.$$

$$\left(K'(SP)^2\oplus K''SP\oplus K'''\right)^{-1}=\begin{pmatrix}1&0&0&0&1&1\\1&1&1&0&1&1\\1&1&1&0&0&0\\1&1&0&1&1&0\\0&0&0&1&1&1\\0&1&1&1&1&0\end{pmatrix}\bmod 2.$$

$$\bar{x}(SP)^2=(100111)\begin{pmatrix}0&0&0&1&0&0\\1&0&1&0&0&0\\1&0&1&0&0&1\\1&0&0&1&1&1\\1&1&0&1&1&0\\0&1&0&0&1&0\end{pmatrix}=(000111);$$

$$\bar{y}\oplus\bar{x}(SP)^2=(010100)\oplus(000111)=(010011);$$

$$K=(\bar{y}\oplus\bar{x}(SP)^2)\cdot(K'(SP)^2\oplus K''SP\oplus K''')^{-1}=$$

$$=(010011)\begin{pmatrix}1&0&0&0&1&1\\1&1&1&0&1&1\\1&1&1&0&0&0\\1&1&0&1&1&0\\0&0&0&1&1&1\\0&1&1&1&1&0\end{pmatrix}=(100010).$$

Задача 14. Оцініть, скільки часу триватиме повний перебір ключів алгоритмів DES і AES-128, якщо його виконувати за допомогою комп'ютеру з процесором з тактовою частотою 2ГГц, а перевірка одного

56-бітового ключа DES і 128-бітового ключа AES потребує виконання 100 операцій.

Р о з в' я з а н н я. Повний перебір ключів криптоалгоритму DES:

$$t = \frac{2^{56}\ \text{ключів} \cdot 100\ \text{операцій}}{60\ \text{с} \cdot 60\ \text{хв} \cdot 24\ \text{год} \cdot 365\ \text{діб} \cdot 2 \cdot 10^9\ \text{Гц}} = 114{,}2\ \text{років};$$

Повний перебір ключів криптоалгоритму AES-128:

$$t = \frac{2^{128}\ \text{ключів} \cdot 100\ \text{операцій}}{60\ \text{с} \cdot 60\ \text{хв} \cdot 24\ \text{год} \cdot 365\ \text{діб} \cdot 2 \cdot 10^9\ \text{Гц}} = 5{,}4 \cdot 10^{23}\ \text{років}.$$

Задача 15. Як відомо, внутрішні функції алгоритму AES визначені у полі $Z_2[x]/m(x)$ многочленів за модулем многочлена $m(x) = x^8 + x^4 + x^3 + x + 1$ над полем Z_2 (поле RIJNDAEL). Чи можливо замінити многочлен $m(x)$ на многочлен $x^8 + x^4 + x^3 + 1$?

Р о з в' я з а н н я. Така заміна неможлива. Для формування таблиці замін для операції SubBytes алгоритму було вибрано мультиплікативну інверсію $(x \to x^{-1})$ у полі $GF(2^8)$. Нехай $n(x) = x^8 + x^4 + x^3 + 1$. Оскільки $n(1) = 0$, то $n(x) \vdots (x+1)$, тобто многочлен $n(x)$ є звідним. Це означає, що кільце многочленів $Z_2[x]/n(x)$ не буде полем. Отже, не до всіх многочленів кільця, що ставляться у відповідність байтам змінної State, можна знайти обернений. Тому замінити многочлен $m(x) = x^8 + x^4 + x^3 + x + 1$ на $x^8 + x^4 + x^3 + 1$ неможливо.

Задача 16. Для формування таблиці замін (S-бокса) в алгоритмі AES вибрано відображення $x \to x^{-1}$ (мультиплікативна інверсія) у полі $F = Z_2[x]/x^8 + x^4 + x^3 + x + 1$. Крім того, для запобігання алгебраїчним атакам на шифр також задіяно додаткове афінне перетворення за модулем $x^8 + 1$. Тому остаточно шифропозначення $c = (c_7 c_6 c_5 c_4 c_3 c_2 c_1 c_0) \in Z_2^8$ для вхідного байта $b = (b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0) \in Z_2^8$ визначається за формулою:

$$\sigma(b) = (x^4 + x^3 + x^2 + x + 1)b^{-1}(x) + (x^6 + x^5 + x + 1) \bmod (x^8 + 1),$$

де $b(x) = b_7 x^7 + b_6 x^6 + b_5 x^5 + b_4 x^4 + b_3 x^3 + b_2 x^2 + b_1 x + b_0 \in F$;

$$\sigma(b) = c(x) = c_7x^7 + c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0 \in F.$$

Знайдіть байт c, що відповідає вхідному байту $b = (11001010)$.

Р о з в' я з а н н я. У полі $F = Z_2[x] / x^8 + x^4 + x^3 + x + 1$ байту $b = (11001010)$ відповідає многочлен $b(x) = x^7 + x^6 + x^3 + x$. На першому етапі знайдемо у цьому полі обернений многочлен $b^{-1}(x)$ до многочлена $b(x)$. За розширеним алгоритмом Евкліда маємо

$$x^6 + x^2 + 1 = (x^8 + x^4 + x^3 + x + 1) + (x + 1)(x^7 + x^6 + x^3 + x);$$

$$x^2 + 1 = (x + 1)(x^8 + x^4 + x^3 + x + 1) + x^2(x^7 + x^6 + x^3 + x);$$

$$1 = (x^5 + x^4 + x^3 + x^2 + 1)(x^8 + x^4 + x^3 + x + 1) + (x^6 + x^4 + x + 1)(x^7 + x^6 + x^3 + x).$$

Отже, $b^{-1} \equiv x^6 + x^4 + x + 1 \bmod x^8 + x^4 + x^3 + x + 1$. Далі обчислимо

$$c = \sigma(b) = (x^4 + x^3 + x^2 + x + 1)(x^6 + x^4 + x + 1) + (x^6 + x^5 + x + 1) =$$
$$= x^{10} + x^9 + x^6 + x^5 + x^4 + x \equiv x^6 + x^5 + x^4 + x^2 \bmod x^8 + x^4 + x^3 + x + 1.$$

Таким чином, $c = x^6 + x^5 + x^4 + x^2 \leftrightarrow (01110100)$.

Задача 17. При виконанні операції MixColumns в алгоритмі AES доводиться множити байти стовпця матриці станів на константи 01, $02, 03$ (у шістнадцятковій системі числення). Нехай байт зображується многочленом $b(x) = b_7x^7 + b_6x^6 ... + b_0$ над полем $Z_2[x]_{m(x)}$, $m(x) = x^8 + x^4 + x^3 + x + 1$, $b_i \in \{0,1\}$, $i = 0,...,7$. Визначте рівняння для обчислення восьми бітів добутків: а) $d(x) = 01 \cdot b(x)$; б) $d(x) = 02 \cdot b(x)$; в) $d(x) = 03 \cdot b(x)$, де $d(x) = d_7x^7 + d_6x^6 ... + d_0$.

Р о з в' я з а н н я. У полі RIJNDAEL $F = Z_2[x] / x^8 + x^4 + x^3 + x + 1$

$$01_{16} = 00000001_2 = 1;$$

$$02_{16} = 00000010_2 = x;$$

$$03_{16} = 00000011_2 = x + 1.$$

а) $d = 01 \cdot b(x) = 1 \cdot (b_7x^7 + b_6x^6 ... + b_0) = b_7x^7 + b_6x^6 ... + b_0 \Rightarrow$

$$d_0 = b_0; \quad d_1 = b_1; \quad d_7 = b_7.$$

б) $d = 02 \cdot b(x) = x \cdot (b_7 x^7 + b_6 x^6 ... + b_0) = b_7 x^8 + b_6 x^7 ... + b_0 x.$

$$x^8 \equiv x^4 + x^3 + x + 1 \bmod m(x) \Rightarrow$$

$$d = 02 \cdot b(x) = x \cdot (b_7 x^7 + b_6 x^6 ... + b_0) = b_7 (x^4 + x^3 + x + 1) + b_6 x^7 ... + b_0 x =$$

$$= b_6 x^7 + b_5 x^6 + (b_3 + b_7) x^4 + b_4 x^5 + (b_2 + b_7) x^3 + b_1 x^2 + (b_0 + b_7) x + b_7 \Rightarrow$$

$$d_7 = b_6; \quad d_6 = b_5; \quad d_5 = b_4; \quad d_4 = b_3 + b_7; \quad d_3 = b_2 + b_7;$$
$$d_2 = b_1; \quad d_1 = b_0 + b_7; \quad d_0 = b_7.$$

в) $d = 03 \cdot b(x) = (x + 1) \cdot b(x) = xb(x) + b(x).$

Використовуючи розв'язання для випадків а) і б), матимемо

$$d = (b_6 + b_7) x^7 + (b_5 + b_6) x^6 + (b_4 + b_5) x^5 + (b_3 + b_4 + b_7) x^4 +$$
$$(b_2 + b_3 + b_7) x^3 + (b_1 + b_2) x^2 + (b_0 + b_1 + b_7) x + (b_0 + b_7)$$

$$d_7 = b_6 + b_7; \quad d_6 = b_5 + b_6; \quad d_5 = b_4 + b_5; \quad d_4 = b_3 + b_4 + b_7;$$
$$d_3 = b_2 + b_3 + b_7; \quad d_2 = b_1 + b_2; \quad d_1 = b_0 + b_1 + b_7; \quad d_0 = b_0 + b_7.$$

Задача 18. Яким буде результат виконання операції MixColumns в алгоритмі AES з аргументом $2E3AF251_{16}$?

Р о з в' я з а н н я. Якщо в алгоритмі AES інтерпретувати стовпець матриці станів як многочлен третього степеня $s(x) = s_3 x^3 + s_2 x^2 + s_1 x + s_0$, де $s_3, s_2, s_1, s_0 \in GF(2^8)$, то операція MixColumns зводиться до множення цього многочлена на фіксований многочлен

$$c(x) = 03x^3 + 01x^2 + 01x + 02$$

(коефіцієнти записані у шістнадцятковій системі числення) за модулем многочлена $x^4 + 1$. Тоді

$$(2E + 3Ax + F2x^2 + 51x^3)(03x^3 + 01x^2 + 01x + 02) \bmod x^4 + 1 \equiv$$

$$\equiv((01010001)x^3+(11110010)x^2+(00111010)x+(00101110))\cdot$$
$$\cdot((00000011)x^3+(00000001)x^2+(00000001)x+(00000010))\bmod x^4+1\equiv$$
$$\equiv(1111001 1)x^6+(00001101+01010001)x^5+(01001110+11110010+$$
$$+01010001)x^4+(01110010+00111010+11110010+10100010)x^3+$$
$$+(00101110+00111010+11111111)x^2+01011010x+01011100\bmod x^4+1\equiv$$
$$\equiv11111001x^6+01011100x^5+11101101x^4+00011000x^3+11101011x^2+$$
$$+01011010x+01011100\bmod x^4+1\equiv$$
$$\equiv00011000x^3+00011000x^2+00000110x+10110001=$$
$$=18x^3+18x^2+06x+B1.$$

Задача 19. За ключовим розкладом у алгоритмі AES використовуються 8-бітові константи $C_i=2^{i-1}$, $i=1,2,...,30$ (усі розрахунки у полі $F=Z_2[x]/x^8+x^4+x^3+x+1$). Наприклад, $C_1=00000001$, $C_2=2=00000010$ і т.д. Чому дорівнюють константи C_8, C_9 та C_{16}?

Р о з в' я з а н н я. В алгоритмі AES константі $C_2=2=00000010$ ставиться у відповідність многочлен x поля Галуа $GF(2^8)=Z_2[x]/m(x)$, де $m(x)=x^8+x^4+x^3+x+1$. Тоді $C_i=2^{i-1}=x^{i-1}$, $i=1,2,...,30$. Оскільки квадрати $x^2, x^4\in Z_2[x]/m(x)$, $x^8\equiv x^4+x^3+x+1\in Z_2[x]/m(x)$, то

$$C_8=2^7=x^7=10000000_2=128_{10}=80_{16};$$
$$C_9=2^8=x^8\equiv x^4+x^3+x+1=00011011_2=27_{10}=1B_{16};$$
$$C_{16}=2^{15}=x^{15}=x^7x^8\equiv x^7(x^4+x^3+x+1)=x^{11}+x^{10}+x^8+x^7.$$

Поле $Z_2[x]/m(x)$ можна подати як векторний простір:

$$\{b_7\omega^7+b_6\omega^6+b_5\omega^5+b_4\omega^4+b_3\omega^3+b_2\omega^2+b_1\omega+b_0\},$$

де ω – корінь многочлена $f(x)=x^8+x^4+x^3+x+1$, а коефіцієнти лінійної комбінації $b_7,b_6,b_5,b_4,b_3,b_2,b_1,b_0\in\{0,1\}$. Тоді

$$\omega^8=\omega^4+\omega^3+\omega+1;$$

$$\omega^{10}=\omega^6+\omega^5+\omega^3+\omega^2;$$

$$\omega^{11}=\omega^7+\omega^6+\omega^4+\omega^3.$$

$$C_{16}=\omega^{11}+\omega^{10}+\omega^8+\omega^7=\omega^7+\omega^6+\omega^4+\omega^3+\omega^6+\omega^5+\omega^3+\omega^2+$$

$$+\omega^4+\omega^3+\omega+1+\omega^7=\omega^5+\omega^3+\omega^2+\omega+1=00101111_2=47_{10}=2F_{16}.$$

Задача 20. Нехай у скінченному полі $F=Z_2[x]/x^3+x+1$ задана функція $f:F\to F$, де $f(z)=z^{-1}$ при $z\neq 0$ і $f(0)=0$. Припустимо, що трираундовий шифр Фейстеля визначено як

$$L_i=R_{i-1};$$

$$R_i=L_{i-1}\oplus f(R_{i-1}\oplus K_i),$$

де раундові ключі $K_i=K^i$, $i=1,2,3$, ключ шифру $K\in F$, $L_i\in F$, $R_i\in F$. Як зловмиснику визначити ключ шифру за умови, що йому відома пара «відкритий текст – відповідний шифротекст», тобто відомі півблоки $L_0=100$, $R_0=001$; $L_3=110$, $R_3=100$?

Р о з в’ я з а н н я. На основі відкритого тексту та шифротексту запишемо два рівняння для визначення півблока R_1:

після першого раунду зашифрування $R_1=100\oplus f(001\oplus K)$;

після другого раунду розшифрування $R_1=L_2=100\oplus f(110\oplus K^3)$.

Отже,

$$f(001\oplus K)=f(110\oplus K^3).$$

z	z^3	$z\oplus z^3$
000	000	000
001	001	000
010	011	001
011	100	111
100	101	001
101	110	011
111	010	101

Оскільки функція $f:F\to F$ має бути бієкцією у полі $F=Z_2[x]/[x^3+x+1]$, то остання рівність може виконуватися тоді і тільки тоді, коли $001\oplus K=100\oplus K^3$, що еквівалентно умові $K\oplus K^3=111$. Далі для визначення ключа шифру обчислимо значення $z\oplus z^3$ для всіх

$z \in F$. Наприклад, трійці бітів $z = 101$ у полі F відповідає многочлен $x^2 + 1$. Тоді

$$z^3 \equiv (x^2+1)^3 \bmod(x^3+x+1) =$$

$$= x^6+x^4+x^2+1 \bmod(x^3+x+1) \equiv x^2+x \leftrightarrow 110;$$

$$z^3 + z = 110 \oplus 101 = 011.$$

Аналіз цих даних свідчить, що рівнянню $K \oplus K^3 = 111$ задовольняє ключ $K = 011$.

Задача 21. Відкритий текст P з блоків $P_1, P_2, ..., P_n$ шифрують у режимі CBC за допомогою шифру AES. При передачі шифрованих даних шифрований блок C_j було передано з помилкою. Скільки блоків будуть розшифровані на приймальній стороні неправильно?

Р о з в' я з а н н я. У режимі CBC $C_{j+1} = E_K(C_j \oplus P_{j+1})$ – правило зашифрування, $P_{j+1} = D_K(C_{j+1}) \oplus C_j$ – правило розшифрування. Якщо помилка виявлена у шифрованому блоці C_j, то тільки розшифровані блоки P_j та P_{j+1} міститимуть помилку.

Задача 22. Припустимо, що атомний завод передає на станцію моніторингу 2^{35} шифротекстів, отриманих за допомогою симетричного шифру. Усі відкриті тексти являють собою дані про вимірювання напруги (ВИСОКЕ чи НИЗЬКЕ) і кодуються двома символами 0 та 1. Проаналізуйте можливі загрози, міру їх впливу на безпеку, якщо для шифрування використано: а) алгоритм DES в режимі CBC; б) алгоритм 2DES в режимі CBC; в) алгоритм AES в режимі ECB.

Р о з в' я з а н н я. Нехай M_1, $M_2, ..., M_s$ – повідомлення, яким відповідають зашифровані тексти C_1, $C_2, ..., C_s$, $s = 2^{35}$. Припустимо, що зловмиснику відомі не тільки зашифровані тексти C_1, $C_2, ..., C_s$, а й що, він отримав кілька відкритих текстів. Наприклад, він знає текст M_1.

а) <u>алгоритм DES в режимі CBC</u>: ключ можна встановити методом повного перебору за допомогою спеціальних машин для пошуку ключів DES. Для проведення диференціального або лінійного криптоаналізу кількість перехоплених текстів занадто мала. Атака на основі парадоксу днів народження стає загрозливою, якщо кількість шифротекстів досягає $2^{n/2}$, де n – довжина блоку. Для алгоритму DES $2^{64/2} = 2^{32} < 2^{35}$, що

менше, ніж 2^{56} у разі повного перебору ключів. Колізія векторів ініціалізації може виявити деякі однакові тексти.

б) 2DES в режимі CBC: завдяки довжині ключа (112 бітів) метод повного перебору ключів не слід вважати загрозою. Атака «зустріч посередині» хоча й потребує 2^{57} шифрувань, але непрактична через високі вимоги до комп'ютерної пам'яті. Реальна загроза – атака на основі парадоксу днів народження, бо довжина блоку 2DES складає тільки 64 біти і при $s = 2^{35} > 2^{32}$ схема не є небезпечною.

в) AES в режимі ECB: велика довжина ключа робить марним спроби проведення повного перебору ключів. Але за умови існування тільки двох типів відкритих текстів режим занадто небезпечний. Дійсно, знаючи M_1, зловмисник може знайти $M_2,...,M_s$ за допомогою такої простої процедури: для кожного i перевірити рівність $C_i = C_1$. Якщо вона правильна, то $M_i = M_1$, інакше $M_i \neq M_1$.

Задача 23. Два користувача **A** і **B** для шифрування застосовують блоковий шифр в одному з двох режимів:

- CBC: $M_1, M_2, ..., M_n \to C_0, C_1, C_2, ..., C_n$,

$$C_i = E_K(M_i \oplus C_{i-1}),\ i > 0,\ C_0 = IV;$$

- CTR: $M_1, M_2, ..., M_n \to C_1, C_2, ..., C_n$,

$$K_i = E_K(IV \,||\, i), \quad C_i = M_i \oplus K_i$$

Припустивши, що зловмисник може перехопити та змінити шифротексти в обох режимах, проаналізуйте безпеку шифрування для двох наступних сценаріїв:

а) останній блок повідомлення, відправленого користувачем **B**, містить випадково згенерований секретний ключ. Зловмисник намагається пошкодити повідомлення так, щоб для користувача **A** при розшифруванні воно виглядало, як незмінене, але містило фальшивий ключ.

б) зловмисник знає перший блок M_1 повідомлень і в змозі замінити його іншим блоком A_1 за своїм вибором.

Р о з в' я з а н н я. а) В обох режимах зловмисник може замінити останній блок зашифрованого тексту на будь-який інший. Коли на приймальній стороні розшифрують повідомлення, то всі попередні блоки не зміняться, а останній блок буде пошкоджений. Але оскільки він є випадковим, то не існує способу виявити заміну;

б) У режимі CTR: $C_1 = M_1 \oplus E_K(IV \| 1)$, звідки $E_K(IV \| 1) = M_1 \oplus C_1$. Якщо зловмисник хоче замінити C_1 на $C_1' = A_1 \oplus E_K(IV \| 1)$, то C_1' він знайде як $C_1' = A_1 \oplus M_1 \oplus C_1$. На решту блоків цей процес не вплине. У режимі CBC $M_1 = D_K(C_1) \oplus C_0$ і зловмисник не зможе непомітно змінити C_1, бо це вплине на розшифрування блока C_2. Але він може намагатися знайти блок шифротексту $C_0' = A_1 \oplus D_K(C_1) = A_1 \oplus M_1 \oplus C_0$. Тоді $A_1 = D_K(C_1) \oplus C_0'$. Отже, в обох режимах знання першого блока зловмисником – небезпечне.

Задача 24. Рядок бітів розбито на трибітові блоки і зашифровано за допомогою прямого P-боксу. Позиції, в які переставляються біти блока, визначені перестановкою $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Розшифруйте текст 101010101010 у режимах: а) ECB; б) CBC; в) OFB. Вектор ініціалізації – 000, для режиму OFB $r = 2$.

Р о з в’ я з а н н я. Розіб’ємо текст на чотири трибітових блоки

101 010 101 010.

Ключ розшифрування $\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.

а) У режимі ECB кожен блок C_i шифротексту розшифровуємо окремо і незалежно від інших: $M_i = \pi^{-1}(C_i)$, $i = 1,2,3,4$.

$$M_1 = \pi^{-1}(101) = 011; \qquad M_2 = \pi^{-1}(010) = 100;$$

$$M_3 = \pi^{-1}(101) = 011; \qquad M_4 = \pi^{-1}(010) = 100.$$

У результаті отримаємо 011100011100.

б) Кожний блок шифротексту перед розшифруванням у режимі CBC додамо за $\mathrm{mod}\,2$ до попереднього блока шифротексту: $M_i = \pi^{-1}(C_i) \oplus C_{i-1}$, $i = 4,3,2,1$; $C_0 = IV = 000$ – вектор ініціалізації. Починаємо з четвертого блока:

$$M_4 = \pi^{-1}(C_4) \oplus C_3 = \pi^{-1}(010) \oplus 101 = 100 \oplus 101 = 001;$$

$$M_3 = \pi^{-1}(C_3) \oplus C_2 = \pi^{-1}(101) \oplus 010 = 011 \oplus 010 = 001;$$

$$M_2 = \pi^{-1}(C_2) \oplus C_1 = \pi^{-1}(010) \oplus 101 = 100 \oplus 101 = 001;$$

$$M_1 = \pi^{-1}(C_1) \oplus C_0 = \pi^{-1}(101) \oplus 000 = 011 \oplus 000 = 011.$$

Остаточно розшифрований текст виглядає 011001001001.

в) Тепер розіб'ємо текст на шість двобітових блоків

10 10 10 10 10 10.

Приймемо такі позначення: C_0 – крайні праві r бітів вектора ініціалізації; $S_r(X)$ – операція відбору крайніх лівих r бітів вектора X, $||$– символ конкатенації. У момент часу i ми вважаємо, що l_{i-1}– це крайні $(n-r)$ лівих бітів регістра перед розшифруванням блока C_i (рис. 3.4). Тоді процедура розшифрування зводиться до обчислення

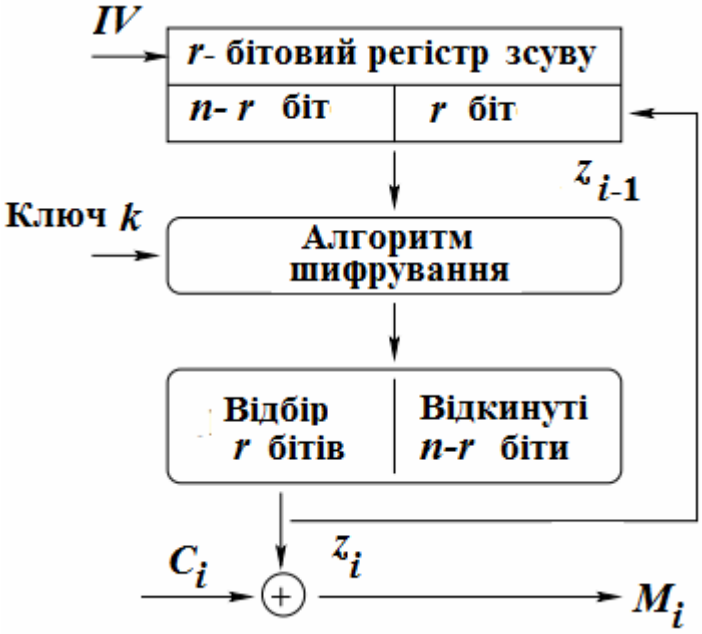


Рис. 3.4

$$M_i = C_i \oplus S_r[\pi(l_{i-1} || z_{i-1})], \quad i \geq 1.$$

За умовою задачі

- при $i = 1 \quad l_0 || z_0 = IV$;

$$M_1 = C_1 \oplus S_2[\pi(l_0 || z_0)] = 10 \oplus S_2[\pi(000)] = 10 \oplus 00 = 10;$$

- при $i = 2 \quad l_1 || z_1 = 0 || 00 = 000$;

$$M_2 = C_2 \oplus S_2[\pi(l_1 || z_1)] = 10 \oplus S_2[000] = 10 \oplus 00 = 10;$$

і т.д. Остаточно дістанемо 101010101010.

Задача 25. Який псевдовипадковий потік даних генерується при використанні 64-бітового OFB режиму, якщо застосувати алгоритм DES із слабким ключем?

Р о з в' я з а н н я. При використанні алгоритму DES у 64-бітовому OFB режимі генерується послідовність

$$E_{DES}(IV),\ E_{DES}(E_{DES}(IV)),\ E_{DES}(E_{DES}(E_{DES}(IV))),...$$

При шифруванні на слабкому ключі K маємо $E_{DES_K}(X) = D_{DES_K}(X)$, звідки $E_{DES_K}(E_{DES_K}(X)) = X$. Отже, результатом за шифрування на слабкому ключі DES у 64-бітному OFB режимі буде послідовність:

$$E_{DES}(IV),\ IV,\ E_{DES}(IV),\ IV,...$$

Задача 26. Нехай банківською мережею пересилається повідомлення $m = M_1M_2M_3$, де $M_1 =$fromAccount, $M_2 =$ toAccount, $M_3 =$amount, згідно з якими певна кількість доларів (amount) має бути переведена з першого рахунку (fromAccount) на другий (toAccount). Зашифрування повідомлень проводять за допомогою алгоритму AES у режимі CTR, тобто $K_i = E_K(IV \| i)$, $C_i = M_i \oplus K_i$. Кожна з трьох частин повідомлення містить по 16 символів (один блок). Нехай зловмисник має рахунок у банку і може перехоплювати та змінювати повідомлення. Якщо йому відомий зміст частини toAccount конкретного шифрованого тексту $C_1C_2C_3$, то яким чином він може змінити шифротекст, щоб зашифрована кількість доларів (amount) потрапила на його рахунок? Чи можна за допомогою MAC- коду запобігти цим діям?

Р о з в' я з а н н я. Нехай рахунку нападника відповідає блок M_2'. Щоб перевести гроші на свій рахунок, він має замінити шифрований блок C_2 на $C_2' = C_2 \oplus M_2 \oplus M_2' = (M_2 \oplus K_2 \oplus M_2 \oplus M_2') = K_2 \oplus M_2'$, оскільки при розшифруванні повідомлення $C_1C_2'C_3$ гроші мають бути переведені на $M_2' =$ toAccount.

Повідомлення можна автентифікувати, приєднавши $MAC_{K_M}(M_1M_2M_3)$ після повідомлення до зашифрування. Якщо отримувач перевірить MAC- код перед прийняттям повідомлення, то атака буде розкрита.

Задача 27. Перетворення $F : (L_{i-1}; R_{i-1}) \to (L_i; R_i)$ i-го раунду шифру Фейстеля виглядає як:

$$\begin{cases} L_i = R_{i-1}; \\ R_i = L_{i-1} \oplus f(R_{i-1} \oplus k_i), \end{cases}$$

де k_i – ключ i-го раунду, f – раундова функція. Нехай $X = (L_0, R_0)$ і $X' = (L_0', R_0')$ – два відкритих тексти, зв'язані умовою $a = R_0 \oplus R_0'$. Довести, що коли $L_2 = L_2'$, то $R_2 = R_2' \oplus a$, де $(L_2; R_2) = F(F(L_0; R_0))$ і $(L_2'; R_2') = F(F(L_0'; R_0'))$– відповідні шифротексти після двох раундів зашифрування (ключ шифру обидва рази однаковий).

Р о з в' я з а н н я. Одна з властивостей шифру Фейстеля – можливість використати для процедури розшифрування ту саму раундову функцію, що була задіяна при зашифруванні.

Зашифрування:	Розшифрування:
$R_i = L_{i-1} \oplus f(R_{i-1} \oplus k_i);$	$L_{i-1} = R_i \oplus f(L_i \oplus k_i);$
$L_i = R_{i-1}$	$R_{i-1} = L_i.$

Отже, з одного боку, зашифрування відкритих текстів $X = (L_0, R_0)$ і $X' = (L_0', R_0')$ дає:

$$L_1 = R_0; \qquad R_1 = L_0 \oplus f(R_0 \oplus k_1);$$

$$L_1' = R_0'; \qquad R_1' = L_0' \oplus f(R_0' \oplus k_1).$$

А з іншого боку, після першого раунду розшифрування шифротекстів $(L_2; R_2)$ і $(L_2'; R_2')$ дістанемо результат

$$R_1 = L_2; \qquad L_1 = R_2 \oplus f(L_2 \oplus k_2);$$

$$R_1' = L_2'; \qquad L_1' = R_2' \oplus f(L_2' \oplus k_2).$$

Тоді $R_0 = L_1 \Rightarrow R_0 = f(L_2 \oplus k_2) \oplus R_2;$

$$R_0' = L_1' \Rightarrow R_0' = f(L_2' \oplus k_2) \oplus R_2'.$$

Почленно додаємо ці рівняння

$$R_0 \oplus R_0' = f(L_2 \oplus k_2) \oplus R_2 \oplus f(L_2' \oplus k_2) \oplus R_2'$$

За умовою $L_2 = L_2'$, тому $f(L_2 \oplus k_2) = f(L_2' \oplus k_2)$, а тоді

$$R_0 \oplus R_0' = R_2 \oplus R_2' \Rightarrow a = R_2 \oplus R_2' \Rightarrow R_2' = R_2 \oplus a.$$

Задача 28. Визначте диференціальний профіль S-боксу

x	00	01	10	11
y	01	10	11	00

.

Р о з в’ я з а н н я. Для зручності перепишемо таблицю замін S-боксу, перевівши входи x і виходи $y = S(x)$ у десяткову систему числення:

x	0	1	2	3
y	1	2	3	0

Для кожної пари входів і виходів відповідно обчислимо побітові різниці $\Delta A = x \oplus x^*$ і $\Delta C = y \oplus y^*$ (табл. 3.1 і 3.2).

Таблиця 3.1

$\Delta A = x \oplus x^*$

x \ x^*	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Таблиця 3.2

$\Delta C = y \oplus y^*$

	x^*	0	1	2	3
x	y \ y^*	**1**	**2**	**3**	**0**
0	**1**	0	3	2	1
1	**2**	3	0	1	2
2	**3**	2	1	0	3
3	**0**	1	2	3	0

Будемо вважати, що четвірка (x, x^*, y, y^*) належіть множині $S_{\Delta C}^{\Delta A}$, якщо

$$\begin{cases} \text{різниця } \Delta A \text{ стоїть у клітині з номерами } x, x^* \text{ у табл. 3.1;} \\ \text{різниця } \Delta C \text{ стоїть у клітині з номерами } y, y^* \text{ у табл. 3.2.} \end{cases}$$

Наша задача – обчислити потужність усіх можливих множин $S_{\Delta C}^{\Delta A}$, тобто знайти, скільки разів у S-боксі одне й те саме значення ΔA відповідає тій же різниці ΔC. Наприклад, щоб знайти потужність множини S_3^1, ми підраховуємо усі четвірки (x, x^*, y, y^*), для яких

$$\begin{cases} 1 \text{ стоїть у клітині з номерами } x, x^* \text{ табл. 3.1;} \\ 3 \text{ стоїть у клітині з номерами } y, y^* \text{ табл. 3.2.} \end{cases}$$

Як видно з табл. 3.1 і 3.2,

$S_1^1 = \{(0,1,1,2), (1,0,2,1), (2,3,3,0), (3,2,0,3)\};$

$S_0^0 = \{(0,0,1,1), (1,1,2,2), (2,2,3,3), (3,3,0,0)\};$

$S_2^2 = \{(0,2,1,3), (1,3,2,0), (2,0,3,1), (3,1,0,2)\};$

$S_3^3 = \{(0,3,1,0), (1,2,2,3), (2,1,3,2), (3,0,0,1)\}$.

Увесь диференціальний профіль S-боксу представлено у табл. 3.3.

Таблиця 3.3

Залежність ΔC від ΔA у S-боксі

ΔA \ ΔC	**0**	**1**	**2**	**3**
0	4	0	0	0
1	0	0	0	4
2	0	0	4	0
3	0	4	0	0

Задача 29. Шифр складається з одного S-боксу з таблицею замін

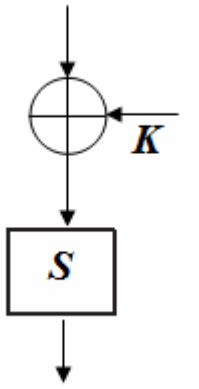


Рис. 3.5

x	000	001	010	011	100	101	110	111
y	000	110	011	100	101	001	111	010

Усі відкриті дані перед входом до S-боксу підсумовуваються за $\mathrm{mod}\,2$ з невідомим трибітовим ключем k (рис. 3.5). Побудуйте диференціальний профіль S-бокса та визначте ключ шифру, якщо двом входам $m_1 = 010$ і $m_2 = 100$ відповідає диференціальна різниця виходів $\Delta C = 100$, а двом входам $m_3 = 001$ і $m_4 = 100$ – диференціальна різниця виходів $\Delta C = 011$.

Р о з в’ я з а н н я. Для зручності перепишемо таблицю замін даного S-боксу компактніше:

x	0	1	2	3	4	5	6	7
y	0	6	3	4	5	1	7	2

Профіль S-бокса означимо так само, як і у задачі 28, спочатку обчисливши для кожної пари входів і виходів різниці $\Delta A = x \oplus x^*$ і $\Delta C = y \oplus y^*$ (табл. 3.4 і 3.5).

Таблиця 3.4

$$\Delta A = x \oplus x^*$$

x \ x^*	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1
7	7	6	5	1	3	2	1	0

Таблиця 3.5

$$\Delta C = y \oplus y^*$$

	x^*	0	1	2	3	4	5	6	7
x	y \ y^*	**0**	**6**	**3**	**4**	**5**	**1**	**7**	**2**
0	**0**	0	6	3	4	5	1	7	2
1	**6**	6	0	5	2	3	7	1	4
2	**3**	3	5	0	7	6	2	4	1
3	**4**	4	2	7	0	1	5	3	6
4	**5**	5	3	6	1	0	4	2	7
5	**1**	1	7	2	5	4	0	6	3
6	**7**	7	1	4	3	2	6	0	5
7	**2**	2	4	1	6	7	3	5	0

Тепер підрахуємо кількість усіх четвірок (x, x^*, y, y^*), що входять до множини $S_{\Delta C}^{\Delta A}$, де $\Delta A = x_1 \oplus x_2$, $\Delta C = y_1{}^* \oplus y_2{}^*$. Наприклад, до множини S_4^3 входять лише дві четвірки $(3,0,4,0)$ і $(0,3,0,4)$, тоді як множина S_3^1 виявляється порожньою. Остаточні підрахунки щодо диференціального профіля S-боксу зведені у табл. 3.6.

Таблиця 3.6

Залежність ΔC від ΔA для S-боксу

ΔA \ ΔC	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	8	0	0	0	0	0	0	0
1	0	0	0	0	2	2	2	2
2	0	0	4	4	0	0	0	0
3	0	0	0	0	2	2	2	2
4	0	0	0	0	2	2	2	2
5	0	4	0	4	0	0	0	0
6	0	0	0	0	2	2	2	2
7	0	4	4	0	0	0	0	0

Перейдемо до визначення ключа. При зашифруванні відкритих повідомлень $m_1 = 010 = 2$ і $m_2 = 100 = 4$ на вхід S-бокса потрапляють відповідно входи $m_1 \oplus k = 2 + k$ і $m_2 \oplus k = 4 + k$. У цьому випадку диференціальна різниця складає

$$\Delta A = m_1 \oplus k \oplus m_2 \oplus k = m_1 \oplus m_2 = 2 + 4 = 6.$$

За умовою різниця $\Delta C = S(m_1 \oplus k) \oplus S(m_2 \oplus k) = 100 = 4$.

Отже, четвірка $(m_1 \oplus k,\ m_2 \oplus k,\ S(m_1 \oplus k),\ S(m_2 \oplus k)) \in S_4^6$.

Множина S_4^6 складається з четвірок (x, x^*, y, y^*), де

$$x \oplus x^* = 6;\ y \oplus y^* = S(x) \oplus S(x^*) = 6.$$

Ці четвірки можна подати у вигляді

$$(x, x \oplus 6, S(x), S(x+6)), \quad \text{де } S(x) \oplus S(x+6) = 4.$$

При цьому треба мати на увазі, що множина S_4^6 є підмножиною множини S^6, складеної з четвірок $(x, x+6, S(x), S(x+6))$, наведених у табл. 3.7 .

Таблиця 3.7

Множина S^6

x	$x \oplus 6$	$S(x)$	$S(x \oplus 6)$	ΔC
0	6	0	7	7
1	7	6	2	4
2	4	3	5	6
3	5	4	1	5
4	2	5	3	6
5	3	1	4	5
6	0	7	0	7
7	1	2	6	4

Із табл. 3.7 безпосередньо видно, що $\Delta C = S(x) \oplus S(x \oplus 6) = 4$ для четвірок $(1,7,6,2)$ і $(7,1,2,6)$. Отже, потрібно розглянути два варіанти:

$$\begin{cases} m_1 \oplus k = 1, \\ (m_1 \oplus k) + 6 = 7 \end{cases} \quad \text{або} \quad \begin{cases} m_1 \oplus k = 7, \\ (m_1 \oplus k) + 6 = 1. \end{cases}$$

Оскільки $\Delta A = m_1 \oplus m_2 = 6$, то $m_1 \oplus 6 = m_2$. А тоді

$$\begin{cases} m_1 \oplus k = 1, \\ m_2 \oplus k = 7 \end{cases} \quad \text{або} \quad \begin{cases} m_1 \oplus k = 7, \\ m_2 \oplus k = 1. \end{cases}$$

За умовою $m_1 = 010 = 2$ і $m_2 = 100 = 4$, то

$$\begin{cases} k = 1 + 2 = 3, \\ k = 7 + 4 = 3 \end{cases} \quad \text{або} \quad \begin{cases} k = 7 + 2 = 5, \\ k = 1 + 4 = 5. \end{cases}$$

Таким чином, можливі значення ключа зашифрування $k = 3$ або $k = 5$.

Для подальшого уточнення ключа використовуємо другу пару відкритих текстів $m_3 = 001 = 1$ і $m_4 = 100 = 4$. На вхід S-бокса відповідно подаватимуться $m_3 \oplus k$ і $m_4 \oplus k$, при цьому

$$\Delta A = m_3 \oplus k \oplus m_4 \oplus k = m_3 \oplus m_4 = 1 + 4 = 5.$$

Цим відкритим текстам відповідає диференціальна різниця виходів $\Delta C = 011$, тому четвірка

$$(m_3 \oplus k,\ m_4 \oplus k,\ S(m_3 \oplus k),\ S(m_4 \oplus k)) \in S_3^5.$$

Елементи множини S_3^5 – це четвірки (x, x^*, y, y^*), для яких

$$x \oplus x^* = 5;\ y \oplus y^* = S(x) \oplus S(x^*) = 3.$$

Скориставшись умовою $x^* = x \oplus 5$, їх можна подати у вигляді $(x,\ x+5,\ S(x),\ S(x+5))$ з умовою $S(x_1) \oplus S(x_1+5) = 3$.

Очевидно, множина S^5, складена з четвірок $(x_1, x_1+5, S(x_1), S(x_1+5))$, містить підмножину S_3^5. Усі елементи четвірок множини S^5 перераховані у табл. 3.8.

Таблиця 3.8

Множина S^5

x	$x+5$	$S(x)$	$S(x+5)$	ΔC
0	5	0	1	1
1	4	6	5	3
2	7	3	2	1
3	6	4	7	3
4	1	5	6	3
5	0	1	0	1
6	3	7	4	3
7	2	2	3	1

З таблиці випливає, що $\Delta C = S(x) \oplus S(x+5) = 3$ для четвірок $(1,4,6,5)$, $(3,6,4,7)$, $(4,1,5,6)$ і $(6,3,7,4)$. Тоді важливий зв'язок між відкритими текстами і ключем може виражатися у вигляді умов:

$$\begin{cases} m_3 \oplus k = 1, \\ (m_3 \oplus k) + 5 = 4, \end{cases} \quad \text{або} \quad \begin{cases} m_3 \oplus k = 3, \\ (m_3 \oplus k) + 5 = 6, \end{cases} \quad \text{або}$$

$$\begin{cases} m_3 \oplus k = 4, \\ (m_3 \oplus k) + 5 = 1, \end{cases} \quad \text{або} \quad \begin{cases} m_3 \oplus k = 6, \\ (m_3 \oplus k) + 5 = 3. \end{cases}$$

Нагадаємо, що $\Delta A = m_3 \oplus m_4 = 5$ і $m_4 = m_3 \oplus 5$. Тому далі

$$\begin{cases} m_3 \oplus k = 1, \\ m_4 + k = 4, \end{cases} \quad \text{або} \quad \begin{cases} m_3 \oplus k = 3, \\ m_4 + 5 = 6, \end{cases} \quad \text{або}$$

$$\begin{cases} m_3 \oplus k = 4, \\ m_4 + 5 = 1, \end{cases} \quad \text{або} \quad \begin{cases} m_3 \oplus k = 6, \\ m_4 \oplus k = 3. \end{cases}$$

За відомими значеннями відкритих текстів знаходимо, що ключ k шифру може набувати значень $0, 2, 5, 7$. Об'єднавши ці результати аналізу з попередніми висновками про ключ, встановлюємо ключ за допомогою операції перетину множин

$$k = \{3,5\} \cap \{0,2,5,7\} = 5,$$

тобто секретний ключ $k = 5$. Експериментально можна перевірити, що при шифруванні даних пар відкритих текстів застосовувався саме цей ключ.

Задача 30. За шифрувальною процедурою деякого блокового трираундового алгоритму вхідний 9-бітовий блок даних розбивають на три підблоки, кожен з яких подають у S-бокс (табл. 3.9), однаковий для всіх раундів. Після заміни отримані біти зазнають перестановки $P = (1,4,7,2,5,8,3,6,9)$. Основна функція у кожному раунді – додавання бітів піключа раунду і відкритого тексту за модулем 2 (підключ у раундах однаковий і збігається з ключем шифру K). У третьому раунді замість перестановки додаткове підсумовування з підключем. Табл. 3.10 демонструє залежність вихідної різниці ΔC із S-боксу від його вхідної різниці ΔA (диференціальний профіль), а табл. 3.11 – пари відкритих текстів із різницею $\Delta x = 110000000$ та відповідні їм шифровані тексти y і y^*.

Таблиця 3.9

Заміна в S-боксі

Вхід	000	001	010	011	100	101	110	111
Вихід	111	000	110	101	010	001	011	100

Таблиця 3.10

Залежність ΔC від ΔA в S-боксі

ΔA \ ΔC	000	001	010	011	100	101	110	111
000	8	0	0	0	0	0	0	0
001	0	0	0	4	0	0	0	4
010	0	4	0	0	0	4	0	0
011	0	0	4	0	0	0	4	0
100	0	4	0	0	0	4	0	0
101	0	0	4	0	0	0	4	0
110	0	0	0	0	8	0	0	0

Таблиця 3.11

Вибрані тексти та результати шифрування

Пара	x	x^*	y	y^*
1	100111010	010111010	111011110	110011011
2	011101110	101101110	011000100	010000101
3	000101111	110101111	101111111	101111010
4	101111111	011111111	000111000	000111001
5	100110100	010110100	111010101	111010100

За допомогою диференціального криптоаналізу визначте три можливі перші біти ключа.

Р о з в’ я з а н н я. Для першої пари текстів $\Delta C = 111011110 \oplus 110011011 = 0010000101 \Rightarrow$ ненульова різниця буде на виходах боксів S_{31} та S_{33}. На їх вхід подається вхідна різниця 100, яка може бути утворена 8 способами:

1. $000 \oplus 100$;
2. $001 \oplus 101$;
3. $010 \oplus 110$;
4. $011 \oplus 111$;
5. $100 \oplus 000$;
6. $101 \oplus 001$;
7. $110 \oplus 010$;
8. $111 \oplus 011$.

Визначаємо відповідні пари виходів за табл. 3.9.

1. $111 \oplus 010 = 101$;
2. $000 \oplus 001 = 001$;
3. $110 \oplus 011 = 101$;
4. $101 \oplus 100 = 001$;
5. $010 \oplus 111 = 101$;
6. $001 \oplus 000 = 001$;
7. $011 \oplus 110 = 101$;
8. $100 \oplus 101 = 001$.

Оскільки на виході боксу S_{31} є різниця 001, то її можна отримати у випадках, що підкреслені. До виходу боксу S_{31} додаються перші три біти ключа K (їх позначимо K_1). Тому

$$000 \oplus K_1 = 111 \qquad 100 \oplus K_1 = 111$$
$$001 \oplus K_1 = 110 \qquad 101 \oplus K_1 = 110$$
$$001 \oplus K_1 = 111 \qquad 101 \oplus K_1 = 111$$
$$000 \oplus K_1 = 110 \qquad 100 \oplus K_1 = 110$$

$\Rightarrow K_1$ може приймати одне з значень 111 або 110 або 011 або 010.

Задача 31. Розглянувши четвертий рядок четвертого S-боксу криптоалгоритму DES

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

як бульову функцію від вхідних бітів $x_1x_2x_3x_4 \to y_1y_2y_3y_4$ (безключовий блок заміни), знайдіть вихідний біт y_i для якого ефективність лінійного статистичного аналогу $x_1 \oplus x_2 \oplus x_3 \oplus y_i$ буде найбільшою.

Р о з в' я з а н н я. Для кожного значення вихідних бітів y_i обчислимо кількість n_i можливих варіантів, при яких сума $x_1 \oplus x_2 \oplus x_3$ бітів дорівнюватиме значенню y_i (бо у такому разі $x_1 \oplus x_2 \oplus x_3 \oplus y_i = 0$). Усі розрахунки зібрані у табл. 3.12. Там же в останньому рядку наведено значення відхилення $\varepsilon_i = \left| \frac{n_i}{16} - \frac{1}{2} \right|$.

Таблиця 3.12

Проміжні розрахунки та відхилення ε_i

$x_1\, x_2\, x_3\, x_4$	S	y_1	y_2	y_3	y_4	$x_1 \oplus x_2 \oplus x_3$
$0000_2 = 0_{10}$	3	0	0	1	1	0
$0001_2 = 1_{10}$	15	1	1	1	1	0
$0010_2 = 2_{10}$	0	0	0	0	0	1
$0011_2 = 3_{10}$	6	0	1	1	0	1
$0100_2 = 4_{10}$	10	1	0	1	0	1
$0101_2 = 5_{10}$	1	0	0	0	1	1
$0110_2 = 6_{10}$	13	1	1	0	1	0
$0111_2 = 7_{10}$	8	1	0	0	0	0
$1000_2 = 8_{10}$	9	1	0	0	1	1
$1001_2 = 9_{10}$	4	0	1	0	0	1
$1010_2 = 10_{10}$	5	0	1	0	1	0
$1011_2 = 11_{10}$	11	1	0	1	1	0
$1100_2 = 12_{10}$	12	1	1	0	0	0
$1101_2 = 13_{10}$	7	0	1	1	1	0
$1110_2 = 14_{10}$	2	0	0	1	0	1
$1111_2 = 15_{10}$	14	1	1	1	0	1

n_i	6	6	8	4	
$\varepsilon_i = \left\| \frac{n_i}{16} - \frac{1}{2} \right\|$	$\frac{1}{8}$	$\frac{1}{8}$	0	$\frac{1}{4}$	

Отже, найбільше відхилення досягається для вихідного біта y_4.

Задача 32. Три біти $x_1x_2x_3$ подані на вхід S-боксу стискання, на виході перетворюються на два біти y_1y_2 згідно з правилами

$$y_1 = x_1x_2 \oplus x_3 \bmod 2,$$

$$y_2 = x_1x_3 \oplus x_2 \bmod 2.$$

Знайдіть вихідний біт y_i, для якого $x_1 \oplus x_2 \oplus y_i$ відрізняється від нуля.

Р о з в' я з а н н я. Для можливих значень вихідних бітів y_1 і y_2 визначаємо кількість n_i випадків, коли сума бітів $x_1 \oplus x_2$ дорівнюватиме значенню y_i і далі обчислюємо відхилення $\varepsilon_i = \left|\frac{n_i}{8} - \frac{1}{2}\right|$ (табл. 3.13).

Таблиця 3.13

Проміжні розрахунки та відхилення ε_i

$x_1\ x_2\ x_3$	y_1	y_2	$x_1 \oplus x_2$
000	0	0	0
001	1	0	0
010	0	1	1
011	1	1	1
100	0	0	1
101	1	1	1
110	1	1	0
111	0	0	0
n_i	4	6	
$\varepsilon_i = \left\|\frac{n_i}{8} - \frac{1}{2}\right\|$	0	$\frac{1}{4}$	

Ненульове відхилення має вихідний біт y_2.

Задача 33. Побудуйте лінійний профіль S-боксу, наведеного у задачі 29.

Р о з в' я з а н н я. Спочатку побудуємо таблицю істинності, що виражатиме відповідність між усіма можливими вхідними бітами b_2, b_1, b_0 у S-бокс, їх лінійними комбінаціями

$$b_0 \oplus b_1,\ b_0 \oplus b_2,\ b_1 \oplus b_2,\ b_0 \oplus b_1 \oplus b_2$$

та вихідним бітами $b_2{*}, b_1{*}, b_0{*}$ і комбінаціями

$$b_0{*} \oplus b_1{*},\ b_0{*} \oplus b_2{*},\ b_1{*} \oplus b_2{*},\ b_0{*} \oplus b_1{*} \oplus b_2{*}$$ (табл. 3.14).

Таблиця 3.14

Таблиця істинності

Вхід у S-бокс							Вихід із S-бокса						
b_2	b_1	b_0	$b_0 \oplus b_1$	$b_0 \oplus b_2$	$b_1 \oplus b_2$	$b_0 \oplus b_1 \oplus b_2$	b_2^*	b_1^*	b_0^*	$b_0^* \oplus b_1^*$	$b_0^* \oplus b_2^*$	$b_1^* \oplus b_2^*$	$b_0^* \oplus b_1^* \oplus b_2^*$
0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	1	1	0	1	1	1	0	1	1	0	0
0	1	0	1	0	1	1	0	1	1	0	1	1	0
0	1	1	0	1	1	0	1	0	0	0	1	1	1
1	0	0	0	1	1	1	1	0	1	1	0	1	0
1	0	1	1	0	1	0	0	0	1	1	1	0	1
1	1	0	1	1	0	0	1	1	1	0	0	0	1
1	1	1	0	0	0	1	0	1	0	1	0	1	1

Лінійний профіль визначатимемо за допомогою обчислень відстані Хеммінга d між лінійними комбінаціями входів і лінійними комбінаціями виходів. Так, наприклад, відстань Хеммінга $d(b_0 \oplus b_2;\ b_0^* \oplus b_1^* \oplus b_2^*)$ дорівнює кількості позицій, в яких біти вхідної комбінації $b_0 \oplus b_2$ і вихідної композиції різні:

$$d(b_0 \oplus b_2;\ b_0^* \oplus b_1^* \oplus b_2^*) = 4.$$

Повторивши аналогічні підрахунки для інших комбінацій, визначимо лінійний профіль S-бокса. Для зручності доцільно переписати результати у вигляді табл. 3.15.

Таблиця 3.15

Лінійний профіль S-бокса

	Вихід							
Вхід	0	b_0^*	b_1^*	b_2^*	$b_0^* \oplus b_1^*$	$b_0^* \oplus b_2^*$	$b_1^* \oplus b_2^*$	$b_0^* \oplus b_1^* \oplus b_2^*$
0	0	4	4	4	4	4	4	4
b_0	4	6	4	4	2	2	4	2
b_1	4	4	2	4	6	4	2	2
b_2	4	2	4	4	2	6	4	2
$b_0 \oplus b_1$	4	2	2	4	4	2	6	4
$b_0 \oplus b_2$ $b_1 \oplus b_2$	4	4	4	0	4	4	4	4
$b_0 \oplus b_1 \oplus b_2$	4	2	6	4	4	2	2	4
	4	4	2	4	2	4	2	6

Зазначимо, що ми знехтували афінними комбінаціями вигляду $b_0 \oplus b_2 \oplus 1$, бо коли відстань Хеммінга d між лінійними комбінаціями $f_{\text{вхід}} = f(b_0, b_1, b_2)$ та $f_{\text{вихід}} = f(b_0^*, b_1^*, b_2^*)$ вхідних і вихідних бітів становить

$$d(f_{\text{вхід}}, f_{\text{вихід}}) = \alpha,$$

то

$$d(f_{\text{вхід}}, f_{\text{вихід}} + 1) = 8 - \alpha;$$

$$d(f_{\text{вхід}} + 1, f_{\text{вихід}}) = 8 - \alpha;$$

$$d(f_{\text{вхід}} + 1, f_{\text{вихід}} + 1) = \alpha.$$

Традиційно якість апроксимації вимірюють імовірністю того, що дана лінійна апроксимація є правильною за умови, що вхідні біти вибираються незалежно і випадково. Наприклад, імовірність апроксимації $b_0 = b_0^* \oplus b_2^*$ дорівнює $6/8$, а апроксимація $b_0 \oplus b_2 = b_2^*$ є достовірною, бо її ймовірність дорівнює 1.

Успішність проведення лінійного аналізу зростає із збільшенням різниці .

Найкращі лінійні апроксимації задаються тими функціями, для яких відстань Хеммінга відрізняється якомога найбільше від середнього значення (у прикладі це 4). Ця різниця називається відхиленням (англ. bias) і змінюється від $\varepsilon = 0$ (коли ймовірність того, що апроксимація правильна, дорівнює 1/2) до $\varepsilon = 1/2$ (коли апроксимація достовірна).

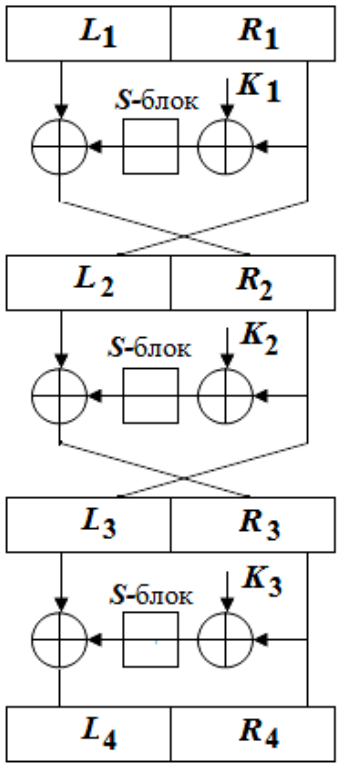


Рис. 3.6

Задача 34. У деякому DES-подібному трираундовому шифрі раундова функція – операція XOR над бітами раундового ключа і відкритого тексту та заміна у S-боксі (рис. 3.6). Таблиця замін S-бокса така, як у задачі 29. Довжина блока – 6 бітів, трибітові раундові ключі k_1, k_2, k_3 генеруються з ключа K шифру. Шифр має структуру Фейстеля: півблоки L_1, R_1 складаються з відкритого тексту, L_4, R_4 – з шифротексту, півблоки L_2, R_2 і L_3, R_3 є вхідними у другий і третій раунди відповідно, при цьому $R_1 = L_2$, $R_2 = L_3$, $R_3 = R_4$.

Використавши лінійний профіль S-боксу, побудований у задачі 33, знайдіть декілька можливих лінійних дворaундових характеристик

для вхідних бітів відкритого тексту, шифротексту і бітів раундових ключів. Яка ймовірність того, що характеристика правильна?

Р о з в' я з а н н я. Для першого раунда використаємо лінійну апроксимацію: $b_0 \oplus b_1 = b_0^* \oplus b_2^*$, для якої ймовірність бути правильною дорівнює $\frac{3}{4}$. За її допомогою для бітів ключа та лівих і правих півблоків знаходимо:

$$K1_{(0,1)} \oplus R1_{(0,1)} = L1_{(0,2)} \oplus R2_{(0,2)}$$

або

$$R2_{(0,2)} = K1_{(0,1)} \oplus R1_{(0,1)} \oplus L1_{(0,2)}.$$

Для другого раунда достовірною є аппроксимація $b_0 \oplus b_2 = b_2^*$ (ймовірність 1). Відтак

$$R2_{(0,2)} \oplus K2_{(0,1)} = R4_{(2)} \oplus R1_{(2)}.$$

Комбінація двох останніх рівнянь дає двораундову лінійну характеристику

$$L1_{(0,2)} \oplus R1_{(0,1,2)} \oplus R4_{(2)} = K1_{(0,1)} \oplus K2_{(0,2)}.$$

За лемою про набігання знаків (piling-up lemma) відхилення – мультиплікативне і ймовірність цієї комбінації становить

$$\varepsilon = 2\varepsilon_1\varepsilon_2 = 2 \cdot \frac{3}{4} \cdot \frac{1}{2} = \frac{3}{4}.$$

Спробуємо отримати більше інформації про ключ. Стартуємо з апроксимації для другого раунду, яку перепишемо у вигляді

$$R2_{(0,2)} = K2_{(0,2)} \oplus R4_{(2)} \oplus R1_{(2)}.$$

З іншого боку,

$$R2_{(0,2)} = L1_{(0,2)} \oplus S1_{(0,2)}(R1, K1),$$

де $S1_{(0,2)}(R1, K1)$ – вихід S-бокса за умови, шо на його вхід подана сума $R1 \oplus K1$ у першому раунді. Якщо припустити, що зловмисник має доступ до збору пар «відкритий текст/шифротекст», отриманих на одному ключі, то за вже «передбаченим» ключем k_1 він зможе перевірити, чи виконується для бітів ключа k_2 умова

$$K_{2_{(0,2)}} \oplus R_{4_{(2)}} \oplus R_{1_{(2)}} \stackrel{?}{=} L_{1_{(0,2)}} \oplus S_{1_{(0,2)}}(R_1, K_1).$$

У разі неправильних припущень щодо ключа зазначене співвідношення не виконуватиметься приблизно для половини варіантів, тоді як правильна здогадка обумовить виконання умови значно частіше.

Д о д а т о к. Лема про набігання знаків. Нехай $X_i \in \{0,1\}$, – незалежні випадкові величини, кожна з яких приймає значення 0 з імовірністю $\frac{1}{2}+\varepsilon_i$, де відхилення ε_i належать інтервалу $\left[-\frac{1}{2};\frac{1}{2}\right]$, $i=1,2,..,n$. Тоді випадкова величина

$$X = X_1 \oplus X_2 \oplus ... \oplus X_n$$

приймає значення 0 з імовірністю $\frac{1}{2}+\varepsilon_i$, де $\varepsilon = 2^{n-1}\prod_{i=1}^{n}\varepsilon_i$.

ТЕСТИ

1. Перемішування інформації під час шифрування приховує зв’язок між

   а) секретним та відкритим ключем;
   б) відкритим текстом та ключем;
   в) між початком та кінцем шифротексту;
   г) шифротекстом та ключем.

2. Ефект розсіювання під час шифрування

   а) збільшує кількість шифротекстів, які зашифровані на одному ключі;
   б) поширює вплив кожного знаку відкритого тексту та елемента ключа на значну кількість знаків шифротексту;
   в) спрощує процедуру розшифрування криптограми;
   г) приховує елементи ключа серед знаків шифрованого тексту.

3. Які з наступних шифрів забезпечують ефективне розсіювання та перемішування інформації?

   а) шифр простої заміни;
   б) шифр Хілла;
   в) шифр Віженера;
   г) криптосистема DES.

4. Алгоритм шифрування є блоковим, якщо

   а) він не застосовує схему Фейстеля;

б) він зашифровує/розшифровує блоки тексту фіксованої довжини;
в) в алгоритмі обов'язково використовуються S-бокси;
г) у ньому ключ завжди поділяється на блоки фіксованої довжини, які послідовно використовуються при шифруванні.

5. Мережу Фейстеля покладено в основу багатьох блокових шифрів, оскільки

а) збільшення кількості раундів шифрування забезпечує підвищення стійкості криптоалгоритму;
б) для оборотності мережі Фейстеля обов'язково потрібна оборотність функції ускладнення;
в) мережа Фейстеля достатньо компактна та проста для реалізації;
г) інших способів реалізації блокових шифрів не існує.

6. Необоротність функцій ускладнення, що застосовані у схемі Фейстеля, можна подолати за допомогою

а) перестановок; б) S-боксів;
в) операції XOR; г) розбиття процесу шифрування на раунди.

7. Нехай мережа Фейстеля, що складається з n раундів, використовує лінійні функції ускладнення, тобто в i-му раунді виконуються такі операції: $L_{i+1} = R_i$; $R_{i+1} = L_i \oplus R_i \oplus K_i$, де K_i – підключ раунду. Як розшифрувати шифрований текст?

а) $R_i = L_{i+1}$, $L_i = R_i \oplus L_i \oplus K_i$, $i = n, n-1, ..., 1$;
б) $R_i = L_{i+1}$, $L_i = R_{i+1} \oplus L_{i+1} \oplus K_i$, $i = n, n-1, ..., 1$;
в) $R_i = L_{i+1}$, $L_i = L_{i+1} \oplus K_{i+1}$, $i = n, n-1, ..., 1$;
г) $R_i = L_i \oplus K_i$, $L_i = L_{i+1} \oplus R_{i+1}$, $i = n, n-1, ..., 1$.

8. Нехай блоковий шифр з довжиною блоку 32 біта реалізує моноалфавітну заміну. Скільки спроб у найгіршому випадку знадобиться виконати криптоаналітику для дешифрування перехопленого шифрованого блоку, що містить 7 одиниць та 25 нулів?

а) 2^7; б) 2^{18}; в) 2^{32}; г) 2^{64}.

9. При шифруванні на вхід блокового шифру, котрий спроектовано як шифр перестановки, мають подаватися 32-бітові блоки відкритого тексту. Скільки спроб має виконати криптоаналітик (у найгіршому випадку), щоб дешифрувати перехоплений шифрований блок, що містить 7 одиниць та 25 нулів?

а) 2^{32}; б) 2^7; в) $32!$; г) C_{32}^7.

10. Стійкість правильно спроектованого блокового шифру при збільшенні кількості раундів шифрування

а) зростає; б) зменшується;
в) не змінюється; г) інша відповідь.

11. Яка інша назва операторів перестановки у блокових шифрах?

а) P-бокси; б) S-бокси;
в) оператори циклічного зсуву ; г) ключовий розклад.

12. Яка інша назва операторів підстановки у блокових шифрах?

а) P-бокси; б) S-бокси;
в) оператори циклічного зсуву ; г) ключовий розклад.

13. S-боксом блокового шифру називають оператор

а) циклічного зсуву на змінну кількість бітів;
б) табличну заміну, за допомогою якої одна група бітів відображається в іншу групу;
в) оператор перевпорядкування бітів у блоці;
г) фіксовану перестановку бітів у блоці.

14. Який оператор блокового шифру називають P-боксом?
а) циклічного зсуву на змінну кількість бітів;
б) табличну заміну, за допомогою якої одна група бітів відображається в іншу групу;
в) оператор упорядкування байтів у блоці;
г) фіксовану перестановку бітів у блоці.

15. Сконструюйте прямий P-бокс 8×8, що у вхідному блоці міняє місцями четвертий і перший біти, а також п'ятий та восьмий відповідно, залишаючи решту бітів без змін.

а) (1 4 5 8); б) (1 2 3 6 7 8);
в) (4 1 8 5 2 3 6 7) ; г) (4 2 3 1 8 6 7 5).

16. Яка з нижченаведених таблиць описує P-бокс розширення довжиною вісім бітів?

а) (1 2 6 7 5 8); б) (1 2 6 4 5 3 7 8);
в) (1 3 7 2 4 5 6 5 7 8); г) (1 3 2 4 6 7 5 8).

17. Яка з нижченаведених таблиць описує P-бокс стискання довжиною вісім бітів?

а) (1 2 6 7 5 8); б) (1 2 6 4 5 3 7 8);
в) (1 3 7 2 4 5 6 5 7 8); г) (1 3 2 4 6 7 5 8).

18. Які з нижченаведених операторів блокових шифрів є оборотними?

а) прямі P-бокси;
б) P-бокси розширення;
в) P-бокси стискання;
г) S-бокси, що мають на вході та виході різну кількість бітів.

19. Яке значення буде на виході S-боксу блокового шифру, який задається нижченаведеною таблицею, якщо на вхід боксу подано комбінацію 101?

	00	01	10	11	Праві біти
Ліві біти 0	011	101	111	100	
1	000	010	001	110	

а) 110; б) 011 ; в) 101 ; г) 010.

20. У шифрах, що реалізують схему Фейстеля, застосовуються оператори (функції перетворення)
а) тільки оборотні;
б) тільки необоротні;
в) оборотні та необоротні;
г) інша відповідь.

21. Які з нижченаведених шифрів побудовані на основі мережі Фейстеля?

а) AES; б) DES; в) RSA; г) DSS; д) ГОСТ 28147-89.

22. Які твердження *правильні* щодо побудови алгоритму DES?

а) в його основі лежить мережа Фейстеля;
б) ефективна довжина ключа шифру дорівнює 64 біти;
в) для шифрування використовується множення за модулем $2^{64}+1$;
г) для шифрування застосовуються S-бокси.

23. Яку довжину має ключ алгоритму DES після вилучення перевірочних бітів?

а) 48 ; б) 56; в) 64; г) 128 .

24. Який розмір раундового ключа у алгоритмі DES?

а) 48 ; б) 56; в) 64; г) 128.

25. Скільки раундів шифрування у алгоритмі DES?

а) 32 ; б) 4; в) 12; г) 16.

26. Після виконання скількох раундів шифрування за допомогою алгоритму DES можна вважати шифрований текст випадковою функцією відкритого тексту та ключа?

а) 5 ; б) 6; в) 7; г) 8.

27. При зашифруванні за алгоритмом DES після 16-го раунду правий та лівий півблоки шифрованого тексту

а) не міняються місцями, а відразу об’єднуються в один блок;
б) міняються місцями, а потім об’єднуються в один блок;
в) міняються місцями, об’єднуються в один блок і далі шифруються останній раз;
г) додаються до лівого та правого півблоків відкритого тексту.

28. За яким порядком використовують раундові ключі при розшифруванні тексту, зашифрованого за допомогою криптоалгоритму DES?

а) у тому ж порядку, що й при зашифруванні;
б) у зворотному порядку порівняно з зашифруванням;
в) у будь-якому порядку;
г) раундові ключі при зашифруванні та розшифруванні не збігаються.

29. Чому під час генерації раундових ключів у алгоритмі DES не використовуються перевірочні біти?

а) вони лінійно виражаються через відповідні інші біти;
б) неможливо побудувати схему формування раундових ключів з ключа довжиною 64 біти;
в) не існує P-боксу стискання з 64 бітів до 48 бітів;
г) не існує P-боксу розширення з 48 бітів до 64 бітів.

30. За допомогою якої операції у алгоритмі DES довжина раундового ключа зменшується до 48 бітів?

а) вилучення перевірочних бітів;
б) зсуву межових бітів;
в) застосування S-боксу;
г) використання стискаючої перестановки.

31. Відомі слабкі ключі алгоритму DES породжують

а) раундові підключі малого розміру;
б) два різних раундових підключі, що повторюються вісім разів;
в) однакові підключі для усіх раундів;
г) раундові підключі великого розміру.

32. Напівслабкі ключі алгоритму DES породжують

а) раундові підключі малого розміру;
б) два різних раундових підключі і далі повторюють їх вісім разів;
в) однакові раундові підключі того самог вигляду, що й ключ шифру;
г) ключі, що не шифрують відкритий текст.

33. На вхід S-боксу алгоритму DES подаються два вектори: $\overline{x}$ та $\overline{y} = \overline{x} \oplus (001100)$. Якою найменшою кількістю бітів відрізнятимуться вектори $\overline{x}$ та $\overline{y}$ на виході S-боксу ?

а) 1; б) 2; в) 3; г) 4.

34. Заміни у S_2 - боксі алгоритму DES мають наступний вигляд

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

Які вхідні бітові вектори мають потрапити на вхід другого S-боксу, щоб на виході з нього отримати комбінацію 0101?

а) 001100; 011101; 100000; 101001;
б) 000110; 011011; 100010; 110011;
в) 011100; 011111; 110000; 111011;
г) 000110; 001111; 101010; 100011.

35. Гіпотетичний S-бокс ($S(x)$)

12	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7

1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

використовується аналогічно стандартним S-боксам алгоритму DES, перетворюючи вхідний 6-бітовий вектор у вихідний 4-бітовий. Установіть відповідність між вхідними векторами 111001, 000110, 000101, 001101 та виходами 0100, 1101, 0111, 0011.

а) S(111001)=0011, S(000110)=0100, S(000101)=1101, S(001101)=0111;
б) S(111001)=0111, S(000110)=1101, S(000101)=0100, S(001101)=0011;
в) S(111001)=0100, S(000110)=1101, S(000101)=0011, S(001101)=0111;
г) S(111001)=0011, S(000110)=1101, S(000101)=0100, S(001101)=0111.

36. Уставте пропущене слово: «За допомогою P-боксів алгоритму DES чотири біти від кожного S- боксу у наступному раунді потрапляють у ……інших різних S-боксів».

а) чотири; б) п’ять; в) шість; г) вісім.

37. З якою метою в алгоритм DES уведена розширювальна перестановка?

а) для перемішування даних;
б) для узгодження розмірів півблока даних та раундового ключа;
в) для зручність подальшої роботи з S-боксами;
г) для уведення далі стискаючої перестановки.

38. Якщо за допомогою криптоалгоритму DES зашифрувати відкритий текст $M = [0]^{64}$ (64 нулі), то отримаємо

а) підключ першого раунду;
б) шифрований текст, що буде відрізнятися від $[0]^{64}$;
в) ключ шифру;
г) шифрований текст у вигляді $[0]^{64}$.

39. Для яких з нижченаведених шифрів буде *правильним* таке твердження: «Композиція двох шифрів з різними ключами K_1 і K_2 еквівалентна такому самому шифру з деяким іншим ключем K_3»?

а) афінний шифр;
б) шифр Віженера з ключами однакової довжини;
в) алгоритм DES;

г) шифр Віженера з ключами різної довжини;
д) шифр Хілла з ключовими матрицями однакового порядку;
е) моноабеткова підстановка.

40. Основний чинник того, що шифрування за допомогою криптоалгоритму DES вважається на сьогодні нестійким – це…

а) виявлення небезпечного дефекту у конструкції S-боксів алгоритму;
б) відмова провідних розробників шифрів від мережі Фейстеля;
в) можливість зламати шифр за допомогою квантового комп'ютера;
г) недостатня довжина ключа шифру в умовах зростання потужності обчислювальної техніки.

41. Відкритий текст $M = [0]^{32}[1]^{32}$ шифрують за допомогою алгоритму DES з ключем $K = [1]^{56}$ і після першого раунду отримують шифрований текст C. Якщо використавши ключа $K' = [0]^{56}$ на вхід алгоритму DES подати відкритий текст $M' = [1]^{32}[0]^{32}$, то після першого раунду отримаємо шифрований текст

а) $\overline{C}$; б) M; в) C; г) $C \oplus \overline{M}$; д) недостатньо інформації.

42. Відкритий текст $M = [1]^{64}$ шифрують за допомогою алгоритму DES та ключа $K = [1]^{56}$. Який проміжний текст буде отримано після першого раунду?

а) FFFFFFFF43272443; б) 1111111143272443;
в)FFFFFFFF27272443 ; г) ABABABABABABABAB;
д) 4327244311111111 .

43. Які з наведених ключів алгоритму DES відносяться до слабких?

а) $[0]^{28}[0]^{28}$; б) $[A]^7[A]^7$; в) $[F]^7[F]^7$; г) $[A]^7[B]^7$;
г) $[B]^7[B]^7$; д) $[0]^{28}[1]^{28}$; е) $[1]^{28}[0]^{28}$.

44. Які твердження *правильні* щодо шифрування за допомогою алгоритму DES?

а) у першому раунді розшифрування використовується раундовий ключ K_1;

б) у тринадцятому раунді розшифрування використовується раундовий ключ K_4;

в) якщо на вхід i-ого раунду зашифрування потрапив блок $L_{i-1} \| R_{i-1}$, то на вхід (16–i)-ого раунду розшифрування подається блок $R_i \| L_i$;

г) у процесі розшифрування на вхід фінальної перестановки IP^{-1} потрапляє блок $L_{16} \| R_{16}$.

45. Алгоритм DES з 56-бітовим ключем у 1979 р., коли він був стандартом шифрування, мав достатню криптостійкість, щоб протистояти повному перебору ключів на стандартному комп'ютері тих часів. Приймемо, що потужність комп'ютерної техніки загального призначення щороку зростає приблизно на 40 %. Тоді у 2013 році алгоритм DES «не поступився» б повному перебору ключів, якби довжина його ключа була б не меншою, ніж

а) 68 біт; б) 70 біт; в) 73 біти; г) 85 біт; д) 98 біт.

46. Криптоалгоритм 2DES вразливий щодо атаки «зустріч посередині». Її суть полягає у наступному: для пари «відкритий текст M – відповідний шифрований текст C» на кожному з можливих ключів зашифровується відкритий текст $E_k(M)$ і розшифровується шифрований текст $D_k(C)$. Ключ шифру складається з пари ключів (k_1, k_2), для якої

а) $E_{k_1}(M) \oplus C = D_{k_2}(C) \oplus M$;

б) $E_{k_1}(C) = D_{k_2}(M)$;

в) $E_{k_1}(M) = E_{k_2}(M)$ і $D_{k_1}(C) = D_{k_2}(C)$;

г) $E_{k_1}(M) = D_{k_2}(C)$.

47. Чому алгоритм 2DES не використовується для шифрування інформації?

а) занадто велика складність обчислень такого шифрування;

б) різко зростає кількість слабких та напівслабких ключів;

в) недостатня довжина ключа;

г) за допомогою атаки «зустріч посередині» стійкість алгоритму 2DES зводиться до стійкості звичайного DES.

48. Яка атака робить шифрування за допомогою криптоалгоритму 2DES марним у порівнянні з шифруванням за алгоритмом DES?

а) атака «зустріч посередині»;

б) атака за допомогою грубої сили;
в) атака на основі вибраного відкритого тексту;
г) атака на основі вибраного шифрованого тексту.

49. Який об'єм комп'ютерної пам'яті знадобиться для проведення атаки «зустріч посередині» на l-блоковий шифр, якщо подвійне зашифрування здійснюється у відповідності з рівнянням $C = E_{k_1}(E_{k_2}(M))$, а довжина кожного з ключів k_1, k_2 складає n бітів? Вважайте, що криптоаналітику відомі дві пари $C_1 = E_{k_1}(E_{k_2}(M_1))$ і $C_2 = E_{k_1}(E_{k_2}(M_2))$.

а) 2^{nl}; б) 2^{n+l}; в) $2^n(n+l)$; г) $2^l(n+l)$; д) $2^n + n + l$.

50. Уставити пропущені слова:

«Якщо відкритий текст шифрують за допомогою криптосистеми 3DES з двома ключами, то найпоширенішою схемою є така: у першому каскаді виконується … , у другому каскаді – …, у третьому каскаді – …»

а) зашифрування, зашифрування, розшифрування;
б) зашифрування, розшифрування, зашифрування;
в) розшифрування, зашифрування, розшифрування;
г) розшифрування, розшифрування, зашифрування.

51. Яким є відношення довжини ефективного ключа алгоритму 3DES до довжини ефективного ключа простого алгоритму DES? Врахувати можливість проведення атаки «зустріч посередині».

а) 80/32; б) 112/64; в) 168/56; г) 80/56.

52. Чому дорівнює відношення швидкості шифрування v_1 за допомогою криптоалгоритму DES до швидкості шифрування v_2 за допомогою криптоалгоритму 3DES?

а) 9; б) 2; в) 3; г) 1/3; д) 6; е) 1/2.

53. Поясніть принцип схеми шифрування криптосистеми 3DES.
а) у криптосистемі 3DES завжди використовуються три окремі 128-бітові ключі, з яких за ключовим розкладом виробляється ефективний ключ довжиною 384 біти;
б) у криптосистемі 3DES спочатку двічі виконується шифрування на двох 56-бітових ключах, а далі – шифрування за допомогою функції «зустріч посередині» і ключа довжиною 112 бітів;

в) у криптосистемі 3DES використовуються два або три 56-бітові ключі, текст обробляється за схемою «зашифрування-розшифрування-зашифрування» або «зашифрування-зашифрування-зашифрування»;

г) у криптосистемі 3DES спочатку виконується зашифрування і розшифрування на двох різних 56-бітових ключах, а далі – шифрування за допомогою функції «зустріч посередині» і ключа довжиною 256 бітів.

54. Який алгоритм став стандартом симетричного алгоритму блокового шифрування США, витіснивши алгоритм DES?

а) RSA; б) KERBEROS; в) BLOWFISH; г) RIJNDAEL.

55. Поліном $x^7 + x^5 + 1$ у полі $GF(2^8)$ відповідає 8-бітовому слову

а) 10100001; б) 10000010; в) 01100001; г) 11100001.

56. У алгоритмі AES певні операції виконуються над байтами, які розглядаються як елементи поля

а) $GF(2^{16})$; б) $GF(2^8)$; в) $GF(2^2)$; г) $GF(2^{32})$.

57. Який многочлен у полі $GF(2^8)$ відповідає байту 01010111 (57 у шістнадцятирічній системі числення)?

а) $x^8 + x^5 + x^3 + x^2 + x$; б) $x^5 + x^3 + x^2 + 1$;

в) $x^7 + x^4 + x^2 + x + 1$; г) $x^6 + x^4 + x^2 + x + 1$.

58. Який многочлен у полі $GF(2^8)$ відповідає байту $F8$ у шістнадцятковій системі числення?

а) $x^8 + x^7 + x^6 + x^5 + x^4$; б) $x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$;

в) $x^7 + x^6 + x^5 + x^4 + x^3$; г) $x^2 + x + 1$.

59. У алгоритмі AES множення елементів поля $GF(2^8)$ зводиться до множення многочленів із зведенням їх за модулем двійкового многочлену

а) $x^8 + x^5 + x^3 + x^2 + 1$; б) $x^6 + x^3 + x^2 + x + 1$;

в) $x^8 + x^4 + x^3 + x + 1$; г) $x^6 + x^4 + x^2 + x + 1$.

60. Чим відрізняється шифрування в останньому раунді алгоритму AES від шифрування у попередніх раундах?

а) відсутністю перемішування стовпців матриці $State$;
б) відсутністю заміни байтів;
в) відсутністю зсуву рядків матриці $State$;
г) відсутністю додавання раундового підключа.

61. Що забезпечує стійкість криптоалгоритму AES?

а) гнучкість;
б) простота реалізації;
в) довжина ключа;
г) можливість шифрувати блоки різної довжини.

62. Довжина ключа криптоалгоритму AES залежить від

а) довжини блока шифрованого тексту;
б) кількості раундів шифрування;
в) версії криптоалгоритму AES;
г) не змінюється у будь-якому разі.

63. Яка довжина ключа у стандарті AES?

а) тільки 128 бітів; б) тільки 192 біта;
в) тільки 256 бітів; г) будь-яка з наведених вище.

64. Яка довжина раундових ключів встановлена у стандарті шифрування AES?

а) тільки 128 бітів; б) тільки 192 біта;
в) тільки 256 бітів; г) залежить від версії криптоалгоритму;
д) залежить від кількості раундів даної версії.

65. При шифруванні за допомогою алгоритму AES відкритий текст розбивається на блоки довжиною

а) тільки 128 бітів; б) тільки 192 біта;
в) тільки 256 бітів; г) залежить від версії криптоалгоритму;
д) залежить від кількості раундів даної версії.

66. Як називають проміжні результати при шифруванні за допомогою алгоритму AES?

а) блоки; б) стани; в) раунди; г) матриці; д) байти.

67. Записати матрицю $State$, що має бути подана на вхід першого раунду алгоритму AES, якщо відкритий текст у шістнадцятковій системі має вигляд

(0B 0A 14 10 02 11 03 07 00 05 0D 20 OE 12 05 1E)$_{16}$

а) $\begin{pmatrix} 0B & 0A & 14 & 10 & 02 & 11 & 03 & 07 \\ 00 & 05 & 0D & 20 & 0E & 12 & 05 & 1E \end{pmatrix}$; б) $\begin{pmatrix} 0B & 00 \\ 0A & 05 \\ 14 & 0D \\ 10 & 20 \\ 02 & 0E \\ 11 & 12 \\ 03 & 05 \\ 07 & 1E \end{pmatrix}$;

в) $\begin{pmatrix} 0B & 0A & 14 & 10 \\ 02 & 11 & 03 & 07 \\ 00 & 05 & 0D & 20 \\ 0E & 12 & 05 & 1E \end{pmatrix}$; г) $\begin{pmatrix} 0B & 02 & 00 & 0E \\ 0A & 11 & 05 & 12 \\ 14 & 03 & 0D & 05 \\ 10 & 07 & 20 & 1E \end{pmatrix}$.

68. Яка з чотирьох внутрішніх операцій раунду шифрування алгоритму AES не змінює вмісту байтів блоку, поданого на її вхід?

а) $\mathrm{SubBytes}(State)$; б) $\mathrm{ShiftRows}(State)$;

в) $\mathrm{MixColumns}(State)$; г) $\mathrm{AddRoundKey}(State, RoundKey)$.

69. У алгоритмі AES операція $\mathrm{SubBytes}(State)$ – це

а) перетворення, при якому рядки матриці $State$ стану циклічно зсуваються на різні значення;

б) операція XOR над байтами ключа раунду і байтами матриці $State$;

в) нелінійна байтова підстановка, що виконується незалежно для кожного байту стану;

г) перемішування стовпців матриці $State$.

70. S-бокс у алгоритмі AES відображає

а) один байт в один байт;

б) шість бітів у чотири біти;

в) шість байтів у чотири байти;

г) чотири біти у шість бітів.

71. Яка алгебра використовується в операції $\mathrm{MixColumns}$ шифра AES?

а) алгебра многочленів над полем $GF(2^8)$;

б) алгебра многочленів над полем $GF(p)$;

в) алгебра многочленів над полем $GF(2^4)$;

г) нечітка логіка.

72. Уставте потрібні числівники: «У алгоритмі AES матриця *State* містить ... рядки, а кількість Nb її стовпців є часткою від ділення довжини блоку на …»

а) чотири; чотири; б) чотири; вісім; в) вісім; шістнадцять;
г) чотири; тридцять два; д) вісім; вісім.

73. За допомогою внутрішньої операцій SubBytes(*State*) байт 45_{16} перетвориться на байт

а) 2016; б) 4716; в) 6E16; г) FD16.

SubBytes(*State*)																
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	**63**	**7C**	**77**	**7B**	**F2**	**6B**	**6F**	**C5**	**30**	**01**	**67**	**2B**	**FE**	**D7**	**AB**	**76**
1	**CA**	**82**	**C9**	**7D**	**FA**	**59**	**47**	**F0**	**AD**	**D4**	**A2**	**AF**	**9C**	**A4**	**72**	**C0**
2	**B7**	**FD**	**93**	**26**	**36**	**3F**	**F7**	**CC**	**34**	**A5**	**E5**	**F1**	**71**	**D8**	**31**	**15**
3	**04**	**C7**	**23**	**C3**	**18**	**96**	**05**	**9A**	**07**	**12**	**80**	**E2**	**EB**	**27**	**B2**	**75**
4	**09**	**83**	**2C**	**1A**	**1B**	**6E**	**5A**	**A0**	**52**	**3B**	**D6**	**B3**	**29**	**E3**	**2F**	**84**
5	**53**	**D1**	**00**	**ED**	**20**	**FC**	**B1**	**5B**	**6A**	**CB**	**BE**	**39**	**4A**	**4C**	**58**	**CF**
6	**D0**	**EF**	**AA**	**FB**	**43**	**4D**	**33**	**85**	**45**	**F9**	**02**	**7F**	**50**	**3C**	**9F**	**A8**
7	**51**	**A3**	**40**	**8F**	**92**	**9D**	**38**	**F5**	**BC**	**B6**	**DA**	**21**	**10**	**FF**	**F3**	**D2**
8	**CD**	**0C**	**13**	**EC**	**5F**	**D7**	**44**	**17**	**C4**	**A7**	**7E**	**3D**	**64**	**5D**	**19**	**73**
9	**60**	**81**	**4F**	**DC**	**22**	**2A**	**90**	**88**	**46**	**EE**	**B8**	**14**	**DE**	**5E**	**0B**	**DB**
A	**E0**	**32**	**3A**	**0A**	**49**	**06**	**24**	**5C**	**C2**	**D3**	**AC**	**62**	**91**	**95**	**E4**	**79**
B	**E7**	**C8**	**37**	**6D**	**8D**	**D5**	**4E**	**A9**	**6C**	**56**	**F4**	**EA**	**65**	**7A**	**AE**	**08**
C	**BA**	**78**	**25**	**2E**	**1C**	**A6**	**B4**	**C6**	**E8**	**DD**	**74**	**1F**	**4B**	**BD**	**8B**	**8A**
D	**70**	**3E**	**B5**	**66**	**48**	**03**	**F6**	**0E**	**61**	**35**	**57**	**B9**	**86**	**C1**	**1D**	**9E**
E	**E1**	**F8**	**98**	**11**	**69**	**D9**	**8E**	**94**	**9B**	**1E**	**87**	**E9**	**CE**	**55**	**28**	**DF**
F	**8C**	**A1**	**89**	**0D**	**BF**	**E6**	**42**	**68**	**41**	**99**	**2D**	**0F**	**B0**	**54**	**BB**	**16**

74. В алгоритмі AES кількість N_k 32-бітових слів, що складають ключ шифру,

а) може дорівнювати тільки 8; б) дорівнює 4,6, або 8;
в) залежить від кількості раундів; г) завжди стала.

75. В алгоритмі AES при зашифруванні на вхід першого раунду подається матриця *State*, що збігається з матрицею …, а виходом останнього раунду є…

а) *OutputBlock*; шифрований текст;
б) *InputBlock*; шифрований текст;

в) $InputBlock$; $OutputBlock$;
г) $\mathrm{SubBytes}(State)$; $\mathrm{ShiftRows}(State)$.

76. Які твердження *правильні* щодо внутрішніх функцій шифру AES?

а) за допомогою функції $\mathrm{SubBytes}(State)$ виконується лінійна підстановка кожного байта змінної $State$;
б) функція $\mathrm{MixColumns}(State)$ починає діяти тільки при великому ключі у 256 бітів;
в) призначення функцій $\mathrm{ShiftRows}$ і $\mathrm{MixColumns}$ – перемішати байти, розташовані в різних місцях блока вихідного повідомлення;
г) функція $\mathrm{ShiftRows}(State)$ вживається до кожного рядка матриці $State$.

77. Результат послідовного застосування яких двох функцій шифру AES не залежить від порядку їх виконання?

а) $\mathrm{SubBytes}$ і $\mathrm{ShiftRows}$; б) $\mathrm{ShiftRows}$ і $\mathrm{MixColumns}$;
в) $\mathrm{MixColumns}$ і $\mathrm{AddRoundKey}$; г) $\mathrm{AddRoundKey}$ і $\mathrm{SubBytes}$.

78. Перед конфіденційною передачею повідомлення M довжиною 128 бітів користувачі **A** та **B** узгоджують таємний, випадково вибраний 128-бітовий ключ K. Зашифрувати повідомлення можна двома шляхами: або за допомогою одноразового шифрувального блокноту згідно з рівнянням шифрування $C_1 = M \oplus K$ або за допомогою криптоалгоритму AES на ключі K, тобто знайшовши $C_2 = AES_K(M)$. Припустимо, що зловмисник знає початкову частину повідомлення M, може перехопити шифрований текст та хоче прочитати все надіслане повідомлення. Якщо в нього є необмежені обчислювальні ресурси та час, щоб у будь-який спосіб знайти ключ, то яке шифрування більш безпечне?

а) шифрування за допомогою одноразового блокноту безпечніше, оскільки тоді, навіть перевіривши всі можливі ключі, відновити невідому частину повідомлення неможливо. У разі ж використання AES супротивник в кінці кінців прочитає все повідомлення;
б) шифрування за допомогою криптоалгоритму AES безпечніше, оскільки перевірка всіх ключів не дає можливості прочитати шифрований текст. При шифруванні ж за допомогою одноразового шифрувального блокноту завдяки повному перебору ключів можна прочитати все повідомлення;

в) обидві схеми шифрування однаково безпечні, бо в обох випадках супротивник зможе за допомогою повного перебору ключів відновити весь текст;
г) обидві схеми шифрування безпечні, оскільки повний перебір ключів не дозволяє за реальний час розшифрувати повідомлення.

79. У скільки разів більше операцій шифрування потрібно провести для проведення атаки за допомогою грубої сили проти алгоритму AES-128, ніж проти алгоритму DES?

а) 2^{72}; б) 2^{64}; в) 2^{56}; г) 2^{18}.

80. Нехай існує програмно-апаратний пристрій, здатний перевіряти 1 млрд 128 -бітових ключів алгоритму AES за секунду. Як довго в цих умовах триватиме пошук ключа алгоритму?

а) менше, ніж годину; б) більше за день, але менше тижня;
в) більше за тиждень, але менше місяця;
г) більше 100 років, але менше ніж мільйон років;
д) більше, ніж мільярд років.

81. Для кожної з наведених операцій, використаних в алгоритмі DES, знайдіть операцію в алгоритмі AES, схожу за своєю дією.

1. Підсумовування за модулем 2 раундового ключа та вихідного значення функції f_{DES};
2. Підсумовування за модулем 2 вихідного значення функції f_{DES} та бітів лівого півблока;
3. S-бокс; 4. P-бокс; 5. Заміна половин блоків.

а) $\mathrm{MixColumns}$; б) $\mathrm{SubBytes}$; в) операція не є необхідною;
г) $\mathrm{ShiftRows}$; д) $\mathrm{AddRoundKey}$.

82. Метод застосування блокового шифру, який перетворює послідовність блоків відкритих даних у послідовність блоків шифрованих даних називають

а) протоколом;
б) режимом шифрування;
в) криптографічним примітивом;
г) гамуванням.

83. Різні режими шифрування блокових шифрів розроблені з метою

а) підвищити стійкість алгоритму;
б) збільшити довжину ключа шифру;

в) забезпечити можливість шифрування відкритого тексту, довжина якого більша, ніж довжина блока шифрування, яка передбачена алгоритмом;
г) забезпечити можливість шифрування відкритого тексту порціями, меншими, ніж довжина блока шифрування, яка передбачена алгоритмом.

84. У яких режимах блокові шифри можна використовувати як потокові?

а) ECB; б) CBC; в) CFB; г) OFB; д) CTR.

85. Для шифрування та дешифрування масивів файлів з довільним доступом доцільно застосовувати блоковий шифр у режимі

а) ECB; б) CBC; в) CFB; г) OFB; д) CTR.

86. У яких режимах DES можна шифрувати блоки від 1 до 8 бітів?

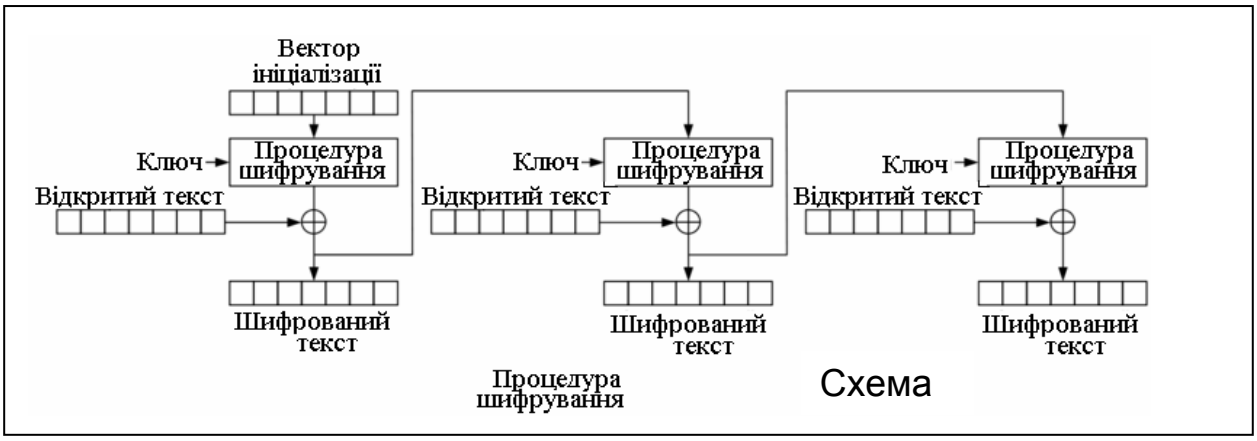
а) CTR, OFB, CFB;
б) OFB, CFB, ECB;
в) OFB, CFB, CBC;
г) CTR, CBC, CFB;
д) CFB, ECB, CBC.

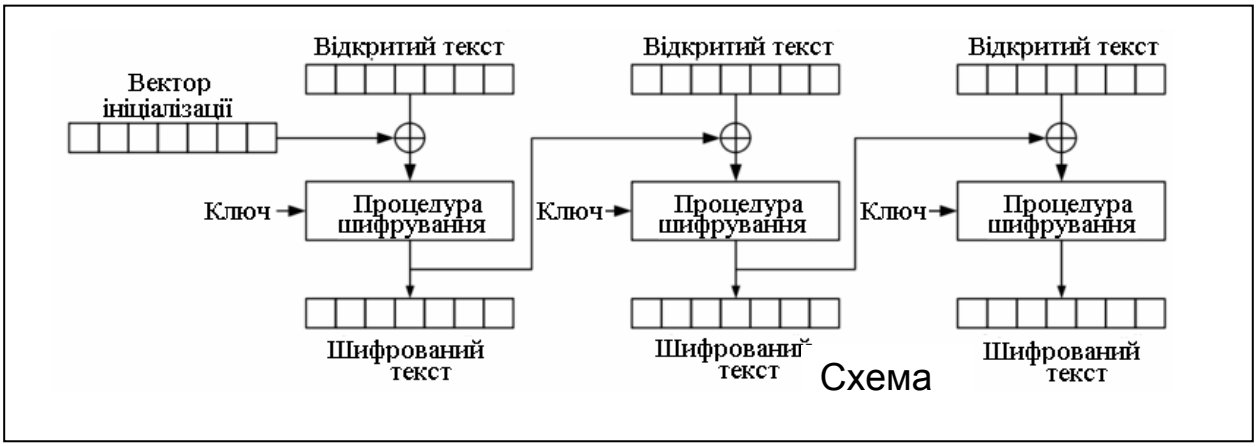
87. Установіть відповідність між наведеними на рис.3.7 схемами 1 – 4 та режимами шифруваня блокових шифрів.

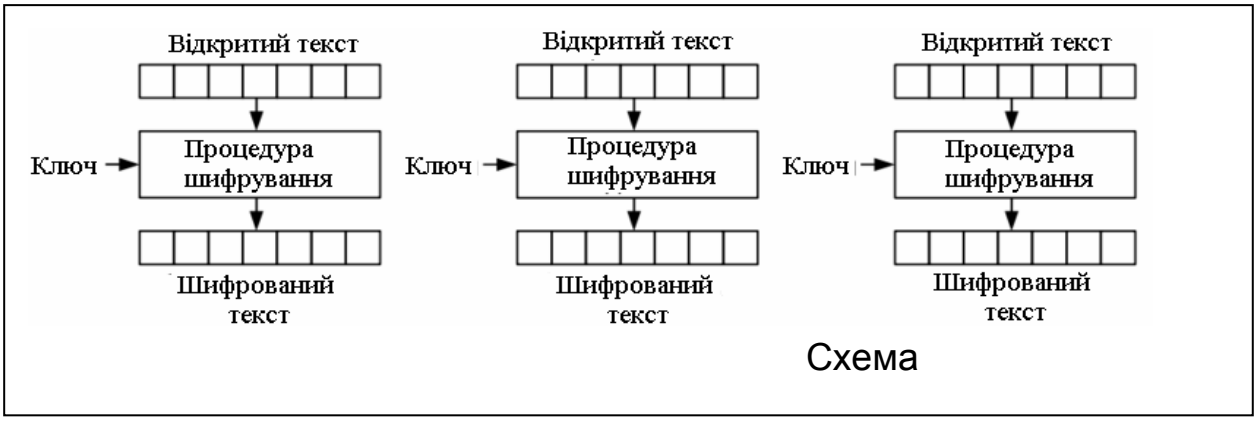
а) схема 1 – ECB; схема 2 – CBC; схема 3 – CFB; схема 4 – OFB;
б) схема 1 –CBC; схема 2 – ECB; схема 3 – OFB; схема 4 – CFB;
в) схема 1 – OFB; схема 2 – CFB; схема 3 – ECB; схема 4 – CBC;
г) схема 1 – CFB; схема 2 – CBC; схема 3 – ECB; схема 4 – OFB.

88. Які режими блокових шифрів дають змогу шифрувати блоки відкритого тексту довжиною від 1 біта до 8 бітів без додаткового доповнення?

а) ECB; б) CBC; в) CFB; г) OFB; д) CTR.


Вектор ініціалізації
Ключ
Процедура шифрування
Відкритий текст
Шифрований текст
Процедура шифрування
Схема


Відкритий текст
Вектор ініціалізації
Ключ
Процедура шифрування
Шифрований текст
Схема


Відкритий текст
Ключ
Процедура шифрування
Шифрований текст
Схема

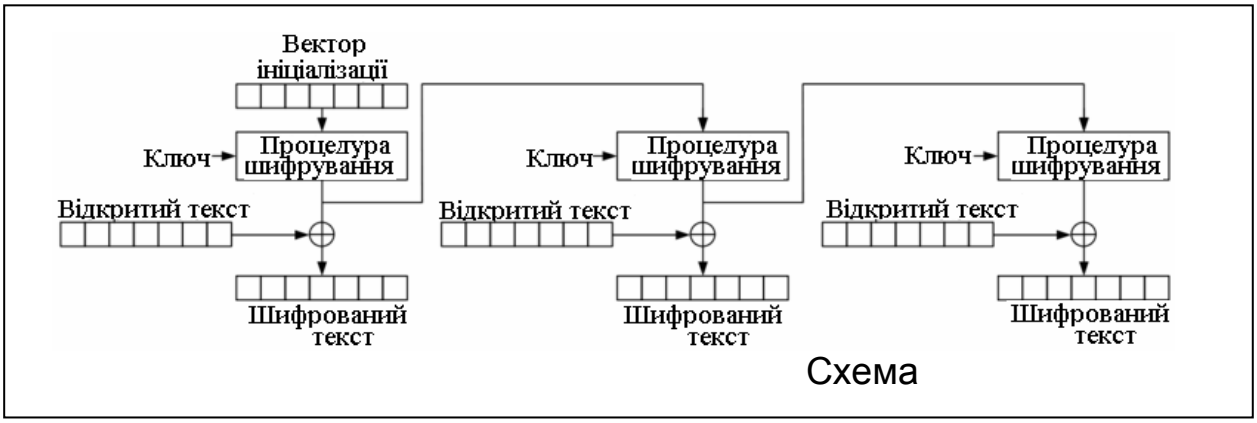

Вектор ініціалізації
Ключ
Процедура шифрування
Відкритий текст
Шифрований текст
Схема

Рис. 3.7

89. Яка з наведених властивостей ***не*** притаманна режиму ECB блокових шифрів?

а) будь-які два однакові блоки відкритого тексту при шифруванні перетворюються на однакові блоки шифротексту;
б) можна здійснити паралельне розшифрування різних зашифрованих блоків;
в) якщо зашифрований блок буде змінено або передано з помилкою, то при розшифруванні відповідний відкритий блок та ***всі*** наступні блоки будуть пошкоджені;
г) властивості а, б, в усі правильні.

90. У режимі ECB відкритий текст порівнюється за допомогою кодової книги з

а) кодовим ключем; б) операцією шифрування;
в) певним алгоритмом; г) шифрованим текстом.

91. Недолік режиму ECB – це

а) детерміністичне шифрування;
б) складність алгоритму реалізації;
в) незначний розмір блоків, що можна шифрувати;
г) необхідність розбиття відкритого тексту на блоки.

92. Які основні проблеми безпеки режиму ECB блокових шифрів?

а) лінійна залежність між блоками шифрованого тексту;
б) висока ймовірність перехоплення одного блока;
в) незалежність блоків та можливість збігу блоків після шифрування;
г) нестійкість до атаки з повторенням блоків.

93. Як можна подолати проблеми безпеки режиму ECB блокових шифрів?

а) збільшенням довжини ключа шифру;
б) застосуванням зворотного зв’язку між вже зашифрованими блоками і ще незашифрованими блоками даних;
в) уведенням вектора ініціалізації;
г) нерівномірним розбиттям відкритого тексту на блоки.

94. За допомогою режиму CBC блокового шифру можливо

а) забезпечити потокоорієнтовану передачу даних;
б) підвищити швидкість шифрування;

в) перетворити однакові блоки відкритого тексту на різні блоки шифротексту;
г) відмовитися від розбиття відкритого тексту на цілу кількість блоків потрібної довжини.

95. Шифрування у режимі CBC виконують згідно з правилом $C_i = E_k(P_i \oplus C_{i-1})$, $i = 1,2,...$, де блок C_0 називається

а) вектором ініціалізації;
б) головною частиною ключа шифру;
в) блоком відбілювання;
г) блоком доповнення.

96. Вектор ініціалізації у режимі CBC застосовують

а) при шифруванні першого блоку відкритого тексту;
б) для відмежування першого блока шифрованого тексту;
в) для спеціальної обробки останнього блока шифрованого тексту;
г) для визначення розмірів першого блока відкритого тексту.

97. Яка з наведених властивостей притаманна режиму CBC блокових шифрів?

а) будь-які два блоки відкритого тексту при шифруванні перетворюються на однакові блоки шифрованого тексту;
б) можна здійснити паралельне розшифрування різних зашифрованих блоків;
в) якщо зашифрований блок буде змінено або передано з помилкою, то при розшифруванні відповідний відкритий блок та всі наступні блоки будуть пошкоджені;
г) режим CBC має всі вищеназвані властивості а, б, в.

98. У яких режимах блокових шифрів символи відкритого тексту зчіплюються, завдяки чому шифрований текст залежить від усього попереднього відкритого тексту?

а) ECB; б) CBC; в) CFB; г) OFB.

99. У яких режимах сторона, що шифрує інформацію, і сторона, що розшифровує, використовують блоковий шифр для шифрування?

а) ECB; б) CBC; в) CFB; г) OFB.

100. Режим OFB базується на тому, що кожен біт у шифрованому тексті залежіть від

а) попередніх бітів відкритого тексту;
б) попередніх бітів шифрованого тексту;

в) бітів ключа;
г) бітів вектора ініціалізації.

101. У якому режимі блокових шифрів не використовується вектор ініціалізації?

а) ECB; б) CBC; в) CFB; г) OFB.

102. Яким буде ефект від помилки в одному біті блока шифрованого тексту, отриманого при шифруванні за допомогою DES у режимі ECB?

а) помилка з ймовірністю 1/2 при розшифруванні у будь-якому біті наступного блока шифрованого тексту;
б) помилка при розшифруванні в тому самому біті цього блока;
в) помилка з ймовірністю 1/2 при розшифруванні у будь-якому біті цього блока;
г) помилка при розшифруванні в одному біті у тій самій позиції у всіх подальших блоках.

103. Яким буде ефект від помилки в одному біті блока шифрованого тексту, отриманого при шифруванні за допомогою DES у режимі CBC?

а) помилка при розшифруванні у будь-якому біті цього блока;
б) помилка при розшифруванні у тому самому біті у наступному блоці;
в) помилка при розшифруванні у будь-якому біті решти блоків;
г) помилка при розшифруванні в одному біті у тій самій позиції у всіх подальших блоках відкритого тексту.

104. Яким буде ефект від помилки в одному біті блока C_j шифрованого тексту, отриманого при шифруванні за допомогою DES у режимі CFB?

а) помилка при розшифруванні у всіх бітах цього блока;
б) помилка при розшифруванні у тому самому біті блока C_j;
в) помилка у біті в тій самій позиції при розшифруванні у всіх блоках з парними номерами;
г) помилка у будь-якому біті при розшифруванні блоків C_j, C_{j+1}, …, $C_{j+n/s}$, де n і s – довжини блока вхідних даних та порції шифротексту.

105. Яким буде ефект від помилки в одному біті блока шифрованого тексту, отриманого при шифруванні за допомогою DES у режимі OFB?

а) помилка при розшифруванні у всіх бітах цього блока;
б) помилка при розшифруванні у тому самому біті цього блока;
в) помилка у біті в тій самій позиції при розшифруванні у всіх блоках;
г) помилка при розшифруванні у тому ж самому біті наступного блока.

106. Яким буде ефект від помилки в i-ому біті вектора ініціалізації при шифруванні за допомогою DES у режимі CBC?

а) помилка при розшифруванні в i-ому біті у кожному блоці;
б) помилка при розшифруванні в $(i+1)$-ому біті останнього блока;
в) помилка в одному біті при розшифруванні першого блока;
г) помилка в i-ому біті вектора ініціалізації не вплине на розшифрування.

107. На рис. 3.8 подано оригінальне бітове зображення емблеми сімейства операційних систем LINUX (пінгвіна Тукс), взяте з вікі-сайту «Режимы шифрования», та результат шифрування цієї емблеми, отриманий за допомогою блокового шифру. Збереження статистичних особливостей відкритого зображення при шифруванні свідчить, що блоковий алгоритм використовувся у режимі

а) ECB; б) CBC; в) OFB; г) CTR.

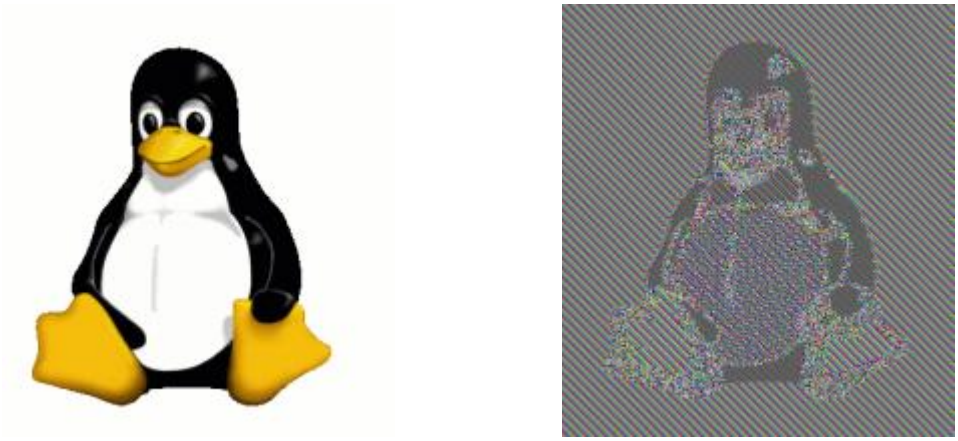


Рис. 3.8

108. Серед блоків $M_1, M_2, ..., M_l$ відкритого тексту i-ий та j-ий блоки однакові, тобто $M_i = M_j$ при $i \neq j$. При якому режимі шифрування

можна бути впевненим, що відповідні шифровані блоки C_i та C_j також збігатимуться?

а) ECB; б) CBC; в) OFB; г) CTR.

109. Шифрування повідомлень, складених з великої кількості блоків, буде ефективнішим, якщо окремі блоки шифрувати паралельно. Це можливо за умови, що шифрування кожного блоку залежить лише від фіксованої кількості попередніх блоків та вектора ініціалізації (якщо останній потрібний). У якому режимі блокового шифрування можна здійснювати паралельне шифрування?

а) ECB; б) CBC; в) OFB; г) CTR.

110. Окремі блоки великого шифрованого повідомлення, складеного зі значної кількості блоків, можна розшифрувати паралельно, якщо розшифрування блока залежить від вектора ініціалізації (якщо він передбачається режимом) та фіксованої кількості попередніх шифрованих блоків. У яких режимах блокового шифрування можна здійснювати паралельне розшифрування?

а) ECB; б) CBC; в) OFB; г) CTR.

111. Довжина відкритого повідомлення менша за довжину блока, що має подаватися на вхід блокового шифру. При яких режимах шифрування можна зашифрувати таке повідомлення без доповнення?

а) ECB; б) CBC; в) CFB; г) OFB.

112. Відомо, що пошкодження під час передачі блоку C_j шифрованого тексту, отриманого за допомогою блокового криптоалгоритму, спричиняє при розшифруванні виникнення помилок у деяких блоках відкритого тексту. Установіть відповідність між режимами шифрування ECB, CBC, CFB, OFB та CTR та пошкодженням блоків відкритого тексту.

1 – пошкодження одного блока M_j відкритого тексту;

2 – пошкодження блоків M_j та M_{j+1} відкритого тексту;

3 – пошкодження блока M_j та наступних $\frac{n}{r}-1$ блоків відкритого тексту (n – розмір блока, r – довжина порції шифротексту).

а) 1 – ECB, CTR, OFB; 2 – CBC; 3 – CFB;
б) 1 – ECB, CTR; 2 – CBC, OFB; 3 – CFB;
в) 1 – ECB, CTR, OFB; 2 – CFB; 3 – CBC;
г) 1 – ECB, OFB; 2 – CBC, CTR; 3 – CFB;
д) 1 – CTR, CFB; 2 – CBC, ECB; 3 – OFB;

е) 1 – ECB, CTR, CBC; 2 – CFB; 3 – OFB.

113. Установіть відповідність між режимами шифрування та кількістю блоків відкритого тексту, що будуть розшифровані з помилками, якщо при передачі один з шифрованих блоків був переданий пошкодженим. Відповіді запишіть у другий рядок таблиці:

ECB	CBC	CFB-*r*	OFB	CTR

114. Установіть відповідність між режимами шифрування та кількістю блоків відкритого тексту, що будуть розшифровані з помилками, якщо при передачі один з шифрованих блоків було втрачено. Відповіді запишіть у другий рядок таблиці:

ECB	CBC	CFB-*r*	OFB	CTR

115. Який режим шифрування дає змогу з'ясувати, що шифротекст був змінений у процесі передачі, тобто переданий шифротекст не відповідає відкритому тексту?

а) ECB; б) CBC; в) OFB; г) CTR.

116. Відкрите повідомлення M, що складається з 128-бітових блоків $M_1, M_2, ..., M_l$, шифрують за допомогою криптоалгоритму AES-128 з ключем K. Перший блок шифротексту – навмання вибраний 128-бітовий блок C_0, а решта шифрованих блоків утворюються за правилом:

$$C_i = C_{i-1} \oplus AES_K(M_i), \quad i = 1, 2, ..., l.$$

Увесь шифрований текст – це конкатенація блоків $C_0 \| C_1 \| C_2 \| ... \| C_l$. У чому полягає небезпека такого режиму шифрування?

а) перестановка блоків шифрованого тексту зумовлює перестановку відповідних блоків відкритого тексту і порушує цілісність інформації;
б) супротивник може непомітно підмінити окремі блоки шифротексту іншими;
в) неможливо приховати структуру інформації, що захищається;
г) пошкодження одного блока шифрованого тексту спричиняє неправильне розшифрування всіх наступних блоків.

117. Відкритий текст довжиною 640 бітів шифрують за допомогою алгоритму DES у режимі ECB. Припустимо, що під час передачі

500-го біта виникла радіоперешкода. При розшифруванні приймальною стороною може бути неправильно розшифровано

а) тільки 500-й біт;
б) тільки 500-й, 564-й і 628-й біти;
в) будь-який біт з 449-го по 512-й;
г) усі біти з 500-го по 640-й;
д) будь-який біт з 449-го по 512-й та 564-й біт.

118. Відкритий текст довжиною 640 бітів шифрують за допомогою алгоритму DES у режимі CBC. Припустимо, що під час передачі 505-го біта виникла радіоперешкода. При розшифруванні приймальною стороною може бути неправильно розшифровано

а) тільки 505-й біт;
б) тільки 505-й, 569-й і 633-й біти;
в) будь-який біт з 449-го по 512-й біт;
г) усі біти з 501-го по 640-й біт;
д) будь-який біт з 449-го по 512-й біт та 569-й біт.

119. Відкритий текст довжиною 640 бітів шифрують за допомогою алгоритму DES у 8-бітовому режимі CFB. Припустимо, що під час передачі 510-го біта виникла радіоперешкода. При розшифруванні приймальною стороною може бути неправильно розшифровано

а) тільки 510-й біт;
б) тільки 510-й, 574-й і 638-й біти;
в) 510-й біт та будь-який біт з 513-го до 640-го;
г) будь-який біт з 449-го по 512-й біт;
д) усі біти з 510-го по 640-й біт.

120. Відкритий текст довжиною 640 бітів шифрують за допомогою криптоалгоритму DES у режимі OFB. Під час передачі 187-го біта шифротексту виникла радіоперешкода. Скільки бітів можуть бути розшифровано неправильно приймальною стороною?

а) 0; б) 1; в) 5; г) 10; д) 13; е) 453.

121. Відкритий текст довжиною 640 бітів шифрують за допомогою алгоритму DES у режимі CTR. Під час передачі 150-го біта шифротексту виникла радіоперешкода. При розшифруванні приймальною стороною може бути неправильно розшифровано

а) тільки 150-й біт;
б) 22-й біт у блоках з третього по десятий;
в) 150-й біт та будь-який біт з 192-го до 640-го;
г) усі біти після 151-го;

д) будь-який біт з 150-го до 640-го.

122. Відкритий текст довжиною 6400 бітів шифрують за допомогою алгоритму DES у 8-бітовому режимі CFB. Під час передачі шифротексту було втрачено 40-й біт. Скільки блоків відкритого тексту приймальна сторона розшифрує неправильно?

а) 0; б) 1; в) 2; г) 9; д) 10; е) 100.

123. Упорядкуйте нижченаведені шифри за спаданням їх швидкості шифрування за умов однакової програмній реалізації

1) 3DES у режимі OFB з $r = 32$;
2) DES у режимі OFB з $r = 8$;
3) DES у режимі CFB з $r = 32$;
4) DES у режимі CBC.

124. Упорядкуйте нижченаведені шифри за спаданням їх швидкості розшифрування при апаратній реалізації, припустивши можливість паралельної обробки даних на чотирьох паралельних працючих машинах DES.

1) DES у режимі OFB з $r = 8$;
2) DES у режимі CFB з $r = 8$;
3) 3DES у режимі OFB з $r = 16$;
4) 3DES у режимі CBC.

РОЗДІЛ 4. ПОТОКОВЕ ШИФРУВАННЯ

Задача 1. Результатом зашифрування відкритого тексту АТАКА НА СВІТАНКУ за допомогою одноразового блокноту став шифротекст

C8C88605B53EA7C714706D3609CE4D56FE598842C8512

(букви кодують за допомогою 12-бітного ASCII-коду (табл. 4.1), пропуск між словами вилучено, шифротекст у шістнадцятковій системі числення). Яким буде шифротекст, якщо відкритий текст ВТЕЧА НА СВІТАНКУ зашифрувати, застосувавши одноразовий блокнот з тією самою гамою?

Таблиця 4.1

ASCII-кодування (CP1251)

А	Б	В	Г	Ґ	Д	Е	Є	Ж	З	И	І	Й	К	Л	М
410	411	412	413	491	414	415	404	416	417	418	406	419	41A	41B	41C
Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
41D	41E	41F	420	421	422	423	424	425	426	427	428	429	42C	42E	42F

Р о з в’ я з а н н я. Зміниться може лише результат шифрування перших чотирьох букв тексту.

С8С 886 05В $53E_{16}$=
=1100 1000 1100 1000 1000 0110 0000 0101 1011 0101 0011 1110_2;

АТАК=410 422 410 $41A_{16}$ =
= 0100 0001 0000 0100 0010 0010 0100 0001 0000 0100 0001 1010_2;

ВТЕЧ=412 422 415 427_{16} =
= 0100 0001 0010 0100 0010 0010 0100 0001 0101 0100 0010 0111.

Визначаємо знаки гами за формулою $k_i = c_i \oplus m_i$:

1000 1001 11001100 1010 01000100 0100 10110001 0010 0100.

Знаки початку нового шифротексту дорівнюють $c_i' = m_i' \oplus k_i$, тобто

1100 1000 1110 1000 1000 0110 0000 0101 1110 0101 0000 0011_2 або C8E88605E503.

Отже, шифротекст для повідомлення ВТЕЧА НА СВІТАНКУ – це

C8E88605E503A7C714706D3609CE4D56FE598842C8512.

Задача 2. Відкрите бітове повідомлення $x_1x_2x_3x_4x_5x_6z_7$ за допомогою одноразового блокноту переведене у шифрований текст 0101011. Помилково замість цього шифротексту користувачеві було

надіслано шифротекст 0100010, отриманий при зашифруванні відкритого тексту $z_0x_1x_2x_3x_4x_5x_6$ також за допомогою одноразового блокноту на тій самій гамі. Знайдіть усі можливі значення бітів $x_1x_2x_3x_4x_5x_6$.

Р о з в' я з а н н я.

$$\begin{array}{r} x_1\,x_2\,x_3\,x_4\,x_5\,x_6\,z_7 \\ \oplus\ \gamma_1\,\gamma_2\,\gamma_3\,\gamma_4\,\gamma_5\,\gamma_6\,\gamma_7 \\ \hline 0\ \ 1\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1 \end{array} \qquad \begin{array}{r} z_0\,x_1\ \ x_2\ \ x_3\ \ x_4\ \ x_5\,x_6 \\ \oplus\ \gamma_1\ \gamma_2\ \ \gamma_3\ \gamma_4\ \gamma_5\ \gamma_6\,\gamma_7 \\ \hline 0\ \ 1\ \ \ 0\ \ 0\ \ 0\ \ 1\ \ 0 \end{array} \Rightarrow$$

$$y_1\,y_2\,y_3y_4y_5\,y_6y_7 \qquad y_1'\ y_2'\ \ y_3'\ y_4'y_5'y_6'y_7'$$

$$x_1 = y_1 - \gamma_1 = 0 - \gamma_1; \qquad z_0 = y_1' - \gamma_1 = 0 - \gamma_1;$$

$$x_2 = y_2 - \gamma_2 = 1 - \gamma_2; \qquad x_1 = y_2' - \gamma_2 = 1 - \gamma_2;$$

$$x_3 = y_3 - \gamma_3 = 0 - \gamma_3; \qquad x_2 = y_3' - \gamma_3 = 0 - \gamma_3;$$

$$x_4 = y_4 - \gamma_4 = 1 - \gamma_4; \qquad x_3 = y_4' - \gamma_4 = 0 - \gamma_4;$$

$$x_5 = y_5 - \gamma_5 = 0 - \gamma_5; \qquad x_4 = y_5' - \gamma_5 = 0 - \gamma_5;$$

$$x_6 = y_6 - \gamma_6 = 1 - \gamma_6; \qquad x_5 = y_6' - \gamma_6 = 1 - \gamma_6;$$

$$z_7 = y_7 - \gamma_7 = 1 - \gamma_7; \qquad x_6 = y_7' - \gamma_7 = 0 - \gamma_7.$$

$$\begin{gathered} 0 - \gamma_1 = 1 - \gamma_2; \\ 1 - \gamma_2 = 0 - \gamma_3; \\ 0 - \gamma_3 = 0 - \gamma_4; \\ 1 - \gamma_4 = 0 - \gamma_5; \\ 0 - \gamma_5 = 1 - \gamma_6; \\ 1 - \gamma_6 = 0 - \gamma_7. \end{gathered}$$

Можливі два випадки:

а) якщо $\gamma_1 = 1$, то $\gamma_2 = 0; \gamma_3 = 1;\ \gamma_4 = 1;\ \gamma_5 = 0;\ \gamma_6 = 1;\ \gamma_7 = 0$. Тоді

$$\begin{array}{r} y = 010101 \\ \oplus\ \gamma = 101101 \\ \hline x = 111000; \end{array}$$

б) якщо $\gamma_1 = 0$, то $\gamma_2 = 1; \gamma_3 = 0;\ \gamma_4 = 0;\ \gamma_5 = 1;\ \gamma_6 = 0;\ \gamma_7 = 1$. Тоді

$$\begin{array}{r} y = 010101 \\ \oplus\gamma = 010010 \\ \hline x = 000111. \end{array}$$

Шуканими бітами можуть бути 111000; 000111.

Задача 3. Відкритий текст складається з незалежно генерованих бітів, об'єднаних попарно у біграми. Імовірність того, що біт відкритого тексту є «0», дорівнює p. Кожен біт такої пари зашифровують на одному ключі k, додаючи його до бітів (за модулем 2), тобто бітова пара m_1, m_2 відкритого тексту перетворюється на пару c_1, c_2 бітів шифротексту згідно з рівнянням $c_i = m_i \oplus k$, $i = 1,2$. Біти ключа генеруються рівномірно й випадково. Припустимо, що Ви отримали блок шифротексту, що містить t нулів і $2-t$ одиниць, $t = 0,1,2$. Визначте ймовірність того, що ключ $k = 0$ для всіх $t = 0,1,2$.

Р о з в' я з а н н я. Розглянемо такі події при $t = 0,1,2$:

A_t={блок відкритого тексту містить t нулів};

B_t={блок шифротексту містить t нулів}.

Із значення умовної ймовірності запишемо $P(k=0|B_t) = \dfrac{P(k=0, B_t)}{P(B_t)}$. Оскільки $P(k=0) = P(k=1) = 1/2$, а ключі для шифрування добираються незалежно від вибору відкритого тексту, то за формулою Бернуллі

$$P(k=0, B_t) = P(k=0, A_t) = P(k=0)P(A_t) = \frac{1}{2}C_2^t p^t (1-p)^{2-t}.$$

$$P(B_t) = P(k=0, A_t) + P(k=1, A_{2-t}) = P(k=0)P(A_t) + P(k=1)P(A_{2-t}) =$$
$$= \frac{1}{2}C_2^t p^t (1-p)^{2-t} + \frac{1}{2}C_{2-t}^t p^{2-t}(1-p)^t.$$

Врахувавши, що $C_2^t = C_{2-t}^t$, отримаємо

$$P(k=0|B_t) = \frac{\frac{1}{2}C_2^t p^t (1-p)^{2-t}}{\frac{1}{2}C_2^t p^t (1-p)^{2-t} + \frac{1}{2}C_{2-t}^t p^{2-t}(1-p)^t} =$$

$$= \frac{p^t (1-p)^{2-t}}{p^t (1-p)^{2-t} + p^{2-t}(1-p)^t} = \frac{1}{1 + p^{2-2t}(1-p)^{2t-2}}.$$

- Якщо $p < 1/2$, то $p < 1-p$, і $P(k=0, B_t)$ має максимум при $t=0$.
- Якщо $p > 1/2$, то $p > 1-p$ і $P(k=0, B_t)$ має максимум при $t=2$.
- Якщо $p = 1/2$, то $p = 1-p$ і $P(k=0, B_t) = 1/2$ при всіх $t = 0,1,2$.

У цьому випадку не можна отримати будь-яку інформацію про ключ. Якщо $t=1$, то $P(k=0, B_1) = 1/2$, що приводить до попереднього висновку щодо стійкості шифрування.

Задача 4. $c(x) = x^9 + x^5 + x^2 + x + 1$ – многочлен зворотного зв'язку 10-бітового LFSR, 0101110010 – початкове заповнення регістру. Знайдіть 10 бітів генерованої послідовності, біти зворотного зв'язку і покажіть проміжні стани регістру.

Р о з в' я з а н н я. За даним многочленом зворотного зв'язку запишемо закон рекурсії, що генеруватиме псевдовипадкову послідовність

$$x_{i+9} = x_{i+5} + x_{i+2} + x_{i+1} + x_i, \quad i = 0,1,...$$

Саме це рівняння формує стани регістру, біти зворотного зв'язку і біти вихідної послідовності.

Стани регістру										Вихідна послідовність	Біт зворотного зв'язку
S_9	S_8	S_7	S_6	S_5	S_4	S_3	S_2	S_1	S_0		
0	1	0	1	1	1	0	0	1	0	0	1
1	0	1	0	1	1	1	0	0	1	1	0
0	1	0	1	0	1	1	1	0	0	0	1
1	0	1	0	1	0	1	1	1	0	0	1
1	1	0	1	0	1	0	1	1	1	1	1
1	1	1	0	1	0	1	0	1	1	1	0
0	1	1	1	0	1	0	1	0	1	1	1
1	0	1	1	1	0	1	0	1	0	0	1
1	1	0	1	1	1	0	1	0	1	1	1
1	1	1	0	1	1	1	0	1	0	0	0

Задача 5. Побудуйте граф станів 4-бітовго LFSR с многочленом оберненого зв'язку $c(x) = x^3 + x^2 + 1$.

Р о з в' я з а н н я. Якщо внутрішній стан 4-бітового LFSR у момент часу t задати вектором $\overline{q(t)} = (s_t, s_{t+1}, s_{t+2}, s_{t+3})$, то стан регістра у наступний момент часу можна дістати з вектора $\overline{q(t)}$ за допомогою рівняння

$$\overline{q(t+1)}^T = A \cdot \overline{q(t)}^T,$$

де верхній індекс позначає операцію транспонування; матриця $A = \begin{pmatrix} c_1 & c_2 & c_3 & c_4 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ – матриця оберненого зв'язку (c_1, c_2, c_3, c_4 – коефіцієнти многочлена оберненого зв'язку $c(x) = c_3x^3 + c_2x^2 + c_1x + 1$).

У нашому випадку $A = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$.

Якщо початкове заповнення регістру 1000, то

$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = 2_{10}; \quad \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = 5_{10}; \ldots$$

Продовжуючи обчислення, можна побудувати граф станів регістра (рис. 4.1)

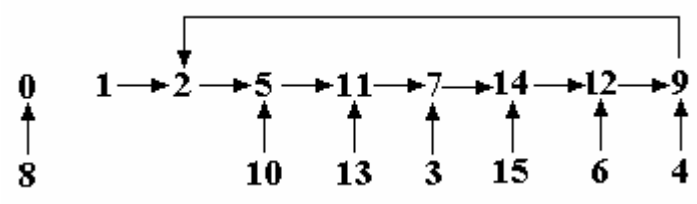


Рис. 4.1

Задача 6. Доведіть наступне твердження: для того, щоб за один такт роботи перехід у кожен внутрішній стан n-бітового регістру зсуву зі зворотним зв'язком здійснювався тільки з одного внутрішнього стану, необхідно і достатньо, щоб функція оберненого зв'язку мала вигляд

$$f(x_1,x_2,...,x_n)=x_1\oplus g(x_2,x_3,...,x_n).$$

Д о в е д е н н я. *Достатність*. Внутрішні стани n-бітового регістру зсуву описуються n-мірними двійковими векторами $\bar{x}=(x_1,x_2,...,x_n)$. При переході регістру із стану $\bar{x}=(x_1,x_2,...,x_n)$ у стан $\bar{y}=(y_1,y_2,...,y_n)$ мають виконуватися умови

$$y_1=x_2;\ y_2=x_3;\ \dots\ ;\ y_{n-1}=x_n;\ y_n=f(x_1,x_2,...,x_n).$$

Припустимо, що існує, крім стану $\bar{x}$, інший стан $\bar{x}'=(x_1',x_2,...,x_n)$, $x_1\neq x_1'$, що за такт роботи також переходить в стан $\bar{y}=(y_1,y_2,...,y_n)$. Очевидно, у цьому разі виконується рівність $f(x_1,x_2,...,x_n)=f(x_1',x_2,...,x_n)$.

Якщо функція оберненого зв'язку лінійна за першим аргументом, тобто $f(x_1,x_2,...,x_n)=x_1\oplus g(x_2,x_3,...,x_n)$, то

$$f(x_1,x_2,...,x_n)=x_1\oplus g(x_2,x_3,...,x_n)\neq x_1'\oplus g(x_2,x_3,...,x_n)=f(x_1',x_2,...,x_n).$$

Отже, приходимо до протиріччя і припущення про існування двох станів, з яких за один такт роботи можна перейти в один й той самий стан, – хибне.

Необхідність. Нехай тепер для будь-якої пари станів $\bar{x}=(x_1,x_2,...,x_n)$ і $\bar{x}'=(x_1',x_2,...,x_n)$, де $x_1\neq x_1'$, справджується рівність

$$f(x_1,x_2,...,x_n)\neq f(x_1',x_2,...,x_n).$$

Поклавши без шкоди для загальності міркувань, що $x_1=1$ і $x_1'=0$, з цієї нерівності дістанемо

$$f(1,x_2,...,x_n)=f(0,x_2,...,x_n)\oplus 1.$$

Позначимо $f(0,x_2,...,x_n)$ через $g(x_2,...,x_n)$ і подамо

$$f(1,x_2,...,x_n)=1\oplus g(x_2,...,x_n).$$

Відтак $f(x_1,x_2,...,x_n)=x_1\oplus g(x_2,x_3,...,x_n)$, що й доводили.

Задача 7. Чи будуть многочлени x^4+x+1 і x^4+1 незвідними над полем $GF(2)$?

Р о з в' я з а н н я. Многочлен $f(x)$ називається незвідним над полем, якщо його не можна подати у вигляді добутку інших многочленів, тобто $f(x)\neq g_1(x)\cdot g_2(x)$, де обидва многочлени $g_1(x)$ і $g_2(x)$ визначені над тим же полем і мають степінь, менший ніж степінь $f(x)$.

Щоб довести незвідність многочлена $f(x)=x^4+x+1$, перевіримо, чи буде він ділитися на незвідні многочлени над полем $GF(2)$, степінь яких менша або дорівнює половині степені $f(x)$. Це многочлени $x;\ x+1;\ x^2+x+1.$

Многочлен $f(x)$ ділитиметься на двочлен $x-\alpha$ тоді і тільки тоді, коли α є коренем цього многочлена, тобто $f(\alpha)=0$. Оскільки $f(1)=1^4+1+1=3\equiv 1\bmod 2\neq 0$, $f(0)=1\neq 0$, то вираз x^4+x+1 на $x+1$ і x не ділиться. Не ділиться даний многочлен і на x^2+x+1, бо $x^4+x+1=(x^2+x+1)(x^2+x)+1$ (усі розрахунки за модулем 2). Отже, многочлен x^4+x+1– незвідний над полем $GF(2)$.

Многочлен $f(x)=x^4+1$ у полі $GF(2)$ має корінь $x=1$, бо $f(1)=1+1\equiv 0(\bmod 2)$. Тому цей многочлен матиме множник $x+1$:

$$x^4+1=(x+1)(x^3+x^2+x+1),$$

і є звідним над полем $GF(2)$.

Задача 8. Знайдіть порядок многочлена x^3+x+1 над полем $GF(2)$.

Р о з в' я з а н н я. За умови, що $f(0)\neq 0$, порядок $ord(f(x))$ многочлена $f(x)$ над полем $GF(2)$ дорівнює найменшому натуральному числу, для якого двочлен x^e-1 ділиться на $f(x)$. За визначенням, врахувавши, що у полі $GF(2)$ виконується рівність $-1\equiv 1$, маємо

$$x^4+1\equiv(x^3+x+1)x+x^2+x+1;$$

$$x^5+1\equiv(x^3+x+1)(x^2+1)+x^2+x;$$

$$x^6+1\equiv(x^3+x+1)(x^3+x+1)+x^2;$$

$$x^7+1\equiv(x^3+x+1)(x^4+x^2+x+1)\Rightarrow order\,(x^3+x+1)=7.$$

Задача 9. Доведіть, що многочлен $f(x)=x^5+x^4+x^3+x^2+1$ є звідним над полем $GF(3)$.

Р о з в' я з а н н я.

$$\left.\begin{array}{l} f(0)=1\not\equiv 0;\\ f(1)=5\equiv 2\bmod 3\not\equiv 0;\\ f(2)=32+16+8+4+1\equiv 1\bmod 3\not\equiv 0\end{array}\right\}\Rightarrow$$

многочлен $f(x)$ не має лінійних множників x, $x+1$, $x+2$.

Перевіримо існування квадратичних множників:

$$f(x)=x^5+x^4+x^3+x^2+1=(x^3+ax^2+bx+c)(x^2+dx+e)=$$

$$=x^5+(a+d)x^4+(b+ad+e)x^3+(c+bd+ae)x^2+(cd+be)x+ce.$$

За методом невизначених коефіцієнтів дістаємо $\begin{cases} ce=1;\\ cd+be=0;\\ c+bd+ae=1;\\ b+ad+e=1;\\ a+d=1.\end{cases}$

Якщо $c=e=1$, то $\begin{cases} d+b=0;\\ bd+a=0;\\ b+ad=0;\\ a+d=1.\end{cases}$

Розв'язків немає.

Якщо $c=e=2$, то $\begin{cases} d+b=0;\\ bd+2a=2;\\ b+ad=2;\\ a+d=1.\end{cases}$

Є розв'язок $(a,b,c,d,e)=(0,2,2,1,2)$.

Отже, $x^5+x^4+x^3+x^2+1=(x^3+2x^2+2)(x^2+x+2)$. Даний многочлен звідний над полем $GF(3)$.

Задача 10. Побудуйте поле Галуа $GF(3^2)$. Знайдіть у цьому полі обернений елемент до елемента $2x+1$ та обчисліть значення x^9+x^2.

Р о з в' я з а н н я. Спочатку виберемо незвідний многочлен другого степеня над простим полем $Z_3 = \{0,1,2\}$. Наприклад, незвідним многочленом буде $f(x) = x^2 + x + 2$ (це випливає з того, що $f(0) = 2 \neq 0$, $f(1) = 4 \equiv 1 \bmod 3 \not\equiv 0$ і $f(2) = 8 \equiv 2 \bmod 3 \not\equiv 0$, і тому многочлен не розкладається на множники). Поле $GF(p^n)$ складається з p^n елементів, які являють собою многочлени степеня, не вищого за $n-1$, з коефіцієнтами із поля Z_p. У нашому випадку це многочлени над полем Z_3:

$$GF(3^2) = Z_3[x] / x^2 + x + 2 = \{0,1,2,x,x+1,x+2,2x,2x+1,2x+2\}.$$

Таблиці додавання та множення елементів поля будуємо, обчислюючи всі $9^2 = 81$ додавань і множень многочленів та у разі необхідності, зводячи результати за модулем вибраного незвідного многочлена $x^2 + x + 2$. Результати наведені у таблицях 4.2 і 4.3.

Таблиця 4.2

Додавання елементів поля

+	0	1	2	x	x+1	x+2	$2x$	$2x$+1	$2x$+2
0	0	1	2	x	$x+1$	x+2	$2x$	$2x$+1	$2x$+2
1	1	2	0	x+1	x+2	x	$2x$+1	$2x$+2	$2x$
2	2	0	1	x+2	x	$x+1$	$2x$+2	$2x$	$2x$+1
x	x	x+1	$x+2$	$2x$	$2x$+1	$2x$+2	0	1	2
x+1	x+1	$x+2$	x	$2x$+1	$2x$+2	$2x$	1	2	0
x+2	x+2	x	x+1	$2x$+2	$2x$	$2x$+1	2	0	1
$2x$	$2x$	$2x$+1	$2x$+2	0	1	2	x	$x+1$	x+2
$2x$+1	$2x$+1	$2x$+2	$2x$	1	2	0	x+1	x+2	x
$2x$+2	$2x$+2	$2x$	$2x$+1	2	0	1	x+2	x	$x+1$

Таблиця 4.3

Множення елементів поля

×	0	1	2	x	x+1	x+2	$2x$	$2x$+1	$2x$+2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	x+1	x+2	$2x$	$2x$+1	$2x$+2
2	0	2	1	$2x$	$2x$+2	$2x$+1	x	x+2	x+1

Продовження табл. 4.3

x	0	x	$2x$	$2x$+1	1	x+1	x+2	$2x$+2	2
x+1	0	x+1	$2x$+2	1	x+2	$2x$	2	x	$2x$+1
x+2	0	x+2	$2x$+1	x+1	$2x$	2	$2x$+2	1	x
$2x$	0	$2x$	x	x+2	2	$2x$+2	$2x$+1	x+1	1
$2x$+1	0	$2x$+1	x+2	$2x$+2	x	1	x+1	2	$2x$
$2x$+2	0	$2x$+2	x+1	2	$2x$+1	x	1	$2x$	x+2

За таблицею множення знаходимо, що

$$(2x+1)(x+2) \equiv 1 \bmod x^2 + x + 2 \Rightarrow (2x+1)^{-1} \equiv x+2 \bmod (x^2 + x + 2).$$

Відзначимо, що кількість елементів у полі $GF(3^2)$ і кільці $Z_9 = \{0,1,...,8\}$ однакова, але кожен елемент поля $GF(3^2)$, крім 0, має обернений, у той час як у кільці Z_9 оборотними є тільки елементи $1,2,4,5,7,8$.

Обчислити значення виразу $x^9 + x^2$ можна двома способами.

Перший спосіб: виконавши ділення $x^9 + x^2$ на $x^2 + x + 2$, отримаємо

$$x^9 + x^2 = (x^7 + 2x^6 + 2x^5 + 2x^3 + x^2 + x + 1)(x^2 + x + 2) + 1.$$

Оскільки у побудованому полі $x^2 + x + 2 \equiv 0$, то $x^9 + x^2 = 1$.

Другий спосіб: знайдемо порядок елемента x поля $Z_3[x] / x^2 + x + 2$. Порядком $ord\ \alpha$ будь-якого ненульового елемента α поля $GF(p^n)$, називається найменше натуральне число δ з умовою $\alpha^\delta \equiv 1$. Оскільки $p^n - 1 = 8$, то за теоремою Лагранжа порядок елемента поля $GF(p^n)$ має ділити число $p^n - 1$. У нашому випадку $p^n - 1 = 8$, тому елемент x може мати порядок $1,2,4$ або 8. Очевидно, $ord\ x \neq 1$. Тому потрібно перевірити, який з виразів $x^2 - 1$, $x^4 - 1$ чи $x^8 - 1$ ділиться без остачі на модуль $x^2 + x + 2$ (усі розрахунки за модулем 3):

$$x^2 - 1 = (x^2 + x + 2) + 2x (\bmod 3) \quad \Rightarrow \ ord\ x \neq 2;$$

$$x^4 - 1 = (x^2 + x + 2)(x^2 + 2x + 2) + 1 (\bmod 3) \quad \Rightarrow \ ord\ x \neq 4;$$

$$x^8-1=(x^6+x^5+2x^4+2x^2+x+1)(x^2+2x+2)(\mathrm{mod}\,3)\ \Rightarrow\ ord\ x=8.$$

Це означає, що елемент $\alpha=x$ – примітивний елемент поля $Z_3[x]/x^2+x+2$ і решта ненульових елементів поля є степенем елементу α. Дійсно, врахувавши, що у полі $Z_3[x]/x^2+x+2$ справедливо $\alpha^2+\alpha+2\equiv 0$, знаходимо;

$$x^2=\alpha^2=-x-2\equiv 2x+1;$$
$$x^3=\alpha^3=2x^2+x\equiv 2(-x-2)+x\equiv 2x+2(\mathrm{mod}\,x^2+x+2);$$
$$x^4=\alpha^4=2x^2+2x\equiv 2(\mathrm{mod}\,x^2+x+2);$$
$$x^5=\alpha^5=2x;$$
$$x^6=\alpha^6=2x^2\equiv x+2(\mathrm{mod}\,x^2+x+2);$$
$$x^7=\alpha^7=x^2+2x\equiv x+1(\mathrm{mod}\,x^2+x+2);$$
$$x^8=\alpha^8=x^2+x\equiv 1(\mathrm{mod}\,x^2+x+2).$$

Тоді

$$x^9+x^2=x^8\cdot x+x^2=1\cdot x+x^2=x+2x+1\equiv 1(\mathrm{mod}\,3).$$

Задача 11. Скільки елементів нараховує поле $Z_2[x]/x^5+x^2+1$? Обчисліть у цьому полі значення: $(x^4+x^2)(x^3+x+1)$.

Р о з в’ я з а н н я. Степінь модуля $f(x)=x^5+x^2+1$ дорівнює 5, потужність поля $|Z_2|=2$, тому поле $Z_2[x]/x^5+x^2+1$ нараховує $2^5=32$ елементи.

$$(x^4+x^2)(x^3+x+1)=x^7+x^5+x^5+x^3+x^4+x^2=x^7+x^3+x^4+x^2=$$
$$=(x^7+x^4+x^2)+x^3=x^2(x^5+x^2+1)+x^3\equiv x^3\,\mathrm{mod}\,x^5+x^2+1=x^3.$$

Задача 12. Який період матимуть вихідні бітові послідовності LFSR, характеристичний многочлен якого $f(x)=x^5+x^4+x^2+x+1$?

Р о з в’ я з а н н я. Період послідовності залежить від того, чи буде характеристичний многочлен LFSR незвідним.

$\left.\begin{array}{l} f(0)=1\neq 0; \\ f(1)=1\neq 0 \end{array}\right\} \Rightarrow x=0,\ x=1-$ не корені многочлена і тому многочлен не має дільників x і $x+1$.

Серед квадратичних тричленів ax^2+bx+c тільки тричлен x^2+x+1 є незвідним, а решту тричленів можна розкласти на лінійні множники. Оскільки наявність лінійних множників у даного характеристичного многочлена вже виключено, то залишається тільки перевірити, чи ділиться $f(x)=x^5+x^4+x^2+x+1$ на x^2+x+1. Очевидно,

$$x^5+x^4+x^2+x+1=(x^2+x+1)(x^3+x)+x+1$$

і тому характеристичний многочлен множників не має і є незвідним. Період послідовності, генерованої LFSR з незвідним характеристичним многочленом степеня n, має ділити число 2^n-1. У нашому випадку це число $2^n-1=2^5-1=31$– просте, тобто ділиться лише на 1 і 31. Якщо період $T=1$, то $x+1$ повинно ділитися на $f(x)$, що неможливо. Звідси приходимо до висновку, що характеристичний многочлен має період $T=31$ і є примітивним. Отже, період послідовностей, що генеруватиме заданий LFSR, при будь-якому ненульовому початковому заповненні дорівнює 31.

Задача 13. Нехай у вихідній послідовності S істинно випадкового генератора для навмання вибраного біта b_i імовірність

$$P\{b_i=0\}=P\{b_i=1\}=1/2$$

і біти послідовності між собою не корелюють. Але ключовий потік є упередженим і ймовірність появи у потоці біта «1» дорівнює $0,5+\varepsilon$, а ймовірність появи біта «0» – відповідно $0,5-\varepsilon$, де $0<\varepsilon<0,5$. Розіб'ємо послідовність S на неперетинні біграми та відкинемо усі біграми типу 00 і 11. Замінивши залишені біграми типу 01 і 10 відповідно на «0» і «1» отримаємо нову бітову послідовність S_1. Знайдіть: а) імовірність появи кожної з біграм 00,01,10, 11 у послідовності S; б) імовірність появи «0» і «1» у модифікованій послідовності S_1; в) як багато бітів потрібно взяти з послідовності S, щоб у послідовності S_1 можна було чекати на виникнення N бітів.

Р о з в' я з а н н я.

а) $P\{b_i\,b_{i+1}=00\}=P\{b_i=0\}P\{b_{i+1}=0\}=(0,5-\varepsilon)^2=0,25-\varepsilon+\varepsilon^2$;

$P\{b_i\,b_{i+1}=01\}=P\{b_i=0\}P\{b_{i+1}=1\}=(0,5-\varepsilon)(0,5+\varepsilon)=0,25-\varepsilon^2$;

$P\{b_i\,b_{i+1}=10\}=P\{b_i=1\}P\{b_{i+1}=0\}=(0,5+\varepsilon)(0,5-\varepsilon)=0,25-\varepsilon^2$;

$$P\{b_i\, b_{i+1} = 11\} = P\{b_i = 1\}P\{b_{i+1} = 1\} = (0,5+\varepsilon)^2 = 0,25+\varepsilon+\varepsilon^2.$$

б) оскільки у послідовності S виникнення біграм 01 і 10 рівноймовірне, то й у послідовності S_1 поява нульових і одиничних бітів також рівноймовірна.

в) N бітів послідовності S_1 утворюються з $2N$ збережених бітів послідовності S. Нехай спочатку послідовність S нараховувала n бітів. Імовірність бути відкинутою для будь-якої бітової пари із S дорівнює

$$P\{b_i\, b_{i+1} = 00\} + P\{b_i\, b_{i+1} = 11\} = 0,25-\varepsilon+\varepsilon^2+0,25+\varepsilon+\varepsilon^2 = 0,5+2\varepsilon^2.$$

Отже, після відкидання $n(0,5+2\varepsilon^2)$ у послідовності S залишиться $n(0,5-2\varepsilon^2)$ бітів. Тоді

$$n(0,5-2\varepsilon^2) = 2N \quad \Rightarrow \quad n = \frac{2N}{0,5-2\varepsilon^2} = \frac{N}{0,25-\varepsilon^2} \text{ бітів.}$$

Задача 14. Чи буде періодична послідовність з періодом 000100110101111 задовольняти постулатам Голомба?

Р о з в' я з а н н я. Постулати Голомба – основні вимоги до статистичних властивостей періодичних псевдовипадкових послідовностей. За першим постулатом Голомба кількість одиниць на періоді послідовності має відрізнятися від кількості нулів не більше, ніж на одиницю. У даній послідовності біт «0» зустрічається сім разів, а біт «1» – вісім разів, отже, перший постулат виконується.

Як того вимагає другий постулат, половина відрізків повинна мати довжину $s=1$, чверть відрізків – довжину $s=2$, восьма частина відрізків – довжину $s=3$ і т.д., де під відрізком довжини s розуміють підпослідовність даної послідовності з s однакових символів, обмежену іншими символами (наприклад, блок $0\overbrace{11...1}^{s}0$ або лакуна $1\overbrace{00...0}^{s}1$). У заданій послідовності можна виділити вісім відрізків:

- чотири відрізка довжиною 1 (два блока починаються у позиціях 3 і 9 та дві лакуни у позиціях 8 і 10), частота появи 1/2;
- два відрізка довжиною 2 (блок починається у позиції 4 та лакуна у позиції 6), частота появи 1/4;
- один відрізок довжиною 3 (лакуна у позиції 0), частота появи 1/8;
- один відрізок довжиною 5 (блок у позиції 11), частота появи 1/8.

Таким чином, другий постулат виконується.

Функція

$$AC(d) = \frac{1}{T}\sum_{i=0}^{T-1}(2x_i - 1)(2x_{i+d} - 1),\ 0 \le d \le T-1,$$

називається функцією автокореляції послідовності $\{x_0, x_1, ..., x_{T-1}\}$ з періодом T. За третім постулатом ця функція має бути двозначною.

При $d = 0$

$$AC(0) = \frac{1}{T}\sum_{i=0}^{T-1}(2x_i - 1)^2 = \frac{1}{15}\left((2\cdot 0 - 1)^2 + (2\cdot 0 - 1)^2 + ... + (2\cdot 1 - 1)^2\right) = 1.$$

Очевидно, що

$(2x_i - 1)(2x_{i+d} - 1) = -1$ при $x_i = 0,\ x_{i+d} = 1$ або $x_i = 1,\ x_{i+d} = 0$;

$(2x_i - 1)(2x_{i+d} - 1) = 1$ при $x_i = 0,\ x_{i+d} = 0$ або $x_i = 1,\ x_{i+d} = 1$.

Тому для обчислення інших значень функції автокореляції зручно порівняти задану послідовність з її копіями, зсунутими на d бітів, і підрахувати кількість збіжних і незбіжних пар бітів (табл. 4.4).

Таблиця 4.4

Обчислення функції автокореляції

d	Послідовність	Кількість збіжних пар	Кількість незбіжних пар	$AC(d)$
0	**000100110101111**	15	0	0
1	001001101011110	7	8	– 1/15
2	010011010111100	7	8	– 1/15
3	100110101111000	7	8	– 1/15
4	001101011110001	7	8	– 1/15
5	011010111100010	7	8	– 1/15
6	110101111000100	7	8	– 1/15
7	101011110001001	7	8	– 1/15
8	010111100010011	7	8	– 1/15
9	101111000100110	7	8	– 1/15
10	011110001001101	7	8	– 1/15
11	111100010011010	7	8	– 1/15
12	111000100110101	7	8	– 1/15
13	110001001101011	7	8	– 1/15
14	100010011010111	7	8	– 1/15

Отже, функція автокореляції двозначна і третій постулат виконується.

Задача 15. Чи проходить послідовність

0100001010010111100000100111010000001010000010010,

частотний (монобітовий), серійний (двобітовий) тести, покер-тест, тест на «дірки» та автокореляційний тест?

Р о з в' я з а н н я. Висунемо гіпотезу Н={дана послідовність випадкова}.

1. Частотний тест (монобітовий тест). Мета тесту – перевірити рівномірність появи «0» і «1» у послідовності. Загальна кількість бітів $n = 50$. Обчислимо різницю $n_0 - n_1$ між кількістю «0» і «1»:

$$n_0 - n_1 = 33 - 17 = 16$$

і величину статистики

$$X_1 = \frac{(n_0 - n_1)^2}{n} = \frac{16^2}{50} = 5{,}12.$$

При $n \geq 10$ статистика має наближатися до розподілу χ^2 з одним ступенем свободи. Порівнюємо обчислене значення X_1 з критичним значенням $\chi^2(1;\, 0{,}05) = 3{,}84$ при рівні значущості $\alpha = 0{,}05$:

$$X_1 = 5{,}12 > \chi^2(1; 0{,}05).$$

Отже, послідовність не проходить монобітовий тест.

2. Серійний тест (двобітовий тест). Нехай n_0, n_1 – кількість появбітів «0» і «1» у досліджуваній послідовності, $n_{00}, n_{01}, n_{10}, n_{11}$– кількість появбіграм 00, 01, 10, 11 відповідно (біграми можуть перетинатися). Мета тесту – визначити, чи будуть ці кількості близькими до їх значень у випадковій послідовності. Використана у тесті статистика

$$X_2 = \frac{4}{n-1}\left(n_{00}^2 + n_{01}^2 + n_{10}^2 + n_{11}^2\right) - \frac{2}{n}\left(n_0^2 + n_1^2\right) + 1$$

у нашому випадку становить

$$X_2 = \frac{4}{50-1}\left(21^2 + 12^2 + 11^2 + 5^2\right) - \frac{2}{n}\left(33^2 + 17^2\right) + 1 = 5{,}55.$$

Якщо $n \geq 21$, то результат можна аналізувати за допомогою критерію χ^2 з двома ступенями свободи. Критичне значення $\chi^2(2;\, 0{,}05) = 5{,}99$ при рівні значущості $\alpha = 0{,}05$. Оскільки

$$X_2 = 5{,}55 < \chi^2(2;0{,}05),$$

то з імовірністю 0,95 послідовність проходить серійний тест.

3. Покер-тест. Нехай m – ціле додатне число, при якому число $k = \left\lfloor \frac{n}{m} \right\rfloor$ задовольняє нерівність $\left\lfloor \frac{n}{m} \right\rfloor \geq 5 \cdot 2^m$. Для заданої послідовності: $n = 50$ – загальна кількість бітів; $\left\lfloor \frac{50}{m} \right\rfloor \geq 5 \cdot 2^m$ при $m = 2$; $k = 25$. Розділимо послідовність на k неперетинних частин, кожна з яких складатиметься з m бітів:

01 00 00 10 10 01 01 11 10 00 00 10 01 11 01 00 00 00 10 10 00 00 10 00 10

(якщо $m = 2$, то частини – звичайні біграми). Підраховуємо:

$n_{00} = 10$ – кількість біграм 00; $n_{01} = 5$ – кількість біграм 01;

$n_{10} = 8$ – кількість біграм 10; $n_{11} = 2$ – кількість біграм 11.

Для тестування використовуємо статистику

$$X_3 = \frac{2^m}{k}\left(\sum_{i=1}^{2^m} n_i^2\right) - k,$$

де n_i – кількість біграм i-го типу. Порівняння експериментального значення $X_3 = \frac{4}{25}\left(10^2 + 5^2 + 8^2 + 2^2\right) - 25 = 5{,}88$ з критичним $\chi^2(3;\, 0{,}05) = 7{,}82$ (число ступенів свободи $2^m - 1 = 2^2 - 1 = 3$)

$$X_3 < \chi^2(3;0{,}05)$$

дозволяє прийняти рішення: з імовірністю 0,95 послідовність проходить покер-тест.

4. Тест на «дірки» виявляє відхилення від рівномірності розподілу «0» та «1» за виявом «дірок» – неперервних відрізків вигляду $0\overbrace{11\ldots1}^{i}0$ або $1\overbrace{00\ldots0}^{i}1$, складених або з i одиниць, або з i нулів. Такі відрізки, як і раніше, називатимемо відповідно блоками та лакунами довжини i. Ймовірність виникнення у випадковій бітовій послідовності «дірки» довжиною i становить $p_i = \frac{1}{2^i}$.

У даній послідовності спостерігаються чотири послідовні одиниці і шість послідовних нулів, тому максимально можлива довжина блоку – 4, а лакуни – 6.

Проміжні розрахунки зводимо у табл. 4.5.

Таблиця 4.5

Розподіл за «дірками»

Тип «дірки»	Довжина «дірки»	Кількість «дірок» (n_i)	Імовірність (p_i)
Блоки (загальна кількість $N=12$)	$i=1$	10	0,5
	$i=2$	0	0,25
	$i=3$	1	0,125
	$i=4$	1	0,0625
Лакуни (загальна кількість $N=13$)	$i=1$	6	0,5
	$i=2$	2	0,25
	$i=3$	1	0,125
	$i=4$	1	0,0625
	$i=5$	2	0,03125
	$i=6$	1	0,015625

Окремо для блоків і лакун сформуємо статистику

$$X_4 = \frac{1}{N}\sum_{i=1}^{k}\left(\frac{n_i^2}{p_i}\right) - N;$$

$$X_{4\,\text{блок}} = \frac{1}{12}\left(\frac{10^2}{0,5} + \frac{0}{0,25} + \frac{1^2}{0,125} + \frac{1^2}{0,0625}\right) - 12 = 6,66;$$

$$X_{4\,\text{лакуна}} = \frac{1}{13}\left(\frac{6^2}{0,5} + \frac{2^2}{0,25} + \frac{1^2}{0,125} + \frac{1^2}{0,0625} + \frac{2^2}{0,03125} + \right.$$

$$\left. + \frac{1^2}{0,015625}\right) = 10,38.$$

Результати оцінимо за допомогою критерію χ^2 при рівні значущості $\alpha = 0,05$ з числом ступенів свободи 3 і 5 відповідно:

$$X_{4\,\text{блок}} < \chi^2(3;0,05) = 7,82;$$

$$X_{4\,\text{лакуна}} < \chi^2(5;0,05) = 11,07.$$

Отже, умови проходження тесту послідовністю успішно виконані в обох випадках.

5. Автокореляційний тест виявляє кореляцію між копіями послідовності, зсунутими одна відносно однієї, що можливо при наявності однакових повторювальних відрізків послідовності. Для $1 \le d \le \lfloor n/2 \rfloor$ підрахуємо кількість збіжних бітів в однакових позиціях у вихідній послідовності і її зсунутій копії:

$$AC(d) = \sum_{i=0}^{n-d-1} x_i \oplus x_{i+d},$$

де d – значення зсуву. При $n - d \ge 10$ статистика

$$X_5 = \frac{2\left(AC(d) - \frac{n-d}{2}\right)}{\sqrt{n-d}}$$

наближено має $N(0,1)$ нормальний розподіл з нульовим середнім та одиничною дисперсією. Наприклад, при $d = 5$

01000010 10010111100000100111010000001010000010001001000001010010111100000100111010000001010000010001,

$$X_5 = \frac{2\left(22 - \frac{50-5}{2}\right)}{\sqrt{50-5}} \approx -0{,}149.$$

За таблицею квантилів стандартного нормального розподілу визначаємо, що на рівні значущості $\alpha = 0{,}05$ обчислена статистика належіть області прийняття гіпотези: $-1{,}64 < X_5 = -0{,}149 < 1{,}64$. Таким чином, висунута гіпотеза H={послідовність випадкова} при зсуві $d = 5$ не суперечить експериментальним даним.

Задача 16. Два рядки з вірша відомої української поетеси Ліни Костенко перетворили на числове повідомлення, вилучивши пропуски між словами та замінивши кожну букву тексту на її двоцифровий номер згідно з підстановкою:

А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

Далі для шифрування використали модульне гамування $y_i = x_i + t_i (\mathrm{mod}\, 31)$, де x_i – цифрове шифропозначення букв відкритого тексту, t_i – знаки гами, утворені згідно з рівнянням рекурсії $t_{i+3} = t_i + t_{i+2} (\mathrm{mod}\, 31)$, $i = 0,1,2,...$ Після переведення числових знаків шифротексту у буквений еквівалент отримали

ЮОТДЄІПТЯЖМТЩЗКД**ГБГ**
ЙШЕММЮМЄОЩЯРДІРЛХЛІЮ**ВЮЧ.**

Визначте три перших знаки гами t_0, t_1, t_2 за умови, що через риму три останніх літери відкритих рядків вірша збігаються. Відновіть вірш.

Р о з в’ я з а н н я. Числовий еквівалент шифротексту має вигляд:

29 16 20 5 6 10 17 20 30 7 14 20 27 8 12 4 **3 1 3**
11 26 5 14 14 29 14 6 16 27 30 18 4 10 18 13 23 13 10 29 **2 29 25**

$x_{16}; x_{17}; x_{18}$ і $x_{39}; x_{40}; x_{41}$ – три останні букви у першому та другому рядках відповідно. Якщо виразити знаки гами $t_{16}; t_{17}; t_{18}$; $t_{39}; t_{40}; t_{41}$ через t_0, t_1, t_2, то врахувавши умову $x_{16} = x_{39}$, $x_{17} = x_{40}$, $x_{18} = x_{41}$, можна буде виразити й різниці знаків шифротексту $y_{16} - y_{39}$, $y_{17} - y_{40}$, $y_{18} - y_{41}$ через t_0, t_1, t_2.

Потрібні знаки гами дістаємо за законом рекурсії

$$t_{i+3} = t_i + t_{i+2} (\mathrm{mod}\, 31):$$

$t_3 = t_0 + t_2$;
$t_4 = t_3 + t_1 = t_0 + t_1 + t_2$;
$t_5 = t_4 + t_2 = t_0 + t_1 + 2t_2$;
$t_6 = t_5 + t_3 = 2t_0 + t_1 + 3t_2$;
$t_7 = t_6 + t_4 = 3t_0 + 2t_1 + 4t_2$;
$t_8 = t_7 + t_5 = 4t_0 + 3t_1 + 6t_2$;
$t_9 = t_8 + t_6 = 6t_0 + 4t_1 + 9t_2$;
$t_{10} = t_9 + t_7 = 9t_0 + 6t_1 + 13t_2$;
$t_{11} = t_{10} + t_8 = 13t_0 + 9t_1 + 19t_2$;
$t_{12} = t_{11} + t_9 = 19t_0 + 13t_1 + 28t_2$;
$t_{13} = t_{12} + t_{10} = 28t_0 + 19t_1 + 10t_2$;
$t_{14} = t_{13} + t_{11} = 10t_0 + 28t_1 + 29t_2$;
$t_{15} = t_{14} + t_{12} = 29t_0 + 10t_1 + 26t_2$;
$t_{16} = t_{15} + t_{13} = 26t_0 + 29t_1 + 5t_2$;

$t_{23} = t_{22} + t_{20} = 7t_0 + 4t_1 + 13t_2$;
$t_{24} = t_{23} + t_{21} = 13t_0 + 7t_1 + 17t_2$;
$t_{25} = t_{24} + t_{22} = 17t_0 + 13t_1 + 24t_2$;
$t_{26} = t_{25} + t_{23} = 24t_0 + 17t_1 + 6t_2$;
$t_{27} = t_{26} + t_{24} = 6t_0 + 24t_1 + 23t_2$;
$t_{28} = t_{27} + t_{25} = 23t_0 + 6t_1 + 16t_2$;
$t_{29} = t_{28} + t_{26} = 16t_0 + 23t_1 + 22t_2$;
$t_{30} = t_{29} + t_{27} = 22t_0 + 16t_1 + 14t_2$;
$t_{31} = t_{30} + t_{28} = 14t_0 + 22t_1 + 30t_2$;
$t_{32} = t_{31} + t_{29} = 30t_0 + 14t_1 + 21t_2$;
$t_{33} = t_{32} + t_{30} = 21t_0 + 30t_1 + 4t_2$;
$t_{34} = t_{33} + t_{31} = 4t_0 + 21t_1 + 3t_2$;
$t_{35} = t_{34} + t_{32} = 3t_0 + 4t_1 + 24t_2$;
$t_{36} = t_{35} + t_{33} = 24t_0 + 3t_1 + 28t_2$;

$t_{17} = t_{16} + t_{14} = 5t_0 + 26t_1 + 3t_2;$ $t_{37} = t_{36} + t_{34} = 28t_0 + 24t_1;$

$t_{18} = t_{17} + t_{15} = 3t_0 + 5t_1 + 29t_2;$ $t_{38} = t_{37} + t_{35} = 28t_1 + 24t_2;$

$t_{19} = t_{18} + t_{16} = 29t_0 + 3t_1 + 3t_2;$ $t_{39} = t_{38} + t_{36} = 24t_0 + 21t_2;$

$t_{20} = t_{19} + t_{17} = 3t_0 + 29t_1 + 6t_2;$ $t_{40} = t_{39} + t_{37} = 21t_0 + 24t_1 + 21t_2;$

$t_{21} = t_{20} + t_{18} = 3t_0 + 29t_1 + 6t_2;$ $t_{41} = t_{40} + t_{38} = 21t_0 + 21t_1 + 14t_2.$

$t_{22} = t_{21} + t_{19} = 4t_0 + 6t_1 + 7t_2;$

$$y_{16} - y_{39} = 3 - 2 = 1;$$

$$y_{16} - y_{39} = x_{16} + t_{16} - (x_{39} + t_{39}) = t_{16} - t_{39} = 26t_0 + 29t_1 + 5t_2 -$$
$$-24t_0 - 21t_2 = 2t_0 + 29t_1 - 16t_2 \Rightarrow 2t_0 + 29t_1 - 16t_2 \equiv 1(\mathrm{mod}\,31);$$

$$y_{17} - y_{40} = 1 - 29 = -28;$$

$$y_{17} - y_{40} = x_{17} + t_{17} - (x_{40} + t_{40}) = t_{17} - t_{40} = 5t_0 + 26t_1 + 3t_2 -$$
$$-21t_0 - 24t_1 - 21t_2 = -16t_0 + 2t_1 - 18t_2 \quad \Rightarrow$$
$$-16t_0 + 2t_1 - 18t_2 \equiv -28(\mathrm{mod}\,31);$$

$$y_{18} - y_{41} = 3 - 25 = -22;$$

$$y_{18} - y_{41} = x_{18} + t_{18} - (x_{41} + t_{41}) = t_{18} - t_{41} = 3t_0 + 5t_1 + 29t_2 -$$
$$-21t_0 - 21t_1 - 14t_2 = -18t_0 - 16t_1 + 15t_2 \quad \Rightarrow$$
$$-18t_0 - 16t_1 + 15t_2 \equiv -22(\mathrm{mod}\,31).$$

Приходимо до системи порівнянь

$$\begin{cases} 2t_0 + 29t_1 - 16t_2 \equiv 1(\mathrm{mod}\,31), \\ -16t_0 + 2t_1 - 18t_2 \equiv -28(\mathrm{mod}\,31), \\ -18t_0 - 16t_1 + 15t_2 \equiv -22(\mathrm{mod}\,31). \end{cases}$$

Шукаємо розв'язок у полі Z_{31} методом Гаусса.

$$A^* = \left(\begin{array}{ccc|c} -2 & -29 & 16 & -1 \\ 16 & -2 & 18 & 28 \\ 18 & 16 & -15 & 22 \end{array}\right) \sim \left(\begin{array}{ccc|c} -2 & -29 & 16 & -1 \\ 0 & -17 & 22 & 20 \\ 0 & -28 & 5 & 13 \end{array}\right) \sim \left\{\begin{array}{l} -17^{-1} \equiv 14^{-1} \equiv \\ \equiv 20 \bmod 31 \end{array}\right\} \sim$$

$$\sim \left(\begin{array}{ccc|c} -2 & -29 & 16 & -1 \\ 0 & 1 & 6 & 28 \\ 0 & -28 & 5 & 13 \end{array}\right) \sim \left(\begin{array}{ccc|c} -2 & -29 & 16 & -1 \\ 0 & 1 & 6 & 28 \\ 0 & 0 & 18 & 22 \end{array}\right)$$

$$\Rightarrow \begin{cases} 2t_0 + 29t_1 - 16t_2 \equiv 1 (\mathrm{mod}\, 31), \\ t_1 + 6t_2 \equiv 28 (\mathrm{mod}\, 31), \\ 18t_2 \equiv 22 (\mathrm{mod}\, 31). \end{cases}$$

$$18^{-1} \equiv 19 (\mathrm{mod}\, 31) \Rightarrow \quad t_2 \equiv 19 \cdot 22 (\mathrm{mod}\, 31) \equiv 15 (\mathrm{mod}\, 31);$$

$$t_1 \equiv -6t_2 + 28 (\mathrm{mod}\, 31) \equiv -6 \cdot 15 + 28 \equiv 0 (\mathrm{mod}\, 31);$$

$$2t_0 \equiv 1 - 29 \cdot 0 + 16 \cdot 12 (\mathrm{mod}\, 31) \equiv 241 (\mathrm{mod}\, 31);$$

$$2^{-1} \equiv 16 (\mathrm{mod}\, 31) \Rightarrow \quad t_0 \equiv 241 \cdot 16 (\mathrm{mod}\, 31) \equiv 12 (\mathrm{mod}\, 31);$$

Отже, $t_0 = 12; t_1 = 0; t_2 = 15$. За таких початкових умов генеруємо гаму

12 0 15 27 27 11 7 3 14 21 24 7 28 21 28 25
15 12 6 21 2 8 29 0 8 6 6 14 20 26 9 29
24 2 0 24 26 26 19 14 9 28.

У відповідності з рівнянням розшифрування визначаємо відкритий текст

17 16 5 8 10 30 10 17 16 17 21 13 30 18 15
10 19 20 28 21 24 28 16 14 21 8 0 2 7 4
9 6 17 16 13 30 18 15 10 19 20 28

або

ПОЕЗІЯ І ПОПУЛЯРНІСТЬ –
У ЦЬОМУ ЗАВЖДИ Є ПОЛЯРНІСТЬ.

Задача 17. Ключовий бітовий потік утворюється з послідовності, генерованої лінійним конгруентним генератором $x_{i+1} = ax_i + d (\mathrm{mod}\, 8)$. При цьому елементи x_i інтерпретуються як трибітові числа $b_{i2}b_{i1}b_{i0}$ (запис від старших бітів до молодших), тобто

$$\{x_i\} = x_0, x_1, ..., x_i, ... = b_{02}b_{01}b_{00}b_{12}b_{11}b_{10}...b_{i2}b_{i1}b_{i0}...,$$

де $x_i = \sum_{k=0}^{2} b_{ik} 2^k$. У результаті виконання операції XOR над бітами утвореної таким чином послідовності та бітами відкритого тексту M отримано шифротекст

$$C = 111\ \ 101\ \ 100\ \ 101\ \ 101\ \ 010\ \ 111.$$

Відновіть відкритий текст за умови, що його перші дев'ять бітів

100 111 001.

Р о з в’ я з а н н я. Перші дев’ять бітів ключового потоку дістанемо, виконавши операцію XOR над бітами відкритого тексту і шифротексту:

$$\begin{array}{r} 111\,101\,100 \\ \oplus\; 100\,111\,001 \\ \hline 011\,010\,101. \end{array}$$

Звідси визначаємо $x_0 = 011_2 = 3;\ x_1 = 010_2 = 2; x_2 = 101_2 = 5$.

Із рівняння $x_{i+1} = ax_i + d (\mathrm{mod}\, 8)$ випливає

$$x_1 = ax_0 + d (\mathrm{mod}\, 8); \quad x_2 = ax_1 + d (\mathrm{mod}\, 8).$$

Тоді

$$\begin{cases} 2 \equiv 3a + d \bmod 8, \\ 5 \equiv 2a + d \bmod 8 \end{cases} \Rightarrow \begin{cases} a \equiv 5 \bmod 8, \\ d \equiv 3 \bmod 8. \end{cases}$$

За цими параметрами лінійний конгруентний генератор породжує послідовність 3, 2, 5, 4, 7, 6, 1. Інтерпретація цих елементів як трибітових чисел дає ключовий потік 011 010 101 100 111 110 001. Тепер відновимо відкритий текст, накладаючи його на шифротекст:

$$\begin{array}{r} 111\,101\,100\,101\,101\,010\,111 \\ \oplus\; 011\,010\,101\,100\,111\,110\,001 \\ \hline 100\,111\,001\,001\,010\,100\,110 = (4,7,1,1,2,4,6). \end{array}$$

Задача 18. Як відомо, непроходження графічного спектрального тесту лінійним конгруентним генератором RANDU, широко розповсюдженим на мейнфреймах IBM у 1960 – 1970 рр., спричинив некоректний вибір параметрів генератора. Виявилось, що точки (x_i, x_{i+1}, x_{i+2}), де x_i, x_{i+1}, x_{i+2} – три послідовні елементи генерованої послідовності, лежать у просторі на 15 паралельних площинах. Знайдіть кореляцію між x_i, x_{i+1}, x_{i+2}, якщо закон рекурсії генератора $x_{i+1} = 65539 x_i (\mathrm{mod}\, 2^{31})$, $i = 1, 2, ...$

Р о з в’ я з а н н я.

$$x_{i+2} \equiv 65539 x_{i+1} (\mathrm{mod}\, 2^{31}) \equiv (2^{16} + 3) x_{i+1} (\mathrm{mod}\, 2^{31}) \equiv (2^{16} + 3)^2 x_i \equiv$$

$$\equiv (2^{32} + 6 \cdot 2^{16} + 9) x_i (\mathrm{mod}\, 2^{31}) \equiv (0 + 6 \cdot (2^{16} + 3) - 9) x_i (\mathrm{mod}\, 2^{31}),$$

$$\Rightarrow \quad x_{i+2} \equiv 6x_{i+1} - 9x_i (\mathrm{mod}\, 2^{31}).$$

Задача 19. Під час відвідування веб-сайту сервер залишає на комп'ютері клієнта HTTP-кукі для його аутентифікації при поверненні на сайт. До складу кукі входить псевдовипадкове число, генероване лінійним конгруентним генератором. При вході клієнта в систему

- за допомогою системного годинника визначається момент входу, дробова частка останньої зафіксованої секунди, виражена у мілісекундах (інтервал від 0 до 999), подається на генератор як початкове заповнення x_0;
- генератор видає значення $x_1 \equiv 1103515245x_0 + 12345 \pmod{2^{31}}$, яке використовується для ідентифікації клієнта і зберігається в кукі.

При роботі системи в Інтернеті виявилось, що деякі користувачі отримали для ідентифікації такі самі псевдовипадкові числа, як і ідентифікатор сеансу. Аналіз списку більше ніж 3000 ідентифікаторів сесії виявив, що найменше значення у списку було 12345, а найбільше – 2144992058. Наприклад, частина списку виглядала так:

8222774625, 8222774625, 827365286, 829860997, 829860997,
829860997, 833686131, 833686131, 834961534, 842565209,
843848608, 843848608, 843848608, 843848608, 846355324, …

У чому причина повторення значень?

Р о з в' я з а н н я. За умовою задачі на вхід генератора може бути передано тільки 1000 різних початкових заповнень x_0, тому існуватиме тільки 1000 різних ідентифікаторів клієнтських сесій. Якщо не змінювати початкове заповнення генератора, то генеровані члени послідовності почнуть повторюватися тільки тоді, коли буде пройдено увесь період.

Задача 20. Відомо, що четвертий та дванадцятий біти відкритого тексту є «0», а восьмий і шістнадцятий біти дорівнюють «1». У результаті побітового підсумовування цього відкритого тексту з послідовністю, генерованою LFSR з многочленом зворотного зв'язку $x^4 + x^3 + x^2 + x + 1$, виник шифрований текст 1110110111100010. Знайдіть початкове заповнення LFSR.

Р о з в' я з а н н я. За умовою

1 1 1 0 1 1 0 1 1 1 1 1 0 0 0 1 0 – шифротекст;
- - - 0 - - - 1 - - - 0 - - - 1– відкритий текст;
- - - 0 - - - 0 - - - 0 - - - 1– ключовий потік.

Порядок многочлена $x^4 + x^3 + x^2 + x + 1$ дорівнює 5, бо у полі $GF(2)$ виконується рівність $(x+1)(x^4 + x^3 + x^2 + x + 1) = x^5 + 1$. Тому період генерованих LFSR послідовностей має ділити число 5, тобто

може дорівнювати лише 1 або 5. Це еквівалентно умові $Z_i = Z_{i+5}$ для всіх $i = 1, 2, ...$ (тривіальний період відкидаємо). Звідси визначимо: $Z_4 = Z_9 = Z_{14} = 0$; $Z_3 = Z_8 = Z_{13} = 0$; $Z_2 = Z_7 = Z_{12} = 0$; $Z_1 = Z_6 = Z_{11} = Z_{16} = 1$. Отже, стають відомими більшість бітів ключового потоку: 1 0 0 0 - 1 0 0 0 - 1 0 0 0 – 1 і початкове заповнення регістру – 1 0 0 0.

Задача 21. LFSR генерує псевдовипадкову гаму x_i, що накладається на біти m_i відкритого тексту: $c_i = m_i \oplus x_i$. Многочлен зворотного зв'язку $f(x) = x^6 + x^4 + x^2 + x + 1$ даного регістру є незвідним і НСД $(f(x),\ x^{21} - 1) \neq 1$. Запишіть рівняння рекурсії для гами та визначте початкове заповнення LFSR за умови, що відомі деякі пари (m_i, c_i) бітів відкритого тексту і відповідного шифротексту :

$$(m_{65}, c_{65}) = 00; \quad (m_{66}, c_{66}) = 01; \quad (m_{84}, c_{84}) = 10;$$

$$(m_{85}, c_{85}) = 11; \quad (m_{109}, c_{109}) = 01; \quad (m_{110}, c_{110}) = 10.$$

Р о з в' я з а н н я. Закон рекурсії для генерованої послідовності запишемо на основі даного многочлена зворотного зв'язку LFSR :

$$x_i = x_{i-2} + x_{i-4} + x_{i-5} + x_{i-6}.$$

За відомими парами бітів відкритого і шифрованого тексту знаходимо відповідні біти гами:

$$x_{65} = m_{65} \oplus c_{65} = 0 \oplus 0 = 0; \quad x_{66} = m_{66} \oplus c_{66} = 0 \oplus 1 = 1;$$

$$x_{84} = m_{84} \oplus c_{84} = 1 \oplus 0 = 1; \quad x_{85} = m_{85} \oplus c_{85} = 1 \oplus 1 = 0;$$

$$x_{109} = m_{109} \oplus c_{109} = 0 \oplus 1 = 1; \quad x_{110} = m_{110} \oplus c_{110} = 1 \oplus 0 = 1.$$

Із умови НСД $(f(x),\ x^{21} - 1) \neq 1$ випливає, що $x^{21} - 1$ ділиться на $f(x)$, елемент x має порядок 21 у полі і період генерованої послідовності дорівнюватиме 21. Тоді

$$x_0 = x_{84} = 1; \quad x_1 = x_{85} = 0; \quad x_2 = x_{65} = 0;$$

$$x_3 = x_{66} = 1; \quad x_4 = x_{109} = 1; \quad x_5 = x_{110} = 1.$$

Отже, початкове заповнення регістру – 100111.

Задача 22. У шифрі гамування зашифрування здійснюється згідно з рівнянням $c_i = m_i \oplus k_i'$, $i = 1, 2, ...$, де m_i, c_i – біти відкритого тексту та

шифротексту відповідно, а знаки гами $k_1', k_2', \ldots$ утворені із вихідної послідовності $\{k_i\}$ LFSR за допомогою правила $k_i' = k_{3i}$, $i = 1, 2, \ldots$ Використаний LFSR має довжину 5 та багаточлен зворотного зв'язку $C(D) = 1 + D^2 + D^5$. Відновіть невідомі біти $m_6, m_7, m_8, m_9, m_{10}$ відкритого тексту $1,1,1,1,1, m_6, m_7, m_8, m_9, m_{10}$, якщо повідомленню відповідає шифротекст 0,1,1,1,1,1,0,1,0,1.

Р о з в' я з а н н я. За умовою $c_1 = 0,\ c_2 = c_2 = c_3 = c_4 = c_5 = 1$.

$$k_i' = c_i \oplus m_i \Rightarrow k_1' = c_1 \oplus m_1 = 0 + 1 = 1;$$

$k_j' = c_j \oplus m_j = 1 + 1 = 0$, де $j = 2,3,4,5$, тобто $k_2' = k_3' = k_4' = k_5' = 0$.

Це дає змогу визначити деякі біти вихідної послідовності LFSR:

$$k_3 = k_1' = 1;$$
$$k_6 = k_9 = k_{12} = k_{15} = 0.$$

Для $i \geq 6$ маємо $k_i = k_{i-5} \oplus k_{i-2}$. Отже

k_1; k_2; $\underline{k_3 = 1}$;

k_4; k_5; $k_6 = k_1 \oplus k_4 = 0 \Leftrightarrow \underline{k_4 = k_1}$;

$k_7 = k_2 \oplus k_5$; $k_8 = k_3 \oplus k_6 = 1$; $k_9 = k_4 \oplus k_7 = \underline{k_1 \oplus k_2 \oplus k_5 = 0}$;

$k_{10} = k_5 \oplus k_8 = k_5 \oplus 1$; $k_{11} = k_6 \oplus k_9 = 0$; $k_{12} = k_7 \oplus k_{10} = k_2 \oplus k_5 \oplus k_5 \oplus 1 = 0$
$\Leftrightarrow \underline{k_2 = 1}$;

$k_{13} = k_8 \oplus k_{11} = 1$; $k_{14} = k_9 \oplus k_{12} = 0$; $k_{15} = k_{10} \oplus k_{13} = k_5 \oplus 1 \oplus 1 = 0$
$\Leftrightarrow \underline{k_5 = 0}$.

Початкове заповнення $k_1, 1, 1, k_1, 0$. Але $k_4 \oplus k_2 \oplus k_5 = 0$, тому $\underline{k_1 = k_4 = 1}$.

Для відновлення відкритого тексту потрібно знати 30 перших членів вихідної послідовності LFSR при початковому заповненні 11101 – це 111 100 110 100 100 001 010 111 011 000. Остаточно отримаємо $\{k'\} = 1,0,0,0,0,1,0,1,1,0$. Тоді відкритий текст 1,1,1,1,1,0,0,0,1,1.

Задача 23. 5-бітовий LFSR генерує вихідну псевдовипадкову послідовність 1110100010. Знайдіть наступні три біти.

Р о з в' я з а н н я. У загальному випадку рівняння рекурсії, що описує роботу 5-бітового LFSR, має вигляд

$$x_{i+5} = a_4 x_{i+4} + a_3 x_{i+3} + a_2 x_{i+2} + a_1 x_{i+1} + a_0 x_i, \quad i = 0,1,...$$

$$i = 0 \Rightarrow x_5 = a_4 x_4 + a_3 x_3 + a_2 x_2 + a_1 x_1 + a_0 x_0;$$
$$i = 1 \Rightarrow x_6 = a_4 x_5 + a_3 x_4 + a_2 x_3 + a_1 x_2 + a_0 x_1;$$
$$i = 2 \Rightarrow x_7 = a_4 x_6 + a_3 x_5 + a_2 x_4 + a_1 x_3 + a_0 x_2;$$
$$i = 3 \Rightarrow x_8 = a_4 x_7 + a_3 x_6 + a_2 x_5 + a_1 x_4 + a_0 x_3;$$
$$i = 4 \Rightarrow x_9 = a_4 x_8 + a_3 x_7 + a_2 x_6 + a_1 x_5 + a_0 x_4.$$

Пронумеруємо біти від 0 до 9 ($x_0 = 1,\ x_1 = 1,\ldots,\ x_9 = 0$) і підставимо в рівняння

$$\begin{cases} a_4 + a_2 + a_1 + a_0 = 0, \\ a_3 + a_1 + a_0 = 0, \\ a_2 + a_0 = 0, \\ a_1 = 1, \\ a_4 + a_0 = 0. \end{cases}$$

Розв'яжемо систему методом виключення, виконуючи еквівалентні перетворення розширеної матриці системи A^* в полі $GP(2)$:

$$A^* = \left(\begin{array}{ccccc|c} 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \end{array}\right) \sim \left(\begin{array}{ccccc|c} 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{array}\right).$$

$$\begin{cases} a_4 + a_2 + a_1 + a_0 = 0, \\ a_3 + a_1 + a_0 = 0, \\ a_2 + a_0 = 0, \\ a_1 = 1, \\ a_2 + a_1 = 0. \end{cases} \Rightarrow \begin{array}{l} a_1 = a_0 = a_2 = a_4 = 1; \\ a_3 = 0. \end{array}$$

Закон рекурсії має вигляд $x_{i+5} = x_{i+4} + x_{i+2} + x_{i+1} + x_i, \quad i = 0,1,...$ За цим законом наступні три біти – це 010.

Задача 24. Гама $k_1k_2k_3k_4k_5k_1k_2k_3k_4k_5k_1k_2k_3k_4k_5...$для шифру гамування формується повторенням випадково генерованого бітового рядка з п'яти бітів. Визначте відстань єдиності шифру, прийнявши, що надлишковість відкритого тексту складає D. Припустимо, що відкритий текст – рядок бітів, утворений за правилом: спочатку два біти вибираються випадково, а третій біт визначається як сума за $\mathrm{mod}\,2$

вибраних бітів. У результаті п'ятикратного повторення такої процедури виник відкритий текст, на який далі накладено зазначену гаму і отримано шифротекст 010101111100001. Знайдіть ключ $k_1k_2k_3k_4k_5$.

Р о з в' я з а н н я. Відстань єдиності шифру

$$L=\frac{\log_2|K|}{D\log_2|P|}=\frac{\log_2\left|2^5\right|}{D\log_2 2}=\frac{5}{D},$$

де $|K|$ – потужність простору ключів, $|P|$ – потужність використаного алфавіту.

Рівняння розшифрування $m_i=c_i+k_i$, $i=1,2,...$, де m_i,c_i,k_i – біти відкритого тексту, шифротексту і ключового потоку відповідно. Надлишковість відкритого тексту полегшує криптоаналіз, оскільки кожен третій біт відкритого тексту виражається лінійно через два інші біти: 100001

$$\begin{cases}m_3=m_1\oplus m_2=(c_1\oplus k_1)\oplus(c_1\oplus k_2)=0\oplus k_1\oplus 1\oplus k_2=k_1\oplus k_2\oplus 1;\\ m_3=c_3\oplus k_3=0\oplus k_3=k_3;\end{cases}$$

$$\begin{cases}m_6=m_4\oplus m_5=(c_4\oplus k_4)\oplus(c_5\oplus k_5)=1\oplus k_4\oplus 0\oplus k_5=k_4\oplus k_5\oplus 1;\\ m_6=c_6\oplus k_6=1\oplus k_1;\end{cases}$$

$$\begin{cases}m_9=m_7\oplus m_8=(c_7\oplus k_7)\oplus(c_8\oplus k_8)=1\oplus k_2\oplus 1\oplus k_3=k_2\oplus k_3;\\ m_9=c_9\oplus k_9=1\oplus k_4;\end{cases}$$

$$\begin{cases}m_{12}=m_{10}\oplus m_{11}=(c_{10}\oplus k_{10})\oplus(c_{11}\oplus k_{11})=1\oplus k_5\oplus 0\oplus k_1=k_5\oplus k_1\oplus 1;\\ m_{12}=c_{12}\oplus k_{12}=k_2;\end{cases}$$

$$\begin{cases}m_{15}=m_{13}\oplus m_{14}=(c_{13}\oplus k_{13})\oplus(c_{14}\oplus k_{14})=0\oplus k_3\oplus 0\oplus k_4=k_3\oplus k_4;\\ m_{15}=c_{15}\oplus k_{15}=1\oplus k_5.\end{cases}$$

$$\begin{cases}k_1\oplus k_2\oplus 1=k_3;\\ k_4\oplus k_5\oplus 1=1\oplus k_1;\\ k_2\oplus k_3=1\oplus k_4;\\ k_5\oplus k_1\oplus 1=k_2;\\ k_3\oplus k_4=1\oplus k_5.\end{cases}\Rightarrow\begin{cases}k_1\oplus k_2\oplus k_3=1;\\ k_1\oplus k_4\oplus k_5=0;\\ k_2\oplus k_3\oplus k_4=1;\\ k_1\oplus k_2\oplus k_5=1;\\ k_3\oplus k_4\oplus k_5=1.\end{cases}\Rightarrow$$

$$\oplus\begin{cases} k_1 \oplus k_2 \oplus k_3 = 1; \\ k_1 \oplus k_4 \oplus k_5 = 0; \\ k_2 \oplus k_3 \oplus k_4 = 1, \end{cases}$$

$$k_5 = 0.$$

$$\oplus\begin{cases} k_1 \oplus k_2 \oplus k_3 = 1; \\ k_1 \oplus k_4 \oplus k_5 = 0; \\ k_3 \oplus k_4 \oplus k_5 = 1. \end{cases}$$

$$k_2 = 0.$$

$$\oplus\begin{cases} k_1 \oplus k_4 \oplus k_5 = 0; \\ k_2 \oplus k_3 \oplus k_4 = 1; \\ k_1 \oplus k_2 \oplus k_5 = 1. \end{cases}$$

$$k_3 = 0.$$

$$\oplus\begin{cases} k_2 \oplus k_3 \oplus k_4 = 1; \\ k_1 \oplus k_2 \oplus k_5 = 1; \\ k_3 \oplus k_4 \oplus k_5 = 1. \end{cases}$$

$$k_1 = 1.$$

$$k_4 = 1 \oplus k_5 \oplus k_3 = 1.$$

Ключ шифру – 10010.

Задача 25. Для кожної з наведених 5-бітових послідовностей обчисліть її лінійну складність та знайдіть, не використовуючи алгоритм Берлекемпа – Мессі, найкоротший LFSR, що генеруватиме послідовність: а) 00111; б) 00011; в) 11100.

Р о з в' я з а н н я. а) Наявність двох послідовних нулів на початку послідовності 00111 вказує на те, що її лінійна складність $L(00111) \geq 3$. Якщо лінійна рекурентна послідовність має третій порядок, то будь який її біт можна виразити рекурентним співвідношенням

$$x_{i+3} = a_0 x_i + a_1 x_{i+1} + a_2 x_{i+2}, \ i = 0,1,...$$

При $i = 0$ та $i = 1$

$$x_3 = a_0 x_0 + a_1 x_1 + a_2 x_2 \ \Rightarrow 1 = a_0 \cdot 0 + a_1 \cdot 0 + a_2 \cdot 1;$$

$$x_4 = a_0 x_1 + a_1 x_2 + a_2 x_3 \ \Rightarrow 1 = a_0 \cdot 0 + a_1 \cdot 1 + a_2 \cdot 1,$$

Звідки $a_2 = 1$ і $a_1 = 0$. Оскільки ми шукаємо повний трибітовий LFSR, то $a_0 = 1$ і тоді мінімальним многочленом регістру може бути $F(\lambda) = \lambda^3 + \lambda^2 + 1$, що відповідає лінійній складності $L(00111) = 3$.

б) Аналогічно розглядаючи другу послідовність, бачимо її складність $L(00011) \geq 4$. Лінійне рекурентне співвідношення четвертого порядку має вигляд

$$x_{i+4} = a_0 x_i + a_1 x_{i+1} + a_2 x_{i+2} + a_3 x_{i+3}, \ i = 0,1,...$$

Якщо $i = 0$, то

$$1 = a_0 \cdot 0 + a_1 \cdot 0 + a_2 \cdot 0 + a_3 \cdot 1,$$

звідки $a_3 = 1$. При $a_0 = 1$ і різних значеннях a_1, a_2 отримаємо чотири розв'язки і відповідно чотири можливих многочлени $F(\lambda) = \lambda^4 + \lambda^3 + a_2\lambda^2 + a_1\lambda + 1$ для LFSR. Лінійна складність $L(00011) = 4$.

в) Ненульова послідовність 11100 містить два послідовних нулі, тому $L(11100) \geq 3$. Тоді

$$x_{i+3} = a_0 x_i + a_1 x_{i+1} + a_2 x_{i+2}, \quad i = 0,1,...$$

$$x_3 = a_0 x_0 + a_1 x_1 + a_2 x_2 \quad \Rightarrow 0 = a_0 \cdot 1 + a_1 \cdot 1 + a_2 \cdot 1;$$

$$x_4 = a_0 x_1 + a_1 x_2 + a_2 x_3 \quad \Rightarrow 0 = a_0 \cdot 1 + a_1 \cdot 1 + a_2 \cdot 0,$$

звідки $a_0 = a_1$ і $a_2 = 0$. Крім того, у випадку повного трибітового LFSR $a_0 = 1$. Таким чином, шуканий многочлен $F(\lambda) = \lambda^3 + \lambda + 1$ і лінійна складність $L(11100) = 3$.

Задача 26. Визначте найкоротший LFSR, який генерує вихідну бітову послідовність 101100001.

Р о з в’ я з а н н я. Користуємось алгоритмом Берлекемпа – Мессі, на вхід якого подається бітова послідовність $X_n = \{x_0, x_1, ..., x_{n-1}\}$ довжини n, а на виході формується мінімальний многочлен $F(\lambda) = 1 + a_1\lambda + a_2\lambda^2 + ... + a_L\lambda^L$ послідовності та визначається її складність $L(X_n)$, $0 \leq L(X_n) \leq n$. За цим алгоритмом потрібно:

1. Задати початкові значення $F(\lambda) = 1;\ L = 0;\ m = -1;$
$G(\lambda) = 1;\quad N = 0.$

2. Поки $N < n$, виконувати дії:

- обчислити $d = (x_N + \sum_{i=1}^{L} a_i x_{N-i}) \bmod 2;$
- якщо $d = 1$, то
  - $T(\lambda) = F(\lambda);\quad F(\lambda) = F(\lambda) + G(\lambda) \cdot \lambda^{N-m};$
  - якщо $2L \leq N$, то $L = N + 1 - L,\ m = N,\ G(\lambda) = T(\lambda).$
- покласти $N = N + 1.$

Роботу алгоритму на кожній ітерації його виконання продемонстровано у таблиці 4.6

Таблиця 4.6

Робота алгоритму Берлекемпа – Мессі

N	x_N	d	$T(\lambda)$	$F(\lambda)$	L	m	$G(\lambda)$
	–	–	–	1	0	-1	1
0	1	1	1	$1+\lambda$	1	0	1
1	0	1	$1+\lambda$	1	1	0	1
2	1	1	1	$1+\lambda^2$	2	2	1
3	1	1	$1+\lambda^2$	$1+\lambda+\lambda^2$	2	2	1
4	0	0	$1+\lambda^2$	$1+\lambda+\lambda^2$	2	2	1
5	0	1	$1+\lambda+\lambda^2$	$1+\lambda+\lambda^2+\lambda^3$	4	5	$1+\lambda+\lambda^2$
6	0	1	$1+\lambda+\lambda^2+\lambda^3$	1	4	5	$1+\lambda+\lambda^2$
7	0	0	$1+\lambda+\lambda^2+\lambda^3$	1	4	5	$1+\lambda+\lambda^2$
8	1	1	1	$1+\lambda^3+\lambda^4+\lambda^5$	5	8	$1+\lambda+\lambda^2$

Таким чином, скінченну послідовність 101100001 може генерувати LFSR, якому відповідає мінімальний многочлен $F(\lambda)=1+\lambda^3+\lambda^4+\lambda^5$, а лінійна складність послідовності дорівнює 5.

Задача 27. Нехай S – бітова послідовність з лінійною складністю L, а $\overline{S}$ – бітова послідовність, отримана S з у результаті інверсії кожного її біта. Доведіть, що лінійна складність послідовності $\overline{S}$ задовольняє нерівність $L(\overline{S}) \le L+1$.

Д о в е д е н н я. Очевидно, $\overline{S} = S \oplus I$, де $I = 11...1...$ – послідовність, складена із одиничних бітів з лінійним многочленом зворотного зв'язку $x+1$. Позначимо через $\Omega(f)$ – множину всіх послідовностей, генерованих LFSR з многочленом $f(x)$ зворотного зв'язку і скористаємося такою ***теоремою***: якщо $h(x)$ – найменше спільне кратне (НСК) многочленів $f(x)$ і $g(x)$, послідовність $S_1 \in \Omega(f)$, послідовність $S_2 \in \Omega(g)$, то їхня сума

$$S_1 \oplus S_2 \in \Omega(h).$$

За цією теоремою послідовність $\overline{S}$ може генерувати LFSR з многочленом $h(x) =$ НСК$(f(x), x+1)$, ступень якого саме більше $L+1$. Відтак, лінійна складність послідовності $L(\overline{S}) \le L+1$, що й треба було довести.

Задача 28. Знайдіть найкоротший LFSR, що генеруватиме всі вихідні послідовності двох інших регістрів LFSR-1 і LFSR-2 з многочленами зворотного зв'язку $f(x) = x^5 + x^4 + 1$ і $g(x) = x^4 + x^2 + 1$ відповідно. Яким буде многочлен $h(x)$ зворотного зв'язку нового LFSR? Визначте порядки всіх многочленів. Якими можуть бути періоди послідовностей в множині $\Omega(h)$ (указівка: використовуйте позначення і теорему задачі 26)?

Р о з в' я з а н н я. Розкладемо многочлени на множники

$$f(x) = x^5 + x^4 + 1 = (x^3 + x + 1)(x^2 + x + 1);$$

$$g(x) = x^4 + x^2 + 1 = (x^2 + x + 1)^2.$$

За зазначеною теоремою LFSR генеруватиме всі вихідні послідовності регістрів LFSR-1 і LFSR-2, якщо його многочлен зворотного зв'язку

$$h(x) = \text{НСК}(f(x), g(x)) = (x^3 + x + 1)(x^2 + x + 1)^2.$$

За умови, що $f(0) \neq 0$, порядком $ord(f(x))$ многочлена $f(x)$ над полем $GF(2)$ дорівнює такому найменшому натуральному числу e, що многочлен $x^e - 1$ ділиться на $f(x)$. Порядок незвідного многочлена степеня m над полем $GF(q)$ має ділити число $q^m - 1$. У нашому випадку порядки множників многочленів зворотного зв'язку дорівнюють:

$$ord(x^3 + x + 1) = 7;$$

$$ord(x^2 + x + 1) = 3;$$

$$ord(x^2 + x + 1)^2 = 6.$$

Порядок добутку попарно взаємно простих ненульових многочленів дорівнює найменшому спільному кратному порядків його множників:

$$\text{НСК}(7,6) = 42 \quad \text{і} \quad ord(h(x)) = 42.$$

Період будь-якої ненульової послідовності з множини $\Omega(h)$ має ділити $ord(h(x))$. Оскільки $42 = 2 \cdot 3 \cdot 7$, то й періоди послідовностей мають ділитися на $2, 3$ і 7.

Задача 29. Простори відкритих текстів і шифротекстів деякого потокового шифру складаються з елементів скінченного поля $F = Z_2[x] / x^4 + x + 1$, а простір ключів – множина $F^* = F \setminus \{0\}$. Алфавіт

відкритих текстів являє собою бітові чотириграми, до складу яких входить один біт «0», а решта бітів – «1». Правило защифрування послідовності x_i чотириграм відкритого тексту має вигляд

$$y_i = x_i \oplus \gamma_i \ , \qquad i = 1,2,...,$$

де $\gamma_i = k^i$ – гама, k – ключ шифру. Якщо третьою чотириграмою шифротексту є $y_3 = 0111 = x^2 + x + 1,$ то які ключі могли використовуватися для зашифрування?

Р о з в' я з а н н я. За умовою $y_3 = x_3 \oplus k^3 = 0111 = x^2 + x + 1$. Якщо врахувати специфіку алфавіту відкритих текстів, то така чотириграма може виникнути тільки за умови, що реалізується одне із значень: $k^3 = 0011;\ k^3 = 0101;\ k^3 = 0110;\ \ k^3 = 1111$. Оскільки потужність $|F^*|$ простору ключів дорівнює $2^4 - 1 = 15,$ то рівняння може мати розв'язки, тільки коли порядок елемента поля справа ділить $|F^*| / 3 = 5$ або що еквівалентно умові: $k \to k^3$ у полі $Z_2[x] / x^4 + x + 1$. Отже, знайдемо куби усіх ненульових елементів поля (табл. 4.7).

Таблиця 4.7

Куби ненульових елементів поля

Ключ k у вигляді двійкового числа та у вигляді многочлена	k^3 у вигляді двійкового числа та у вигляді многочлена
$k = 0001 = 1$	$k^3 = 0001 = 1$
$k = 0010 = x$	$k^3 = x^3 = 1000$
$k = 0011 = x + 1$	$k^3 = (x+1)^3 = x^3 + x^2 + x + 1 = \underline{1111}$
$k = 0100 = x^2$	$k^3 = x^6 = x^3 + x^2 = 1100$
$k = 0101 = x^2 + 1$	$k^3 = (x^2+1)^3 = x^3 + x = 1010$
$k = 0110 = x^2 + x$	$k^3 = (x^2 + x)^3 = 1 = 0001$
$k = 0111 = x^2 + x + 1$	$k^3 = (x^2 + x + 1)^3 = 1 = 0001$
$k = 1000 = x^3$	$k^3 = (x^3)^3 = 1010$
$k = 1001 = x^3 + 1$	$k^3 = (x^3 + 1)^3 = \underline{1111}$
$k = 1010 = x^3 + x$	$k^3 = (x^3 + x)^3 = \underline{1111}$

Продовження табл. 4.7

$k = 1011 = x^3 + x + 1$	$k^3 = (x^3 + x + 1)^3 = 1100$
$k = 1100 = x^3 + x^2$	$k^3 = (x^3 + x^2)^3 = 1000$
$k = 1101 = x^3 + x^2 + 1$	$k^3 = (x^3 + x^2 + 1)^3 = 1010$
$k = 1110 = x^3 + x^2 + x$	$k^3 = (x^3 + x^2 + x)^3 = 1000$
$k = 1110 = x^3 + x^2 + x + 1$	$k^3 = (x^3 + x^2 + x + 1)^3 = 1100$

Аналізуючи таблицю, приходимо до висновку, що $k^3 = 1111$, а можливі значення ключа k – $0011;\ 1001;\ 1010$.

Задача 30. Нехай $\{0,4;\ 0,3;\ 0,2;\ 0,1\}$ і $\{0,35;\ 0,1;\ 0,25;\ 0,3\}$ – розподіл імовірностей знаків 0,1,2 і 3 відповідно у гамах $\{\gamma_i \bmod 4\}$ та $\{\gamma_i' \bmod 4\}$. Знайдіть розподіл імовірностей знаків у гамі $\{k_i\}$, де $k_i = \gamma_i + \gamma_i{}' \bmod 4$, $i = 0,1,...$

Р о з в' я з а н н я.

$$P\{k_i = 0\} = P\{\gamma_i = 0\}P\{\gamma_i{}' = 0\} + P\{\gamma_i = 2\}P\{\gamma_i{}' = 2\} + P\{\gamma_i = 1\}P\{\gamma_i{}' = 3\} +$$

$$+ P\{\gamma_i = 3\}P\{\gamma_i{}' = 1\} = 0,4 \cdot 0,35 + 0,2 \cdot 0,25 + 0,3 \cdot 0,3 + 0,1 \cdot 0,1 = 0,29;$$

$$P\{k_i = 1\} = P\{\gamma_i = 0\}P\{\gamma_i{}' = 1\} + P\{\gamma_i = 1\}P\{\gamma_i{}' = 0\} + P\{\gamma_i = 2\}P\{\gamma_i{}' = 3\} +$$

$$+ P\{\gamma_i = 3\}P\{\gamma_i{}' = 2\} = 0,4 \cdot 0,1 + 0,3 \cdot 0,35 + 0,2 \cdot 0,3 + 0,1 \cdot 0,25 = 0,23;$$

$$P\{k_i = 2\} = P\{\gamma_i = 1\}P\{\gamma_i{}' = 1\} + P\{\gamma_i = 2\}P\{\gamma_i{}' = 0\} + P\{\gamma_i = 0\}P\{\gamma_i{}' = 2\} +$$

$$+ P\{\gamma_i = 3\}P\{\gamma_i{}' = 3\} = 0,3 \cdot 0,1 + 0,2 \cdot 0,35 + 0,4 \cdot 0,25 + 0,1 \cdot 0,3 = 0,23;$$

$$P\{k_i = 3\} = P\{\gamma_i = 3\}P\{\gamma_i{}' = 0\} + P\{\gamma_i = 2\}P\{\gamma_i{}' = 1\} + P\{\gamma_i = 1\}P\{\gamma_i{}' = 2\} +$$

$$+ P\{\gamma_i = 0\}P\{\gamma_i{}' = 3\} = 0,1 \cdot 0,35 + 0,2 \cdot 0,1 + 0,3 \cdot 0,25 + 0,4 \cdot 0,3 = 0,25.$$

Розподіл імовірностей – $(0,29;\ 0,23;\ 0,23;\ 0,25)$.

Задача 31. Ключовий потік утворюється у результаті виконання операції XOR над вихідними послідовностями 17-бітового LFSR-1 і 25-бітового LFSR-2. Ключ шифру – початкові заповнення регістрів (многочлени, утворені з послідовностей відводів регістрів вважаються відомими). Розробіть сценарій атаки на шифр за умови, що Ви перехопили 100 бітів ключового потоку.

Р о з в' я з а н н я. Перший варіант атаки – повний перебір $2^{17+25}=2^{42}$ можливих початкових станів генератора. Запропонуємо більш ефективний підхід:

1. Для кожного з 2^{17} можливих станів LFSR-1 згенеруємо 100 бітів вихідної послідовності цього регістра. Позначимо їх $K_{100}^{(1)}$;
2. Знайдемо перші 100 бітів $K_{100}^{(2)}$ вихідної послідовності, додавши перехоплені біти K_{100} ключового потоку і біти $K_{100}^{(1)}$:
$$K_{100}^{(2)}=K_{100}\oplus K_{100}^{(1)}.$$
3. На другому кроці виникне 2^{17} можливих послідовностей $K_{100}^{(2)}$. Прийнявши перші 25 бітів кожної з них за початкове заповнення LFSR-2, генеруємо вихідні 100 бітів $K_{100}^{(2)}$ регістра. Очевидно, при правильному виборі початкового заповнення регістр видасть біти, що збігатимуться з бітами $K_{100}^{(2)}$, обчисленими на попередньому кроці.

Задача 32. У генераторі Геффе задіяні три LFSR максимальної довжини і нелінійна комбінувальна функція
$$f(l_1,l_2,l_3)=l_1l_2\oplus l_2l_3\oplus l_3$$
(рис. 4.2) Закон рекурсії першого LFSR $x_{5+i}=x_{2+i}+x_i,\ \ i=0,1,...$ Відновіть його початкове заповнення за перехопленим ключовим потоком генератора:

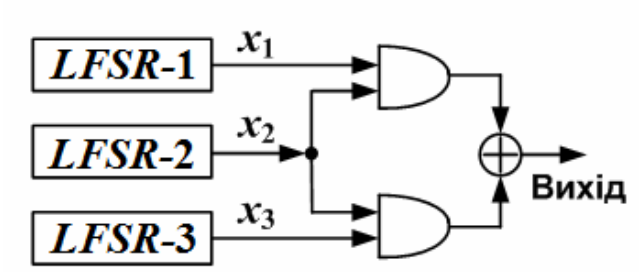


Рис. 4.2

10011111100110101010000010010.

(для кореляційної атаки вибрати порогове значення $T=0,394$).

Р о з в' я з а н н я. Позначивши через x_{1i}, x_{2i}, x_{3i}, γ_i вихідні біти трьох LFSR та гами на виході генератора відповідно, обчислимо кореляційну ймовірність того, що біт гами γ_i збігається з відповідним бітом x_{i1} послідовності на виході першого регістра:
$$P\{\gamma_i=x_{1i}\}=P\{x_{2i}=1\}+P\{x_{2i}=0\}\cdot P\{x_{3i}=x_{1i}\}=\frac{1}{2}+\frac{1}{2}\cdot\frac{1}{2}=\frac{3}{4}$$

(оскільки $P\{\gamma_i = x_{3i}\} = 3/4$, то аналогічно ситуація має місце щодо кореляції гами та вихідної послідовності третього регістра).

Довжина гами $l = 30$ бітів, довжина першого регістра $L = 5$. За даним законом рекурсії визначимо послідовності, генеровані ним при різних початкових заповненнях, та обчислимо значення крос-кореляційної функції

$$C(d) = \frac{1}{l}\sum_{i=1}^{l}(-1)^{\gamma_i + x_{1i+d}}, \quad d = 1....2^L.$$

Наприклад, якщо при початковому заповненням 11000 на виході першого регістра отримано послідовність

11000110111010100001001011001111,

то

$$C(d) = \frac{1}{30}\left((-1)^{1+1} + (-1)^{0+1} + (-1)^{0+0} + ... + (-1)^{1+1} + (-1)^{0+1}\right) = 0{,}13.$$

Усі результати зведемо у табл. 4.8 (жирним шрифтом виділено початкове заповнення).

Таблиця 4.8

Значення крос-кореляційної функції при різних початкових заповненнях першого регістра

Гама 10011111100110101010000010010		
№	Вихідна послідовність $x_0x_1x_2...$ LFSR-1	$C(d)$
1	**10000**10010110011111000110111010	0
2	**01000**01001011001111100011011101	0,13
3	**11000**11011101010000100101100111	0,13
4	**00100**10110011111000110111010100	0,07
5	**10100**00100101100111110001101110	0,07
6	**01100**11111000110111010100001001	0
7	**11100**01101110101000010010110011	0,23
8	**00010**01011001111100011011101010	0,07
9	**10010**11001111100011011101010000	0,07
10	**01010**00010010110011111000110111	0
11	**11010**10000100101100111110001101	0,33
12	**00110**11101010000100101100111110	0,07
13	**10110**01111100011011101010000100	0,07
14	**01110**10100001001011001111100011	0,13
15	**11110**00110111010100001001011001	0,13
16	**00001**00101100111110001101110101	0,13
17	**10001**10111010100001001011001111	0,07

Продовження табл. 4.8

18	**01001**01100111110001101110101000	0,07
19	**11001**11110001101110101000010010	0,07
20	**00101**10011111000110111010100001	0
21	**10101**00001001011001111100011011	0,26
22	**01101**11010100001001011001111100	0,07
23	**11101**01000010010110011111000110	0,1
24	**00011**01110101000010010110011111	0
25	**10011**11100011011101010000100101	**0,9**

Якщо початкове заповнення регістра 10011, то $C(d) = 0,9 > T$, а це означає: до регістра «завантажено» саме вектор $(1,0,0,1,1)$.

Таким чином, навіть з довгим періодом і достатньо високою лінійною складністю генератор Геффе криптографічно слабкий.

Задача 33. Комбінувальний генератор сформовано з трьох регістрів зсуву із зворотним лінійним зв'язком, виходи яких комбінуються у такий спосіб: якщо два чи три вихідних біти регістрів дорівнюють «1», то символом гами буде «1», інакше – «0». $C_1(D) = 1 + D + D^4$, $C_2(D) = 1 + D + D^3, C_3(D) = 1 + D + D^2$ – многочлени оберненого зв'язку першого, другого і третього регістрів відповідно. За відомим відрізком гами

001111101011 011011111001011001011011

визначте секретний ключ $K = (K_1, K_2, K_3)$ шифру, утворений з початкових заповнень K_1, K_2, K_3 регістрів.

Р о з в' я з а н н я. Схему данного генератора наведено на рис. 4.3 , де через $b_i^{(1)}, b_i^{(2)}, b_i^{(3)}, k_i$ позначено відповідно вихідні послідовності першого, другого і третього регістрів та гами генератора.

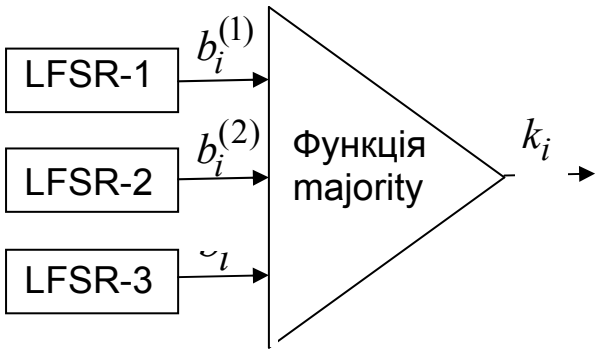


Рис.4.3

Розглянемо можливі варіанти отримання знаків гами:

$$b_i^{(1)}=0 \begin{cases} b_i^{(2)}=0;\quad b_i^{(3)}=0 \Rightarrow k_i=0; \\ b_i^{(2)}=1;\quad b_i^{(3)}=0 \Rightarrow k_i=0; \\ b_i^{(2)}=0;\quad b_i^{(3)}=1 \Rightarrow k_i=0; \\ b_i^{(2)}=1;\quad b_i^{(3)}=1 \Rightarrow k_i=1. \end{cases}$$

Отже, $P\{k_i=0 \mid b_i^{(1)}=0\}=\frac{3}{4}$ – умовна ймовірність того, що вихідний біт гами $k_i=0$ за умови, що $b_i^{(1)}=0$. Звідси, завдяки симетрії, дістаємо

$$P\{b_i^{(1)}=k_i\}=P\{b_i^{(2)}=k_i\}=P\{b_i^{(3)}=k_i\}=\frac{3}{4},$$

Ця ймовірність достатньо велика і тому висунемо таку ідею: правильний ключ $K=(K_1,K_2,K_3)$ скоріше за все буде складатися з тих початкових заповнень K_1,K_2,K_3 регістрів, при яких регістри генеруватимуть послідовності, найбільш близькі до заданого відрізка гами генератора. Традиційно метрикою відмінності двох бітових рядків однакової довжини вважають відстань Хеммінга – кількість позицій, в яких відповідні біти рядків різні. Очевидно, нас цікавитимуть вихідні послідовності регістрів, для яких відстань Хеммінга між ними і гамою буде мінімальною.

1). $K_3=01$– початкове заповненні третього регістра.

Вихід третього регістра: 0**1**1**0**11 **01**10110110110**0** 110 **1**1011**0**1 011011.
Гама: 0**01**111**10**1011011011 **1**110 **0**10110 **0**1011011.

Біти не збіглися сім разів на 36 позиціях (ці біти виділені напівжирно), а відтак, відстань Хеммінга $d_H=7$.

2). $K_3=11$.

Вихід третього регістра: **11**011 **01101** 1**01101**1**0** 11 **011011011 01101**1**0**.
Гама: **001**111**1 010110110** 1111 **10010**1**100 10**11**01**1.

$$d_H=25.$$

3). $K_3=01$.

Вихід третього регістра: **1**011 **0**1101 **10110** 1**10** 11 **0**11**0**1 **10** 11**0**1**10** 1**10**1.
Гама: **0**011**1**11 0**10**11**0**11**0** **1**1 1 **11 0** 01**01** 1**0**0 1**011011**.

$$d_H=17.$$

Відстань Хєммінга мінімальна при початковому заповненні $K_3 = 01$ і тоді генерована третім регістром послідовність найбільш близька до гами шифру. Приймемо ключ $K_3 = 01$ і вихідну послідовність третього регістра 0110110110110110110110110110110110011. Порівняння її з гамою шифру дає такий результат: другий і четвертий біти двох інших регістрів мають бути «0» і «1» відповідно. Тоді, прийнявши $b_2^{(2)} = 0$, знову визначаємо відстань Хеммінга між гамою шифру і виходом другого регістру.

1). $K_2 = 100$ – початкове заповнення другого регістра.

Вихід другого регістра: **1**0**0** 111**010**0111**10** 10**0**111**010**0**01**110**10**011**10**1.
Гама: 001111101011 **01**10**1**111**10**0**10**110**01**011**01**1.

$$d_H = 16.$$

2). $K_2 = 001$.

Вихід другого регістра: 00111**0**10**01** 1101**0**0111**0**1001**1**1**01**0**01**1101**0**.
Гама: 00111**1**10**10**110 1**1**0111**1**1001**0**1**10**0**10**1101**1**.

$$d_H = 11.$$

3) $K_2 = 101$.

Вихід другого регістра: **1**01 **00**11**101001** 1101 **00**11**1**010**01110100**11.
Гама: **0**01**11**11**01011** **0**1101 **11**1**0**010**1**1**0010110**11.

$$d_H = 20.$$

Найменше значення відстані Хеммінга досягається при початковому заповненні $K_2 = 001$, тому це заповнення, мабуть, слід вважати другою частиною ключа шифру.

Порівняння визначених нами вихідних послідовностей другого і третього регістрів з гамою генератора додаткової інформації про ключ шифру не дає. Залишається перевірити всі початкові заповнення першого регістра, які матимуть вигляд □0□1, де невідомі біти позначені пустими квадратиками.

1). $K_1 = 0001$ – початкове заповнення першого регістра.

Вихід першого регістра: 00**0**1111 010110**0**10001111010110010000111.
Гама**:** 00**1**1111 010110**1**10**11**111**0**0101100101**10**11

$$d_H = 8.$$

2). $K_1 = 1001$.

Вихід першого регістра: **1**0**0**1**0001**1**110** **10**11**00**1**00**0**111**1**01**01**100100**.
Гама: **0**0**1**1**11101**0**11** **01**1**011111**00**1**0**1**1**00**1**011011**.

$$d_H = 25.$$

3). $K_1 = 0011.$

Вихід першого регістра: 001111 **0101**10**0**10 **00**111**1**010110010 **001**11.
Гама: 001111**1010** 10**1**10**11**111**0**010110010 11011.

$$d_H = 11.$$

3). $K_1 = 1011.$

Вихід першого регістра: **1**011**00**10**0**01 **1**110 1**0**11**0**0**1**0**0**0**11**10 1**0**11**0**.
Гама: **0**011**11**10**1**01**0**110 1**1**111**0** **0**10**1**1**00**10 1**10**1**1**.

$$d_H = 15.$$

Найменша відстань Хеммінга $d_H = 8$ між гамою та вихідною послідовністю спостерігається при початковому заповненні $K_1 = 0001.$ Перевіркою упевнюємося, що при знайденому ключі

$$K = (0001, 001, 01)$$

генератор дійсно видає заданий відрізок гами.

Задача 34. Фільтрувальний генератор побудовано на основі LFSR із законом рекурсії $x_i = x_{i-15} + x_{i-18}$ (для $i \geq 18$) за допомогою фільтрувальної функції

$$f(x_{i-17}, x_{i-16}, ..., x_{i-2}, x_{i-1}, x_i) = x_{i-14}x_{i-12}x_{i-10} \oplus$$
$$\oplus x_{i-8}x_{i-6}x_{i-4} \oplus x_{i-14}x_{i-12} \oplus x_{i-6}x_{i-4} \oplus x_{i-8} \oplus 1.$$

Генератор ініціалізується 9-бітовим ключем $K = k_0, k_1, ..., k_8$ і 8-бітовим вектором ініціалізації $IV = IV_0, IV_1, ..., IV_7$ за схемою

x_0	x_1	x_2	x_3	...	x_{15}	x_{16}	x_{17}
k_0	IV_0	k_1	IV_1	...	IV_7	k_8	p

,

де контрольний біт p у 17-й чарунці вибирається так, щоб кількість одиниць у початковому заповненні регістру була непарною. Згенеруйте перші вісім бітів послідовності, якщо $K = 111000111$, $IV = 01010101.$ Припустивши, що криптоаналітик перехопив шифротекст 1100, отриманий накладанням гами, породженої даним генератором з деяким іншим ключем і старим вектором ініціалізації, визначте, якому з двох відкритих текстів він може відповідати: 0000 чи $1111.$

Р о з в’ я з а н н я. У послідовності, генерованій LFSR із законом рекурсії $x_i = x_{i-15} + x_{i-18}$, біти з номерами від 0 до 17 відповідають

початковому заповненню регістра (жирним шрифтом виділені біти ключа, нежирним – біти вектора ініціалізації, а підкреслений біт – контрольний), біти зворотного зв'язку мають номери 18, 19, 20,….

№ біта	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Біт	**1**	0	**1**	1	**1**	0	**0**	1	**0**	0	**0**	1	**1**	0	**1**	1	**1**	1	*0*	*1*	*1*	*1*	*0*	*0*	*0*	*1*

Визначаємо біти γ_i послідовності на виході генератора

При $i=18$: $\gamma_1 = x_4x_6x_8 \oplus x_{10}x_{12}x_{14} \oplus x_4x_6 \oplus x_{12}x_{14} \oplus x_{10} \oplus 1 =$

$$= 1\cdot 0\cdot 0 \oplus 0\cdot 1\cdot 1 \oplus 1\cdot 0 \oplus 1\cdot 1 \oplus 0 \oplus 1 = 0;$$

при $i=19$: $\gamma_2 = x_5x_7x_9 \oplus x_{11}x_{13}x_{15} \oplus x_5x_7 \oplus x_{13}x_{15} \oplus x_{11} \oplus 1 =$

$$= 0\cdot 1\cdot 0 \oplus 1\cdot 0\cdot 1 \oplus 0\cdot 1 \oplus 0\cdot 1 \oplus 1 \oplus 1 = 0.$$

Провівши аналогічні розрахунки, дістаємо перші вісім нульових бітів генерованого ключового потоку: 00000000.

Якщо для створенні першого біта на виході генератора задіяні біти ключа, то другий вихідний біт залежіть тільки від бітів вектора ініціалізації. За даним вектором ініціалізації другий біт генерованої послідовності дорівнює «0». Тому другий біт m_2 відкритого тексту знайдемо як

$m_2 = c_2 \oplus \gamma_2 = 1 \oplus 0 = 1 \Rightarrow$ скоріше зашифровано шифротекст 0000.

Задача 35. У генераторі «stop-and-go» тактовий вихід LFSR L_2 керується виходом LFSR L_1, а ключовий потік – вихідна послідовність LFSR L_2. Генератор працює за принципом: LFSR L_2 змінює свій стан у момент часу t лише за умови, що вихід LFSR L_1 на момент часу $t-1$ дорівнював «1». Якщо ж вихідний біт LFSR L_1 дорівнював «0», то біт ключового потоку дорівнює старому вихідному біту LFSR L_2. Наприклад, якщо LFSR L_1 генерує послідовність 101001…, а LFSR L_2 – послідовність $x_0x_1x_2\ldots$, то на виході генератора з'явиться послідовність $x_0x_0x_1x_1x_1x_2\ldots$. Припустимо, криптоаналітик дізнався, що перехоплений ним відрізок шифротексту

C: 1001 1101 0110 1001 0001 0010 1110 0101

може бути результатом накладання ключового потоку, виданого генератором, на один з трьох відкритих текстів

M_1: 1110 1000 1011 1111 1101 0001 0111 1100;

M_2: 1101 1010 1100 0101 1001 1101 1011 1111;

M_3: 1010 1100 1001 0110 1000 0101 0010 0101.

Якому відкритому тексту відповідає шифротекст?

Р о з в’ я з а н н я. За відомим шифротекстом і даними відкритими текстами визначимо можливі ключові потоки:

$$\Gamma_1 = C \oplus M_1 = 0111\ 0101\ 1101\ 0110\ 1100\ 0011\ 1001\ 1001;$$

$$\Gamma_2 = C \oplus M_2 = 0100\ 0111\ 1010\ 1100\ 1000\ 1111\ 0101\ 1010;$$

$$\Gamma_3 = C \oplus M_3 = 0011\ 0001\ 1111\ 1111\ 1001\ 0111\ 1100\ 0000.$$

Якщо ключовий потік істинно випадковий, то ймовірність того, що два послідовні біти збігатимуться, дорівнює 1/2. Для вихідної послідовності $\gamma_1\gamma_2...\gamma_{i-1}\gamma_i...$генератора «stop-and-go» ця імовірність більша:

$$P\{\gamma_{i-1}=\gamma_i\}= P\{L_{1,i}=0\}+P\{L_{1,i}=1\}P\{L_{2,j}=L_{2,j-1}\}=\frac{1}{2}+\frac{1}{2}\cdot\frac{1}{2}=0,75,$$

де $L_{1,i}L_{2,j}$ – *i*-ий та *j*-ий біти вихідних послідовностей, генерованих LFSR L_1 і LFSR L_2 відповідно. Імовірності виникнення біграм з двох однакових бітів у послідовностях Γ_1,Γ_2 і Γ_3 відповідно складають: $\frac{14}{31}\approx 0,45$; $\frac{13}{31}\approx 0,41$ і $\frac{23}{31}\approx 0,75$. Отже, перехоплений шифротекст C є результатом зашифрування тексту M_3.

Задача 36. Нехай спрощена версія шифру RC4 працює з 8-байтовим масивом та 2-байтовим ключем, тобто всі обчислення виконуються за $\bmod 8$. Визначте чотири байти вихідної гами, якщо ключ шифру $K_0 = 6, K_1 = 2$ (початкове заповнення масиву S).

Р о з в’ я з а н н я. Запишемо початковий масив S та знайдемо ключовий розклад:

$S = (0,1,2,3,4,5,6,7)$;

$j = 0$;

$i = 0 \Rightarrow j = (j + S_0 + K_0 \bmod 2) \bmod 8 = 0 + 0 + 6 \bmod 8 = 6;$

$S = (6,1,2,3,4,5,0,7);$

$i = 1 \Rightarrow j = (j + S_1 + K_1 \bmod 2) \bmod 8 = 6 + 1 + 2 \bmod 8 = 1;$

$S = (6,1,2,3,4,5,0,7);$

$i = 2 \Rightarrow j = (j + S_2 + K_2 \bmod 2) \bmod 8 = 1 + 2 + 6 \bmod 8 = 1;$

$S = (6,2,1,3,4,5,0,7);$

$i = 3 \Rightarrow j = (j + S_3 + K_3 \bmod 2) \bmod 8 = 1 + 3 + 2 \bmod 8 = 6;$

$S = (6,2,1,0,4,5,3,7);$

$i = 4 \Rightarrow j = (j + S_4 + K_4 \bmod 2) \bmod 8 = 6 + 4 + 6 \bmod 8 = 0;$

$S = (4,2,1,0,6,5,3,7);$

$i = 5 \Rightarrow j = (j + S_5 + K_5 \bmod 2) \bmod 8 = 0 + 5 + 2 \bmod 8 = 7;$

$S = (4,2,1,0,6,7,3,5);$

$i = 6 \Rightarrow j = (j + S_6 + K_6 \bmod 2) \bmod 8 = 7 + 3 + 6 \bmod 8 = 0;$

$S = (3,2,1,0,6,7,4,5);$

$i = 7 \Rightarrow j = (j + S_7 + K_7 \bmod 2) \bmod 8 = 0 + 5 + 2 \bmod 8 = 7;$

$S = (3,2,1,0,6,7,4,5).$

Тепер визначимо елементи псевдовипадкової послідовності:
$i = 0;\ j = 0;$

$i = i + 1 \bmod 8 = (0 + 1) \bmod 8 = 1;\ j = j + S_1 \bmod 8 = (0 + 2) \bmod 8 = 2;$

$S = (3,1,2,0,6,7,4,5);\qquad S_1 + S_2 \bmod 8 = 1 + 2 = 3$

Вихід: $t_1 = S_3 = 0;$

$i = i + 1 \bmod 8 = (1 + 1) \bmod 8 = 2;\ j = j + S_2 \bmod 8 = (2 + 2) \bmod 8 = 4;$

$S = (3,1,6,0,2,7,4,5);\qquad S_2 + S_4 \bmod 8 = 6 + 2 \bmod 8 \equiv 0$

Вихід: $t_2 = S_0 = 3;$

$i = i + 1 \bmod 8 = (2 + 1) \bmod 8 = 3;\ j = j + S_3 \bmod 8 = (4 + 0) \bmod 8 = 4;$

$S = (3,1,6,2,0,7,4,5)$; $S_3 + S_4 \bmod 8 = 2 + 0 \bmod 8 \equiv 2$

Вихід: $t_3 = S_2 = 6$;

$i = i + 1 \bmod 8 = (3+1) \bmod 8 = 4$; $j = j + S_4 \bmod 8 = (4+0) \bmod 8 = 4$;

$S = (3,1,6,2,0,7,4,5)$; $S_4 + S_4 \bmod 8 = 0 + 0 \bmod 8 \equiv 0$

Вихід: $t_4 = S_0 = 3$.

ТЕСТИ

1. До потокових відносять шифри, які
   а) шифрують від 64 до 256 бітів відкритого тексту, розбивши їх на байти;
   б) здатні зашифрувати блоки вхідних даних різного розміру за один й той самий час;
   в) перетворюють кожен символ відкритого тексту у символ шифротексту залежно не тільки від ключа, а й від його місцерозташування у відкритому тексті;
   г) переводять відкритий текст будь-якого розміру у бітову послідовність фіксованої довжини.

2. Ключовий потік – це:
   а) бітова послідовність, що визначається за допомогою ключа шифру;
   б) бітова послідовність, що не залежіть від ключа шифру;
   в) послідовність потоку відкритих даних, що потрібно зашифрувати;
   г) шифрування без ключа.

3. З якою метою при потоковому шифруванні використовують генератори псевдовипадкових числових послідовностей?
   а) для отримання «нескінченної» гами на основі ключа малої довжини;
   б) для захисту інформації від випадкових перешкод при передачі;
   в) для захисту інформації від навмисних змін вже переданої інформації;
   г) для стискання інформації при шифруванні;
   д) для формування відкритих ключів.

4. Що з нижченаведеного є ознакою стійкого потокового шифру?
   а) невідтворюваність гами;

б) великий період;
в) статистична передбачуваність гами;
г) нелінійний зв'язок гами з ключем шифру.

5. Яку з нижчезазначених властивостей ***не*** можна віднести до переваг потокових шифрів?

а) один й той самий шифратор може використовуватися і для зашифрування, і для розшифрування текстів;
б) апаратна реалізація потокових шифрів обумовлює високу швидкість обробки текстів;
в) у синхронних потокових шифрах відсутнє розповсюдження помилок;
г) генератори гами на передавальній та приймальній сторонах мають бути синхронізовані.

6. Перерахуйте переваги потокових шифрів над блоковими?

а) у потокових шифрів більш висока швидкість шифрування;
б) у потокових шифрах відсутнє розповсюдження помилок;
в) зміна одного біта відкритого тексту приводить до лавинного ефекту;
г) ключовий потік можна визначити заздалегідь до операції шифрування.

7. Потокові шифри доцільно використовувати

а) для зашифрування даних у режимі реального часу;
б) за потребою у негайному зашифруванні окремих бітів чи коротких бітових послідовностей;
в) для зашифрування інформації, що передається у спеціалізованих мікропроцесорних системах керування (банкомати, платіжні термінали);
г) коли при шифруванні не мають поширюватися помилки.
д) для зашифрування бази даних на жорсткому диску;
е) для створення імітовставки;
ж) для аутентифікації у глобальному цифровому стандарті GSM для мобільного сотового зв'язку;
з) для зашифрування даних RFID-меток (радіохвильова ідентифікація).

8. В яких прикладних задачах криптографії застосовують випадкові числа?

а) генерація ключів;
б) зашифрування за допомогою одноразового шифроблокноту;
в) обчислення значень однобічних функцій;

г) сіль у схемах електронного цифрового підпису;
д) диференціальний криптоаналіз;
е) одноразові випадкові числа для протоколів (nonce);
ж) у всіх вищенаведених задачах.

9. Яке висловлювання *неправильне* ?

а) якщо після використання ключа потокового шифру двічі нападник дізнається, який відкритий текст шифрували вперше, то, перехопивши обидва шифротексти, він зможе знайти відкритий текст, відповідний другому шифротексту;
б) якщо нападник знає відкритий текст і відповідний йому шифрований текст, отриманий за допомогою криптоалгоритму AES, то він може знайти використаний ключ, провівши повний перебір ключів;
в) атака на потоковий шифр з вибором відкритого тексту може бути ефективніша, ніж «атака грубої сили»;
г) подовження ключа ускладнює повний перебір ключів, що обумовлює більшу криптографічну стійкість асиметричних шифрів порівняно з симетричними.

10. Який тип шифру найімовірніше атакував нападник, якщо його атаки базувалися на аналізі довжини повідомлень?

а) блокові; б) потокові; в) асиметричні; г) симетричні.

11. Яка властивість непритаманна синхронним потоковим шифрам?

а) непоширення помилок;
б) зміна у шифротексті одного символу призводить до неправильного розшифрування решти символів;
в) у разі втрати символу шифротексту неможливо правильно розшифрувати весь текст за втраченим символом;
г) вставка активним супротивником додаткового символу в шифротекст порушує подальше розшифрування.

12. Які з нижченаведених властивостей мають самосинхронізовані потокові шифри?

а) непоширення помилок;
б) обмежене поширення помилок;
в) для гарантій цілісності даних потрібні додаткові контрольні заходи;
г) самосинхронізація;
д) розсіяння статистики відкритого тексту.

13. Який режим зашифрування не має сенсу використовувати для потокового шифрування?

а) ECB; б) CFB; в) OFB; г) CTR.

14. Що з нижченаведеного є потоковим шифром?

а) RC4; б) AES; в) DES;
г) AES-OFB; д) AES-CBC; е) AES-CTR.

15. Одна з перших версій мережевого протоколу SSH застосовувала потокові шифри так, що шифровані дані передавали в обох напрямках (від користувача до хосту та від хосту до користувача) із використанням одного й того самого ключа (тобто гама, що накладалась на відкритий текст, двічі була однаковою). Які проблеми Ви бачити у цьому?

а) виникає загроза проведення атаки з перекриттям;
б) жодної, бо у цьому випадку кількість можливих гам велика і метод повного перебору ключів потребуватиме необмежених обчислювальних можливостей;
в) загроз безпеці не виникає, оскільки доведена теоретико-інформаційна стійкість усіх шифрів гамування;
г) використана гама через подвоєння своєї довжини втрачає рівномірний розподіл імовірностей своїх знаків;
д) можливо здійснити атаку за допомогою вставки символу між двома сеансами.

16. За стандартом 802.11b у Wireless LAN системі використовується потоковий шифр Wireless Equivalence Protocol з 40-бітовим ключем і 24-бітовим вектором ініціалізації, за допомогою яких генерується ключовий потік. Яке призначення вектора ініціалізації у цьому шифрі?

а) ускладнити повний перебір ключа;
б) запобігти «атаці вставкою»;
в) дати можливість двічі використовувати один й той самий ключ для зашифрування;
г) увести часову мітку.

17. WEP – старий стандарт захисту бездротового трафіку, заснований на потоковому кодуванні з використанням алгоритму RC4. Цей стандарт виявився вразливим до активних атак, коли нападник змінює біти в зашифрованому тексті, що спричиняє несанкціоновану модифікацію повідомлення, отриманого законним користувачем. Що є кращим захистом від таких атак?

а) використання різних ключів кожною стороною для кожного бездротового пристрою;
б) захист шифротексту за допомогою MAC;
в) зашифрування за допомогою шифру AES в режимі CBC;
г) зашифрування за допомогою шифру AES р ежимі ECB.

18. Яку з наступних криптосистем можна вибрати як високошвидкісну систему шифрування при передачі даних?

а) MAC; б) MD5 ; в) RC4; г) RSA.

19. Якщо за допомогою шифру гамування зашифрувати відкритий текст 0000000000…, то

а) отримаємо ключ шифру;
б) ключ шифру автоматично подвоїться;
в) отримаємо шифрований текст 0000000000…;
г) дістанемо вектор ініціалізації.

20. На біти $x_1x_2x_3x_4x_5x_6$ чотирьох різних відкритих текстів накладається гама $\gamma_1\gamma_2\gamma_3\gamma_4\gamma_5\gamma_6$ у відповідності з рівнянням шифрування $y_i = x_i + \gamma_i (\mathrm{mod}\ 2)$, де y_i – біти шифротексту. Установіть відповідність між виглядом відкритого тексту та виглядом шифротексту.

Відкритий текст	Шифротекст
1) 00000000	А) $\overline{\gamma_1\gamma_2\gamma_3\gamma_4\gamma_5\gamma_6}$
2) 11111111	Б) $\gamma_1\gamma_2\gamma_3\gamma_4\gamma_5\gamma_6$
3) 01010101	В) $\overline{\gamma_1}\gamma_2\overline{\gamma_3}\gamma_4\overline{\gamma_5}\gamma_6$
4) 10101010	Г) $\gamma_1\overline{\gamma_2}\gamma_3\overline{\gamma_4}\gamma_5\overline{\gamma_6}$

21. Криптоаналітик перехопив криптограму 2,3,5,0,6,4,4, отриману за допомогою шифру гамування при шифруванні відкритого тексту 1,2,4,4,0,3,5 за рівнянням шифрування $y_i = x_i + \gamma_i (\mathrm{mod}\ 7)$. Яку криптограму він має надіслати законному користувачеві, щоб при розшифруванні при старій гамі той отримав текст 5,3,0,4,4,2,1?

а) 6,5,3,2,2,1,0; б) 2,1,5,6,6,3,4; в) 4,4,6,0,5,3,2; г) 6,4,1,0,3,3,0.

22. Які з нижченаведених тверджень щодо шифру одноразового блокноту не є *правильними*?

а) довжина ключа шифру має бути не меншою за довжину відкритого повідомлення;
б) ключ шифру можна створити за допомогою регістру зі зворотним лінійним зв'язком;
в) шифр має теоретико-інформаційну стійкість;
г) якщо передавальна і приймальна сторони мають спільний псевдовипадковий ключ, то його потрібно змінювати після кожного сеансу передачі, якщо ж ключ істинно випадковий, то його не потрібно змінювати.

23. При використанні одноразового шифрувального блокноту відкритий текст M можна перетворити на шифротекст C за допомогою

а) тільки одного ключа; б) двох ключів;
в) багатьох ключів; г) $M-1$ ключів.

24. Чи будуть наведені в табл. 4.9 шифри досконало стійкими, обчислювально стійкими чи криптографічно нестійкими? Вважайте, що в усіх системах використовується блоковий криптоалгоритм AES як синхронний потоковий шифр (у разі потреби прийняти, що AES – безпечна псевдовипадкова функція); $||$– символ конкатенації; k – ключ криптоалгоритму AES; b – біт відкритого тексту.

Таблиця 4.9

Шифри

№ схеми	Генерація ключів	Зашифрування
1	Випадковий вибір 128-бітового ключа	$c = AES_k(b \| r)$, де r – випадковий 63-бітовий рядок
2	Ключ k вибирається навмання з деяких двох 128-бітових рядків k_1 і k_2	$c = AES_k(b \| r \| 0^{64})$, де r – випадковий 63-бітовий рядок
3	Ключ k вибирається навмання з деяких двох 128-бітових рядків k_1 і k_2	1. r – такий 128-бітовий рядок, для якого найменший значущий біт $AES_{k_1}(r)$ дорівнює 0, а найменший значущий біт $AES_{k_2}(r)$ дорівнює 1. 2. Якщо $k = k_1$, то $c = (r, b)$, якщо ж $k = k_2$, то $c = (r, 1-b)$.

25. Абонент А відкрив акаунт для брокера В, щоб отримати доступ до торгів в он-лайн режимі. За домовленістю між брокером та абонентом команда «купуй» кодуватиметься однією буквою «К», а команда «продай» – буквою «П». Після букви через пробіл у повідомленні стоятиме п'ятизначне десяткове число, що вказує на кількість акцій, які абонент хоче купити чи продати (якщо кількість акцій виражається числом меншим за п'ятизначне, то попереду проставляється необхідна кількість додаткових нулів). Далі повідомлення має містити знову пробіл і чотирибуквений тікер компанії, чиї акції цікавлять абонента. Наприклад, повідомлення «К 04000 UTEL» означає «Купити 4000 акцій Укртелекому», а повідомлення «П 10000 AZST» – «Продати 10000 акцій Азовсталі». Загальна довжина повідомлення не перевищує 96 бітів. Для підвищення безпеки акаунта абонент задіяв шифрування повідомлень за допомогою одноразового блокноту, вибравши за гаму шифру одну істинно випадкову 96-бітову послідовність. Яку інформацію може отримати криптоаналітик, перехопивши два шифротексти c_1 і c_2?

а) визначити обидва відкриті тексти m_1 та m_2, що відповідають шифротекстам c_1 і c_2;

б) відновити тільки один з відкритих текстів: або m_1 , або m_2;

в) визначити $m_1 \oplus m_2$;

г) обчислити значення $2^{m_1 \oplus m_2}$;

д) жодної інформації отримати неможливо, бо одноразовий блокнот належить до досконало стійких шифрів.

26. Чи можна визначити ключ шифру одноразового блокноту, якщо відома пара «відкритий ключ – відповідний шифротекст»?

а) ні, бо шифр одноразового блокноту має досконалу стійкість;

б) так, $k_i = c_i + m_i$, де k_i, c_i, m_i – біти ключа шифротексту і відкритого тексту ;

в) можна визначити тільки половину бітів ключа;

г) так, $k_i = 2m_i$.

27. Поставте у відповідність тип послідовності та її визначення.

1. істинно випадкова послідовність;
2. псевдовипадкова послідовність;
3. послідовність збалансована;
4. ідеальна випадкова послідовність.

а) послідовність знаків скінченного алфавіту, в якій кожен знак зустрічається однакову кількість разів;
б) генерована недетермінованим фізичним пристроєм або процесом;
в) реалізація послідовності незалежних випадкових величин, що мають рівномірний розподіл на даному скінченому алфавіті.
г) генерована детермінованим пристроєм або програмою;

28. Поставте у відповідність тип послідовності і спосіб її генерування.

1. Ідеальна випадкова послідовність;
2. Псевдовипадкова послідовність;
3. Істинно випадкова послідовність.

а) детермінований пристрій або програма;
б) недетермінований фізичний пристрій або процес;
в) реалізація послідовності незалежних випадкових величин, що мають рівномірний розподіл.

29. Послідовність істинно випадкових чисел

а) має нормальний закон розподілу ймовірностей;
б) має рівномірний закон розподілу ймовірностей;
в) є монотонно зростаючою;
г) є монотонно спадною.

30. Збалансовані бітові послідовності – це послідовності, на періоді яких спостерігається однакова кількість нулів та одиниць. Скільки збалансованих послідовностей мають період 10?

а) 232; б) 242; в) 252; г) 374; д) 384; е) 394; ж) $5!$.

31. Згідно з постулатами Голомба на псевдовипадкову бітову послідовність накладаються обмеження на

а) зустрічальність знаків;
б) зустрічальність мультиграм;
в) автокореляційну функцію;
г) профіль лінійної складності;
д) розподіл елементів послідовності на площині;
е) ступінь стискання послідовності.

32. Для ідеальної випадкової послідовності ймовірність збігу біта з будь-яким його прогнозним значенням

а) дорівнює 1; б) дорівнює 1/2; в) більше 1/2; г) близька до 1.

33. Сукупність статистичних критеріїв, призначених для перевірки відповідності аналізованої числової послідовності гіпотезі про незалежність і рівноймовірнсть її елементів, називається

а) статистичним вимірами послідовності;
б) тестами виявлення залежності;
в) тестами дисперсного аналізу;
г) набором статистичних тестів.

34. Критерій перевірки якості двійкової псевдовипадкової послідовності, оснований на порівнянні сумарної кількості серій з нулів і серій з одиниць з розподілом цього числа для ідеальної випадкової послідовності, називається

а) серійним тестом;
б) перевіркою профілю лінійної складності;
в) універсальним тестом Маурера;
г) перевіркою пересічних серій;
д) перевіркою непересічних серій.

35. На рис. 4.4 наведено гістограми розподілу деяких числових послідовностей. Якій з послідовностей притаманна випадковість?

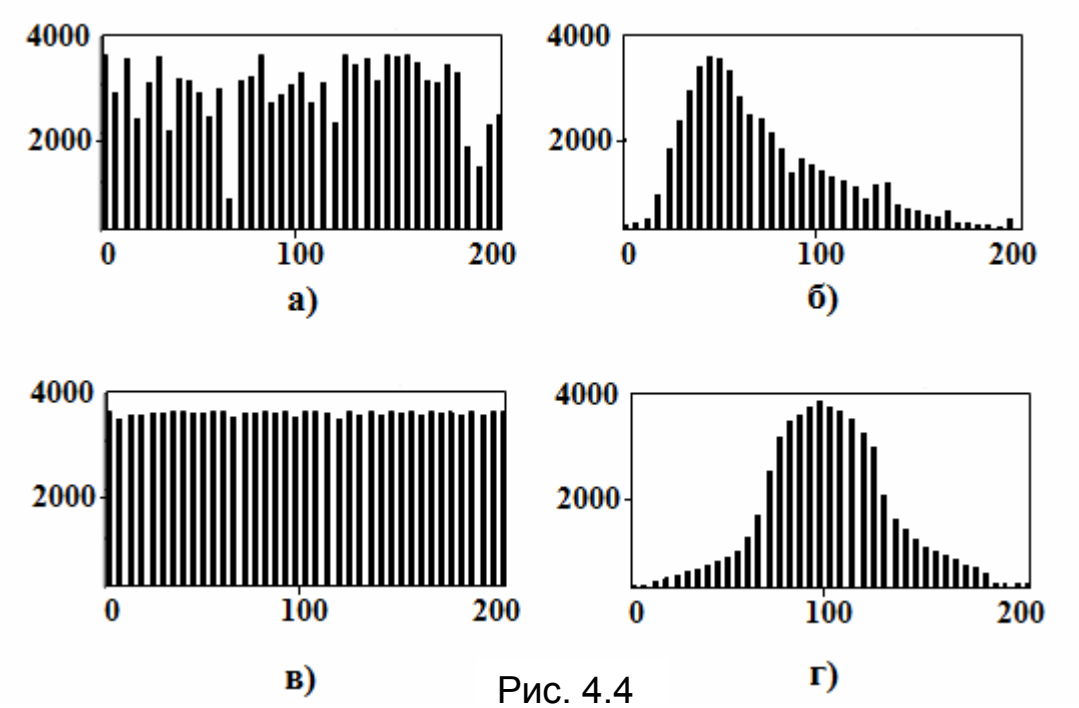


Рис. 4.4

36. Якщо двійкова послідовність, чиї властивості близькі до властивостей ідеальної випадкової послідовності, проходить графічний спектральний тест, то кількість гармонік, чиї амплітуди значно перевищують середню амплітуду гармонік

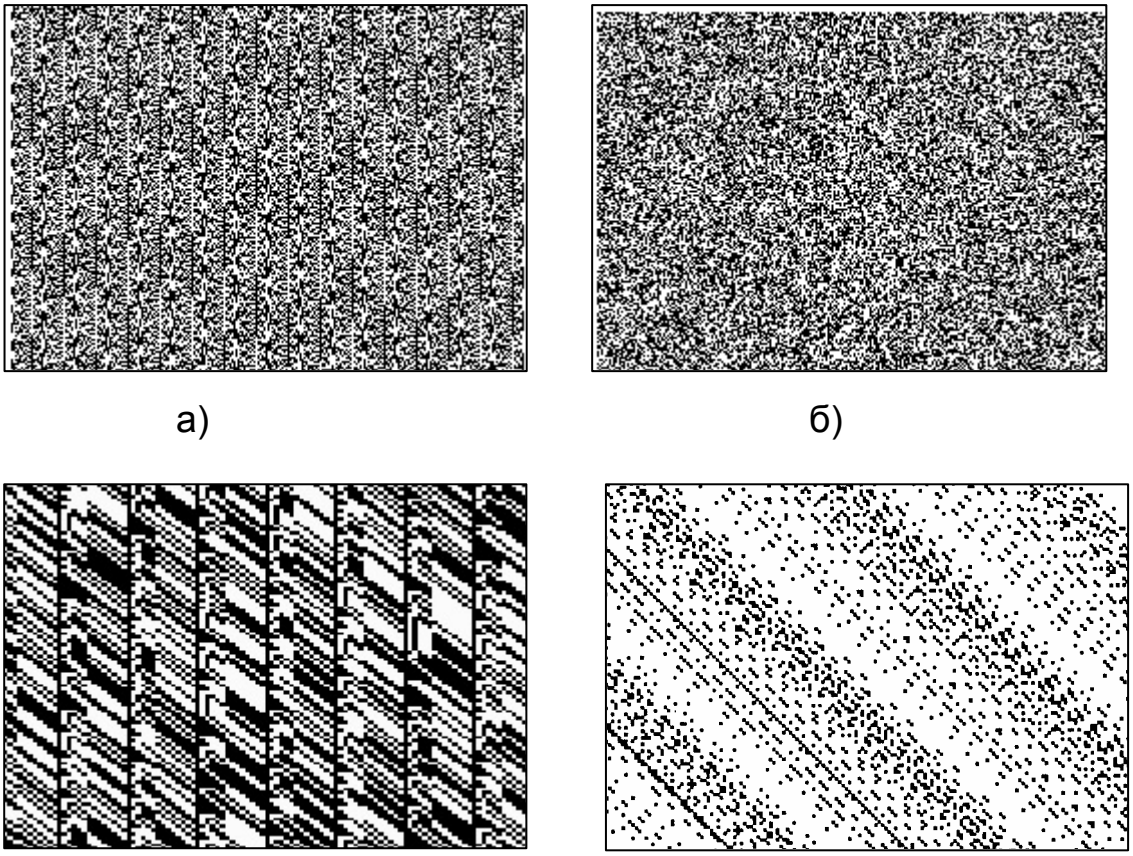
а) складає половину від кількості всіх гармонік;

б) більше за половину кількості всіх гармонік;
в) прямує до одиниці;
г) прямує до нуля.

37. Перевірка якості псевдовипадкової послідовності, що основана на обчисленні лінійної складності її відрізків, виконується за допомогою

а) алгоритму Берлекемпа – Мессі;
б) постулатів Голомба;
в) універсального тесту Маурера;
г) обчислення автокореляційної функції.

38. За даними рис. 4.5 (http://boallen.com/random-numbers.html) встановіть, яка з двійкових послідовностей проходить тест розподілу на площині.



а) б) в) г)

Рис. 4.5

39. Який дефект двійкової послідовності можна виявити за допомогою статистичного тесту перевірки кумулятивних сум? (тест з пакету NIST)
а) періодичність послідовності;
б) надмірну зустрічальність m-бітових послідовностей з одиниць;

в) більшу можливість стискання, ніж в істинно випадкової послідовності;
г) наявність значної кількості нулів чи одиниць на початку або в кінці послідовності.

40. За даними рис. 4.6 визначте двійкову послідовність, яка проходить тест профіля лінійної складності.

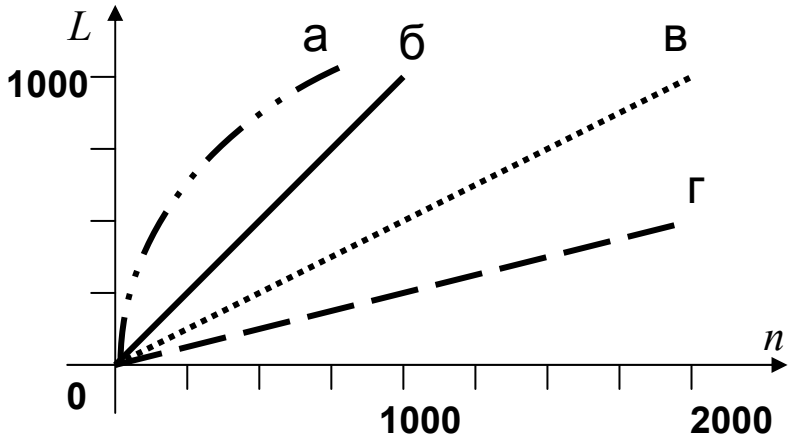


Рис. 4.6

41. Який дефект бітової послідовності можна виявити за допомогою універсального статистичного тесту Маурера? (тест з пакету NIST)
а) можливість стискання послідовності;
б) відхилення від теоретичного емпіричного закону розподілу значень;
в) локалізовані відхилення частоти появи одиниць у блоці від ідеального значення 1/2;
г) нерівномірність розподілу m-грам у послідовності.

42. При тестуванні бітової послідовності за допомогою універсального статистичного тесту Маурера її розбивають на неперетинні блоки і далі обчислюють
а) вибіркове середнє значення квадрата відстані між однаковими блоками конкретного вигляду;
б) середнє значення логарифма відстані між однаковими блоками конкретного вигляду;
в) відстані між однаковими блоками конкретного вигляду;
г) ранг матриць, складених з блоків разного вигляду.

43. Установіть відповідність між статистичними тестами пакету NIST для перевірки якості псевдовипадкових послідовностей та статистиками.
1. Частотний монобітний тест;
2. Універсальний тест Маурера;

3. Перевірка стискання за алгоритмом Лемпеля – Зіва;
4. Перевірка серій.

а) сума логарифмів відстаней між шаблонами;
б) кількість різних слів у послідовності;
в) загальна кількість серій на всій довжині послідовності;
г) нормалізована абсолютна сума значень елементів послідовності.

44. Що розуміють під тестом на наступний біт?

а) останній біт будь-якої псевдовипадкової послідовності слугує часовою міткою;
б) для полегшення розшифрування має існувати поліноміальний алгоритм, який за відомими першими n бітами випадкової послідовності достовірно визначає значення $(n+1)$-го біта;
в) не повинно існувати поліноміального алгоритму, який за відомими першими n бітами випадкової послідовності зможе передбачити значення $(n+1)$-го біта з імовірністю, більшою ніж 1/2;
г) при ініціалізації двома різними випадковими значеннями генератор має видавати послідовності, які відрізняються лише одним бітом.

45. Генератор псевдовипадкових послідовностей проходить усі тести статистичної перевірки на випадковість. Які додаткові вимоги він має задовольняти, щоб вважатися криптографічно безпечним псевдовипадковим генератором?

а) період генерованої послідовності має бути дуже великим, порівняним з довжиною відкритого повідомлення;
б) вихідні біти мають генеруватися за допомогою експоненціального алгоритму;
в) обчислювально неможливо визначити біт b_{i-1} послідовності за відомим фрагментом біт

$$b_i b_{i+1} \ldots b_{i+n-1}$$

та біт b_{i+1} за відомим фрагментом

$$b_{i-n+1} \ldots b_{i-2} b_{i-1} b_i$$

(непередбачуваний генератор);
г) при ініціалізації випадковими значеннями генератор має видавати статистично залежні послідовності.

46. Як називається генератор псевдовипадкових чисел, що обчислює наступне число x_{i+1} за формулою $x_{i+1} = ax_i + b(\mathrm{mod}\, m)$, $a, b, m - const$?

а) генератор Фібоначчі з запізненням;
б) лінійний конгруентний генератор;
в) генератор BBS;
г) генератор з модульним лишком.

47. За якою з наведених формул можна визначати послідовні числа, генеровані лінійним конгруентним генератором з множником a, інкрементом b та модулем m?

а) $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_{i-1} \\ 1 \end{pmatrix} \bmod m = \begin{pmatrix} x_i \\ 1 \end{pmatrix}$; б) $\begin{pmatrix} b & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_{i-1} \\ 1 \end{pmatrix} \bmod m = \begin{pmatrix} x_i \\ 1 \end{pmatrix}$;

в) $\begin{pmatrix} a+b & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_{i-1} \\ 1 \end{pmatrix} \bmod m = \begin{pmatrix} x_i \\ 1 \end{pmatrix}$; г) $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \cdot \begin{pmatrix} x_{i-1} \\ 1 \end{pmatrix} \bmod m = \begin{pmatrix} x_i \\ 1 \end{pmatrix}$.

48. Параметрами лінійного конгруентного генератора є модуль $m = 10$, множник $a = 3$, інкремент $b = 4$, початкове значення $x_0 = 5$. Яким буде третій член генерованої послідовності?

а) 3; б) 4; в) 5; г) 6; д) 7.

49. Знайдіть загальну формулу, що зв'язує члени x_i і x_{i+k}, $k = 1, 2...$ лінійної конгруентної послідовності $x_{i+1} \equiv a\,x_i + b (\bmod m)$, $i = 0, 1, ...$, $a > 1$.

а) $x_{i+k} = \left(a^k x_i + \dfrac{b}{a-1} \right) (\bmod m)$; б) $x_{i+k} = \left(b x_i + \dfrac{a^k - 1}{a-1} \right) (\bmod m)$;

в) $x_{i+k} = \left(x_i + \dfrac{a^k - 1}{b-1} \right) (\bmod m)$; г) $x_{i+k} = \left(a^k x_i + \dfrac{a^k - 1}{a-1} b \right) (\bmod m)$.

50. Вихідна послідовність якого з нижченаведених лінійних конгруентних генераторів матиме максимальний період?

а) $x_{i+1} \equiv 27 x_i + 48 (\bmod 13)$; б) $x_{i+1} \equiv 5 x_i + 3 (\bmod 11)$;
в) $x_{i+1} \equiv 17 x_i + 7 (\bmod 32)$; г) $x_{i+1} \equiv 6 x_i + 3 (\bmod 23)$.

51. На рис. 4.7 подано результати тестування за допомогою спектрального графічного тесту широко розповсюдженого на мейнфреймах IBM у 1960 – 1970 рр. лінійного конгруентного генератора RANDU із законом рекурсії $x_{i+1} = 65539 x_i (\bmod 2^{31})$,

$i = 1, 2, ...$ За даними рис. 4.7 (http://cer.freeshell.org/renma/Randu/) виберіть *правильні* твердження:

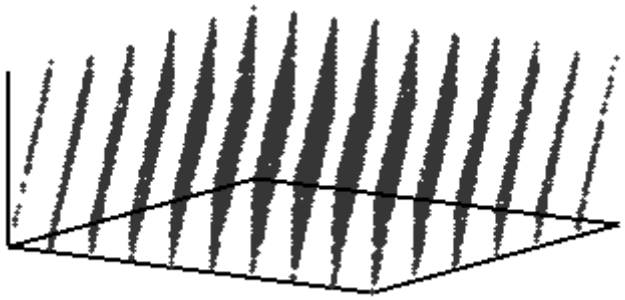


Рис. 4.7

а) кожній трійці x_i, x_{i+1}, x_{i+2} елементів генерованої послідовності на рисунку відповідає точка $(x_i; x_{i+1}; x_{i+2})$;

б) розташування точок на п'ятнадцяти паралельних площинах вказує, що період генерованої послідовності $2^{15} - 1$;

в) оскільки модуль 2^{31}значно перевищує кількість утворених площин, то послідовність випадкова;

г) генератор не проходить тест.

52. Припустимо, що 128-бітовий ключ криптоалгоритму AES-128 формується за допомогою лінійного конгруентного генератора ANSI-C, який видає псевдовипадкові числа з інтервалу $[0;\ 2^{31} - 1]$ у відповідності із законом

$$x_i = (1103515245 x_{i-1} + 12345) \bmod 2^{31}.$$

Початкове заповнення генератора – 31-бітове випадкове число. Для формування ключа AES-128 вибирають п'ять послідовних чисел, генерованих ANSI-C, і далі ключ утворюють за правилом: 28 бітів із першого генерованого числа, 28 бітів – із другого, 24 – із третього, 24 – із четвертого, 24 – із п'ятого. Якщо криптоаналітику відома процедура вибору бітів ключа, то яку максимальну кількість ключів AES-128 він має перевірити при повному переборі ключів?

а) 2^{31}; б) 2^{24}; в) 2^{52}; г) 2^{7}.

53. Для генерації псевдовипадкових чисел використовується 24-бітовий LFSR з максимальним періодом. Чому дорівнює цей період?

а) 24; б) 24^2; в) 2^{24}; г) $2^{24} - 1$; д) $2^{12} + 1$.

54. Незвідний нормований многочлен $f(x)$ степеня n називається примітивним над полем $GF(2)$, якщо $f(0) \neq 0$ і мінімальне значення e, при якому виконується порівняння $x^e \equiv 1 \bmod f(x)$, дорівнює

а) $2^n + 1$; б) 2^n; в) $2^n - 1$; г) $n^2 - 1$;
д) $n^2 + 1$; е) $2n - 1$; ж) $2n + 1$.

55. За якої умови незвідний нормований многочлен $f(x), f(0) \neq 0$, степеня n над скінченним полем $GF(q)$ буде примітивним?

а) $x^{(q^n-1)/p} \not\equiv 1 \bmod f(x)$ при всіх простих дільниках p числа $q^n - 1$;

б) $x^{(q^n-1)/p} \equiv 1 \bmod f(x)$ при всіх простих дільниках p числа q;

в) $f(x)^{(q^n-1)/p} \equiv 1 \bmod q$ при всіх простих дільниках p числа q^n;

г) $f(x)^{(q^n-1)/p} \not\equiv 1 \bmod q$ при всіх дільниках p числа q.

56. Назвіть дві основні складові регістрів зсуву із зворотним лінійним зв'язком.

а) арифметико-логічний пристрій;
б) регістр пам'яті;
в) пристрій для генерації функції оберненого зв'язку;
г) регістр зсуву;
д) пристрій для фільтрації бітів;
е) пристрій для нелінійної комбінації виходів регістру.

57. Чим визначається розрядність LFSR?

а) кількістю вихідних бітів;
б) швидкістю роботи регістру;
в) кількістю бітів, що можна одночасно зберігати у регістрі;
г) довжиною імітовстаки.

58. Які з нижченаведених рекурентних рівнянь задають лінійні однорідні послідовності другого порядку над полем $GF(5)$?

а) $x_i = 4x_{i-1}^2$; б) $x_i = x_{i-1} + x_{i-3}$;
в) $x_i = 3x_{i-2}$; г) $x_i = 3x_{i-2} + 1$.

59. На рис. 4.8 зображено LFSR, характеристичний многочлен якого

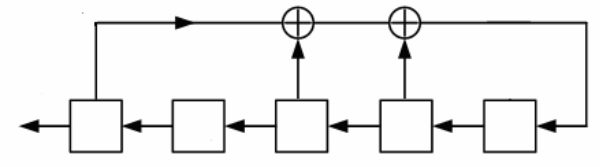


Рис. 4.8

а) $F(\lambda)=\lambda^5+\lambda^4+\lambda+1;$ б) $F(\lambda)=\lambda^4+\lambda^3+\lambda^2+1;$

в) $F(\lambda)=\lambda^3+\lambda^2+1;$ г) $F(\lambda)=\lambda^5+\lambda^3+\lambda^2+1.$

60. На рис. 4.9 зображено LFSR, характеристичний многочлен якого

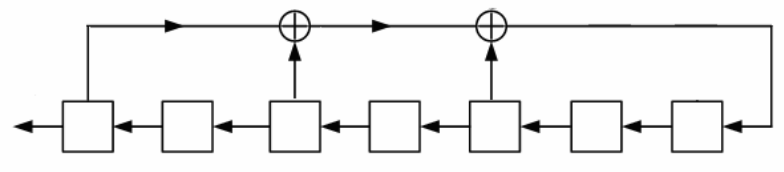


Рис. 4.9

а) $F(\lambda)=\lambda^6+\lambda^4+\lambda^2+1;$ б) $F(\lambda)=\lambda^7+\lambda^4+\lambda^2+1;$

в) $F(\lambda)=\lambda^7+\lambda^5+\lambda^3+1;$ г) $F(\lambda)=\lambda^6+\lambda^5+\lambda^3+1.$

61. Відтворить графічно принцип дії LFSR за його відомим характеристичним многочленом $F(\lambda)=\lambda^6+\lambda^4+1,$ утвореним з послідовності його відводів (рис. 4.10).

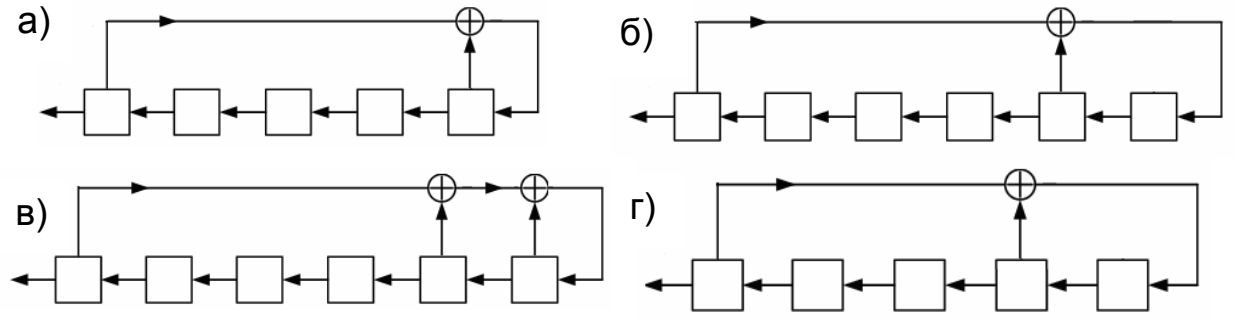


Рис. 4.10

63. LFSR генерує бітову послідовність, яка описується законом рекурсії $x_{i+3}=x_{i+1}+x_i(\mathrm{mod}\,2)$ для $i\geq 1$. Опишіть структуру цього LFSR.

а) LFSR містить дві чарунки S_2, S_1, біт зворотного зв'язку дорівнює сумі їх вмісту і подається на вихід;

б) LFSR містить чотири чарунки S_4, S_3, S_2, S_1, біт зворотного зв'язку дорівнює сумі бітів в чарунках S_2, S_1 і повертається в чарунку S_3;

в) LFSR, який би працював у відповідності з цим законом рекурсії, не існує;

г) LFSR містить три чарунки S_3, S_2, S_1, біт зворотного зв'язку дорівнює сумі бітів в чарунках S_2, S_1.

62. Відтворить графічно принцип дії 5-бітового LFSR за відомим законом рекурсії $x_{5+i} = x_{4+i} \oplus x_{2+i} \oplus x_i$ (рис. 4.11).

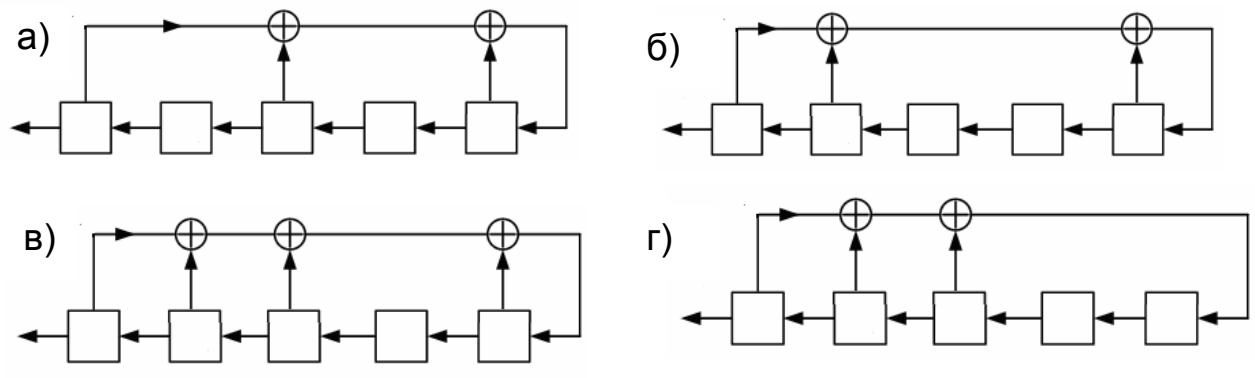


Рис. 4.11

64. Характеристичний многочлен, утворений з відводів LFSR, є примітивним. Чому послідовність, генеровану таким LFSR, небезпечно використати як гаму потокового шифру?

а) гама не буде задовольняти постулати Голомба;

б) за допомогою алгоритму Берлекемпа – Мессі можна провести атаку на основі відкритого тексту, яка розкриє ключ;

в) гама не буде мати максимальний період;

г) гама буде істинно випадковою і її важко буде повторити на приймальній стороні при розшифровці.

65. Якщо трійка бітів (a, b, c) – початкове заповнення трибітового LFSR з характеристичним многочленом $f(x) = x^2 + x + 1$, то п'ятим бітом генерованої регістром послідовності буде

а) $a \oplus b$; б) $a \oplus c$; в) $a \oplus b \oplus c$; г) $b \oplus c$.

66. Нехай LFSR довжини l генерує бітову гаму довжини n. Яке твердження *неправильне*?

а) l послідовних станів регістру лінійно незалежні;
б) $l+1$ послідовних станів регістру лінійно незалежні;
в) щоб однозначно визначити многочлен зворотного зв'язку для даного регістру, потрібно задати $n \geq 2l$ послідовних символів гами, згенерованої регістром;
г) період гами залежіть від функції зворотного зв'язку.

67. Укажіть декілька послідовних станів LFSR з характеристическим многочленом $f(x) = x^4 + x^3 + x^2 + x + 1$ при початковому заповненні 0111.

а)	б)	в)	г)
0111	0111	0111	0111
1111	1111	1110	1011
1110	1010	1101	0101
1101	1100	1010	1010
1011	1001	0101	1011

68. Яким буде ключовий потік, що генерує LFSR, якщо його характеристический многочлен $f(x) = x^4 + x + 1$, а початковий стан 1101?

а) 1101010111011010001;
б) 1101010100101010110;
в) 1101011110001001101;
г) 0010101011010101001.

69. Яке з тверджень щодо періоду T вихідної послідовності, генерованої 128-бітовим LFSR, є *правильним*?

а) $T = 2^{128} - 1$;
б) $T = 2^{64} - 1$;
в) період може бути більшим за $2^{128} - 1$;
г) за наданою інформацією неможливо встановити довжину періоду.

70. Яка довжина LFSR, якщо максимальна довжина періоду послідовності, що ним генерується, дорівнює 31?

а) 2; б) 3; в) 4; г) 5; д) 16; е) 32; є) 62.

71. Скільки нульових бітів з'являється на періоді m-послідовності, генерованої L-бітовим LFSR з примітивним характеристичним многочленом?

а) 2^{L-1}; б) $2^{L-1}-1$; в) 2^{L+1};

г) $L/2$; д) $(L/2)-1$; е) $2^{L/2}$.

72. LFSR з максимальним періодом використовується Інтернет-казіно для генерації псевдовипадкової бітової послідовності з метою імітації рулетки. Початкове заповнення регістра мало довжину 32 біти, а генерована послідовність нараховувала 4096 бітів. Якщо навмання вибрати нове початкове заповнення регістру, то яка ймовірність, що нова 4096-бітова послідовність на виході регістру збігатиметься із старою?

а) 2^{-32}; б) 2^{-31}; в) 2^{-64}; г) 2^{-128}; д) 2^{-4096}.

73. За якої умови період вихідної послідовності LFSR довжини n над скінченним полем $GF(q)$ набуває максимального значення?

а) мінімальний многочлен, утворений з послідовності відводів регістра, має бути незвідним над полем;
б) степінь характеристичного многочлена, утвореного з послідовності відводів регістра, має бути більшою за n;
в) характеристичний многочлен, утворений з послідовності відводів регістра, має бути примітивним над полем;
г) початкове заповнення регістру має дорівнювати 111…1;
д) порядок характеристичного многочлена, утвореного з послідовності відводів регістра, має дорівнювати n.

74. Період вихідної бітової послідовності регістра зсуву з лінійним зворотним зв'язком довжини n не може перевищити значення

а) 2^n-1; б) 2^n; в) $2^{n-1}+1$; г) $2^{n-1}-1$.

75. Якщо LFSR при початковому заповненні x генерує послідовність $x_0x_1x_2\ldots$, а при початковому заповненні s – послідовність $s_0s_1s_2\ldots$, то при початковому заповненні $x \oplus s$ LFSR видаватиме на виході послідовність

а) $x_0s_0,\ x_1s_1,\ x_2s_2, \ldots$; б) $x_0, s_0, x_1, s_1, x_2, s_2, \ldots$;

в) $x_0+s_0,\ x_1+s_1,\ x_2+s_2, \ldots$; г) інша відповідь.

76. Який зв'язок між многочленом $P(x)$ зворотного зв'язку n-бітового LFSR і його характеристичним многочленом $P^*(x)$?

а) $P^*(x) = x^n P\left(\frac{1}{x}\right)$; б) $P^*(x) = x^n - P(x)$;

в) $P^*(x) = P(x) + 1$; г) $P^*(x) = \frac{P(x)}{x-1}$.

77. Бітова послідовність, генерована LFSR, однозначно визначається за допомогою

а) многочлена зворотного зв'язку;
б) характеристичного многочлена;
в) початкового заповнення;
г) правильні відповіді а) і в);
д) правильні відповіді б) і в).

78. Установіть відповідність між многочленами, що описують лінійну рекурентну послідовність, генеровану LFSR, та її властивостями.

Многочлен і його характеристики	Властивості послідовності
1) характеристичний многочлен;	а) лінійна складність;
2) мінімальний многочлен;	б) період;
3) порядок мінімального многочлена;	в) многочлен зворотного зв'язку;
4) порядок закону рекурсії;	г) многочлен зворотного зв'язку найкоротшого регістра, здатного генерувати послідовність

78. t – максимальний час неперервної роботи криптографічного засобу для захисту інформації, основаного на потоковому шифрі, v – швидкість передачі у каналі зв'язку, n – розрядність послідовності на виході генератора гами. За цих умов мінімальний період гами, необхідний для безпечного шифрування має бути більшим, ніж…

а) $t + vn$; б) $t(\frac{v^2}{n^2} + n)$; в) $0,5tvn$; г) tvn.

80. Алгоритму Берлекемпа – Мессі дає змогу

а) визначити лінійну складність числової послідовності, згенерованої LFSR;
б) знайти коефіцієнти многочлена зворотного зв'язку LFSR, що породив дану числову послідовність;
в) розв'язати разом обидві задачі, описані в пунктах а) і б);
г) жодної з описаних задач алгоритм нездатний розв'язати.

81. Яка часова складність алгоритму Берлекемпа – Мессі для обчислення лінійної складності числової бітової послідовності, згенерованої LFSR довжини n?

а) $O(n^2)$; б) $O(n^3)$; в) $O(\log_2 n)$;
г) $O(2^n)$; д) $O(n)$; е) $O(\sqrt{n})$.

82. Скільки послідовних бітів гами потрібно задати, щоб за допомогою алгоритму Берлекемпа – Мессі однозначно визначити многочлен зворотного зв'язку для регістру, що згенерував дану послідовність максимальної довжини, якщо кількість чарунокрегістру дорівнює n?

а) n^2; б) $2n$; в) $\log_2 n$; г) 2^n; д) n.

83. У якому випадку лінійна складність бітової послідовності дорівнює нескінченності?

а) якщо послідовність нульова $000...0$;
б) якщо послідовність має вигляд $(0,0,0,...,01)$;
в) якщо послідовність має вигляд $(0,1,0,1,...,0,1)$;
г) коли не існує регістру зсуву із зворотним лінійним зв'язком, що може генерувати таку послідовність;
д) нескінченну лінійну складність може мати тільки нескінченна послідовність.

84. Уставте пропущені слова у наведені твердження.

1. Якщо характеристичний многочлен LFSR є …., то генерована ним послідовність буде m-послідовністю;
2. Якщо характеристичний многочлен LFSR є …., то період генерованої ним послідовності залежатиме від початкового заповнення;
3. Якщо характеристичний многочлен LFSR є …., то генерована ним послідовність не відноситься до m-послідовністей, але довжина її періода не залежатиме від початкового заповнення.

а) звідний; б) незвідний; в) примітивний.

85. Буліва функція, на основі якої побудовано комбінувальний або фільтрувальний генератор потокового шифру, має бути

а) збалансованою; б) асоціативною;
в) монотонною; г) з високою нелінійністю;
д) симетричною; е) з кореляційним імунітетом;
є) самодвойстою; ж) лінійною;
з) задовольняти суворому лавинному критерію.

86. Буліва функція має кореляційний імунітет порядку k, якщо

а) її вихідна послідовність збалансована;
б) зміна однієї вхідної координати спричиняє заміну k значень вихідної послідовності;
в) на протилежних один одному наборах з k аргументів функція приймає протилежні значення;
г) її вихідна послідовність статистично не залежить від будь-якої підмножини з k вихідних координат.

87. Мінімальна відстань Хеммінга між булівою функцією від n змінних до множини афінних функцій називається

а) збансованістю функції;
б) нелінійністю функції;
в) алгебраїчним імунітетом функції;
г) вагою функції за Хеммінгом.

88. Генератор Геффе складається з трьох LFSR максимальної довжини, комбінувальна функція $f(x_1,x_2,x_3)=x_1x_2 \oplus x_2x_3 \oplus x_3$. За умови, що довжини L_1,L_2,L_3 регістрів виражаються взаємно простими числами, період вихідної послідовності генератора дорівнює

а) $2^{L_1L_2+L_2L_3+L_3}$; б) $2^{L_1}\cdot 2^{L_2}\cdot 2^{L_3}$;

в) $2^{L_1}+2^{L_2}+2^{L_3}-1$; г) $(2^{L_1}-1)(2^{L_2}-1)(2^{L_3}-1)$.

89. Генератор Геффе складається з трьох LFSR максимальної довжини, комбінувальна функція $f(x_1,x_2,x_3)=x_1x_2 \oplus x_2x_3 \oplus x_3$. За умови, що довжини L_1,L_2,L_3 регістрів дорівнюють 5, 7 і 11 відповідно, лінійна складність вихідної послідовності генератора становить

а) 23; б) 88; в) 93; г)123; д)385.

90. Який відсоток бітів гами на виході генератора Геффе (рис. 4.12) збігається з відповідним бітами вихідної послідовності першого регістра?

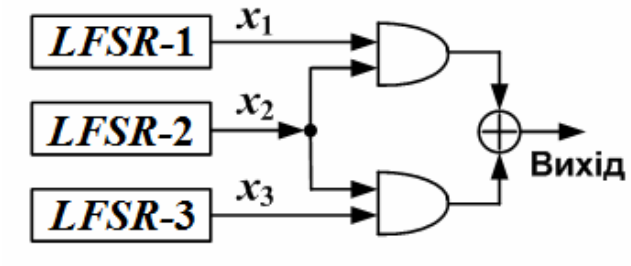


Рис. 4.12

а) 75%; б) 50%;
в) 33%; г) 25%;
д) 66%.

91. Завдяки чому забезпечується нелінійність гами у шифрі A5/1?

а) роботі регістрів за правилом «stop-and-go»;
б) частій ініціалізації алгоритму;
в) застосуванню у регистрах проріджених многочленів оберненого зв'язку;
г) каскадному з'єднанню трьох регістрів;
д) завдяки непарній кількості регістрів, задіяних в генераторі.

92. Яка ймовірність зсуву вмісту одного регістру з лінійним зворотним зв'язком в одному такті роботи алгоритму A5/1?

а) 1/4; б) 3/4; в) 1/2; г) 1/3; д) 2/3.

93. На вхід якої булівої функції подаються «серединні» біти вихідних послідовностей LFSR для змінного керування тактуванням в алгоритмі A5/1?

а) $f(x_1, x_2, x_3) = x_1 x_2 x_3$;
б) $f(x_1, x_2, x_3) = x_1 + x_2 + x_3$;
в) $f(x_1, x_2, x_3) = x_1 x_2 + x_1 x_3 + x_2 x_3$;
г) $f(x_1, x_2, x_3) = x_1 x_2 + x_1 x_3 + x_2 x_3 + x_1 x_2 x_3$.

94. На рис. 4.13 подана схема роботи генератора ключового потоку шифру …

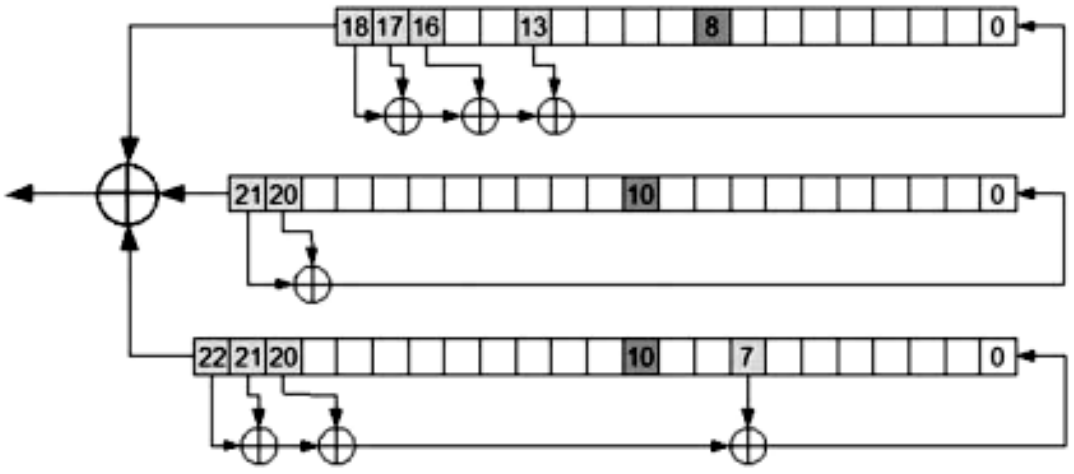


Рис. 4.13

а) RC4; б) SNOW; в) A5/1; г) SEAL.

95. Яку з наступних криптосистем можна вибрати як високошвидкісну систему шифрування при передачі даних?

а) MAC; б) MD5; в) RC4; г) RSA.

96. Яка довжина ключа потокового шифру A5/1?

а)256 бітів; б)128 бітів; в) 64 біти; г) 32 біти; д) інша відповідь.

97. Генератор «stop-and-go» побудовано на трьох LFSR. Мінімальні характеристичні многочлени $F_1(\lambda)=\lambda^2+\lambda+1$ і $F_2(\lambda)=\lambda^3+\lambda+1$ двох регістрів є примітивними. Виберіть серед наведених нижче многочленів той, що міг би бути характеристичним многочленом третього регістра за умови, що період вихідної послідовності має бути якомога більшим.

а) $F_3(\lambda)=\lambda^4+\lambda+1;$ б) $F_3(\lambda)=\lambda^7+\lambda+1;$

в) $F_3(\lambda)=\lambda^9+\lambda+1;$ г) будь-який з многочленів а) – б).

98. Генератор «stop-and-go» складається з двох регістрів LFSR-1 і LFSR-2, вихідні послідовності яких $\{a(t)\}$ і $\{b(t)\}$ відповідно. Принцип роботи генератора: якщо на момент часу t на виході регистра LFSR-2 з'являється біт $b_t=1$, то генератор видає поточний біт $a(i_t)=1$, генерований регістром LFSR-1. У разі ж появи вихідного біта $b_t=0$ генератор повторно видає попередній біт $a(i_t-1)$, генерований LFSR-1:

$$u(t)=\begin{cases} a(i_t), \text{ якщо } b_t=1; \\ a(i_t-1), \text{ якщо } b_t=0. \end{cases}$$

Знайдіть перші 20 бітів на виході генератора за відомими вихідними послідовностями регістрів:

LFSR-1 – 10000101011101100011,
LFSR-2 – 11111011100010101100.

а) 10001100101001001111; б) 00000100011101010011;
в) 01111010100010011100; г) 10000010111100111110.

99. З яким з нижченаведених тверджень Ви ***не*** згодні?

а) для генерування псевдовипадкової послідовності можна використати алгоритм 3DES;
б) істінно випадкова числова послідовність має бути непередбачуваною і невідтворюваною;
в) числова бітова послідовність з великою лінійною складністю обов'язково має непогані випадкові властивості;

г) максимальний період лінійної рекурентної послідовності над полем $GF(q)$ порядку q може дорівнювати лише $q^n - 1$.

100. Як називається генератор псевдовипадкових числових послідовностей, що складаються з бітів парності чисел $x_i = x_{i-1}^2 (\mathrm{mod}\, n)$, де $i = 1, 2, ...,$ $n = pq$, p, q – великі прості числа?

а) генератор Фібоначчі із запізненням;
б) генератор BBS;
в) квадратичний конгруентний генератор;
г) лінійний конгруентний генератор;
д) генератор Міллера – Рабіна.

101. Вихідна послідовність генератора BBS складається з бітів парності чисел, утворених за законом

а) $x_i = x_{i-1}^2 \bmod n$, де $n = pq$; б) $x_{i+1} = (x_i + x_{i-1}) \bmod n$;

в) $x_{i+1} = (x_i \cdot x_{i-1}) \bmod n$; г) $x_{i+1} = (ax_i^{-1} + b) \bmod n$.

102. Якій умові повинні задовольняти числа p і q, щоб їх добуток доцільно було використати як модуль для генератора BBS?

а) бути простими числами Марсенна ; б) $p \equiv q \not\equiv 4 (\mathrm{mod}\, 3)$;

в) символ Лежандра $\left(\frac{p}{q}\right) = 1$; г) $p = q^2$; д) $p \equiv q \equiv 3 (\mathrm{mod}\, 4)$.

103. Для збільшення періоду вихідної псевдовипадкової послідовності генератора BBS для чисел p і q має виконуватися умова

а) $p \equiv q \equiv 4 (\mathrm{mod}\, 3)$;
б) $p \equiv q - 3 (\mathrm{mod}\, 2)$;
в) НСД$(\varphi(p-1),\ \varphi(q-1))$ повинен бути малим;
г) $p - 1 = 2^k q$, $q - 1 = 2^m p$, $k \neq m$.

104. Уставте пропущені слова: «Висока стійкість генератора BBS забезпечена обчислювальною складністю задачі…., що покладена в основу його роботи».

а) піднесення до степеня за модулем;
б) тестування чисел щодо простоти;
в) дискретного логарифмування;
г) факторизації великих чисел.

105. Два користувача для безпечного листування за допомогою електронної пошти планують використати потоковий шифр RC4 з 256-бітовим ключем k. Процедура шифрування бітового повідомлення m: $c = RC4(\mathrm{IV} \,||\, k) \oplus m$, де символ || позначає конкатенацію, а IV –випадково вибраний 80-бітовий вектор. Отримувачу інформації надсилається бітовий рядок $\mathrm{IV} \,||\, c$. Які з нижченаведених тверджень описують розшифрування шифротексту?

а) $m = RC4(\mathrm{IV} \,||\, k) \oplus c$;
б) $m = RC4(\mathrm{IV} \,||\, c) \oplus k$;
в) $m = RC4(k \,||\, c) \oplus \mathrm{IV}$;
г) $m = RC4(\mathrm{IV} \,||\, k \oplus c)$.

106. Який варіант шифрування на основі алгоритму DES використовується у псевдовипадковому бітовому генераторі із стандарту ANSI X9-52 ?

а) $DESX$;
б) $2DES$;
в) $3DES$ з трьома ключами у режимі EEE;
г) $3DES$ з двома ключами у режимі EDE.

РОЗДІЛ 5. КРИПТОГРАФІЯ З ВІДКРИТИМ КЛЮЧЕМ

Задача 1. Припустимо, абонент **A** використовує для шифрування криптосистему RSA з великим модулем n, наприклад, довжина якого 1024 біти. Щоб надіслати йому шифроване текстове повідомлення, абонент **B** ототожнює українську абетку з кільцем лишків Z_{33}, записує числовий еквівалент повідомлення та окремо шифрує кожну його букву. Опишіть, як можна дешифрувати шифрований текст, отриманий у такий спосіб (модуль не факторизувати). Ілюструючи атаку, дешифруйте шифротекст, здобутий при побуквеному шифруванні одного слова українською за допомогою криптосистеми RSA з модулем $n = 18721$ і відкритою експонентою $e = 11$:

2080 12254 0 12254 12254 6627.

Як можна запобігти такого несанкціонованого дешифрування?

Р о з в' я з а н н я. При запропонованому способі шифрування простір відкритих текстів складається з 33 елементів (букв абетки). Це означає, що для кожної букви y_i шифротексту потрібно перевірити лише 33 можливі букви j відкритого тексту:

$$y_i \overset{?}{\equiv} j^e \pmod{18721}, \quad j = 0,1,2,...,32.$$

Аналіз шифротексту виявляє, що у відкритому тексті, по-перше, третьою буквою може бути лише буква А (нумерація букв абетки з нуля), а по-друге, дві збіжні передостанні букви найімовірніше можуть бути біграмою НН, досить поширеною наприкінці українських слів. Буква Н має номер 17, тому перевіряємо

$$17^{11} \pmod{18721} \equiv 12254 - \text{правильно}.$$

Отже, у шуканому слові тепер відомі чотири букви:

□НАНН□.

Очевидно, що це фрагмент слова ЗНАННЯ, у чому упевнюємося за допомогою перевірки.

Один з шляхів розв'язання проблеми – шифрування кількох букв одночасно в одному блоці, хоча навіть при такому підході криптосистема RSA залишається детерміністичною. Інший спосіб створення стійкої криптосистеми полягає у доповненні відкритого тексту перед шифруванням випадковими даними.

Задача 2. При зашифруванні відкритого тексту за допомогою криптосистеми RSA з відкритим ключем (n, e) було отримано шифротекст C. Криптоаналітик, перехопивши його, помітив, що

$C^{100} \equiv 1 \bmod n$, а НСД$(e, 100) = 1$. Як використавши цю інформацію він може прочитати відкритий текст?

Р о з в' я з а н н я. Оскільки $M = C^d \bmod n$, то

$$M^{100} = C^{100d} \equiv 1 \bmod n,$$

де d – секретний ключ криптосистеми. За умовою НСД$(e, 100) = 1$, тому існує обернений елемент $\alpha = e^{-1} (\mathrm{mod} 100)$. Тоді

$$C^{\alpha} \equiv M^{e\alpha} \bmod n \equiv M^{e\alpha - 1} M (\mathrm{mod}\, n).$$

Беручи до уваги, що $\alpha e \equiv 1 (\mathrm{mod} 100)$ і $M^{100} \equiv 1 \bmod n$, можна записати $M^{e\alpha - 1} \equiv 1 (\mathrm{mod}\, n)$, звідки $M \equiv C^{\alpha} (\mathrm{mod}\, n)$.

Задача 3. Нові рекорди факторизації великих чисел вимагають постійно збільшувати модуль криптосистеми RSA, зворотною стороною чого стає низька швидкість криптографічних перетворень. Припустимо, що при одному множенні або піднесенні до квадрату k-бітових чисел виконується ck^2 операцій, де c – деяка константа. Наскільки повільнішим буде розшифрування з ключем RSA-1024, ніж з ключем RSA-512? Врахувати, що за евристичними оцінками при невеликих значеннях відкритої експоненти довжина закритої близька до довжини модуля.

Р о з в' я з а н н я. Зашифрування/розшифрування у криптосистемі RSA зводиться до операції модульного піднесення до степеня. Для спрощення розрахунків приймемо, що $k \approx k - 1$. Якщо показник степеня випадковий, то для піднесення до степеня з k-бітовим показником потрібно в середньому виконати k піднесень до квадрату і $k/2$ множень, тобто загалом $1{,}5k$ множень. Часова складність одного множення (піднесення до квадрату) складає ck^2, тому складність одного піднесення до степеня дорівнюватиме $1{,}5ck^3$ операцій. Обчислюємо відношення часів:

$$\frac{t_{1024}}{t_{512}} = \frac{1{,}5c(2k)^3}{1{,}5ck^3} = 8.$$

Задача 4. Як відомо, в криптосистемі RSA вибір відкритої експоненти e обмежується умовою НСД$(e, \varphi(n)) = 1$, де $\varphi(n)$ – значення функції Ейлера, n – модуль криптосистеми. Доволі популярним став вибір $e = 3$ або $e = 2^{16} + 1$. Чому ці значення переважають над іншими?

Р о з в’ я з а н н я. Генерування відкритих ключів у асиметричних криптосистемах виконується нечасто і основна складність обчислень у криптоалгоритмі RSA припадає саме на операції піднесення до степеня $M^e (\mathrm{mod}\, n)$ за модулем великого числа n. Якщо показник степеня випадковий, то реалізація піднесення до степеня потребує в середньому k піднесень до квадрату за модулем і $k/2$ множень, де k – довжина двійкового запису показника. Очевидно, час виконання операцій зростатиме із збільшенням кількості ненульових бітів у двійковому зображенні показника. З цього погляду відкриту експоненту вибирають серед простих чисел $2+1=3$, або $2^{16}+1=65537$, двійковий запис яких містить мінімальну кількість одиниць. У цьому разі

$$M^3 \equiv M^2 \cdot M (\mathrm{mod}\, n); \quad M^{2^{16}+1} \equiv (((M^2)^2)^2)^2 \cdot M (\mathrm{mod}\, n).$$

Задача 5. Для модуля криптосистеми RSA вибрано множники $p=3307$ і $q=4409$, відкрита експонента $e=139$. Чи можна знайти закриту експоненту d з системи порівнянь

$$\begin{cases} d \equiv -5 (\mathrm{mod}\, 24), \\ d \equiv 111 (\mathrm{mod}\, 551)? \end{cases}$$

Р о з в’ я з а н н я. Оскільки закрита і відкрита експоненти криптосистеми RSA зв’язані співвідношенням $ed \equiv 1 \mathrm{mod}\, \varphi(n)$, де $\varphi(n) = \varphi(pq) = (p-1)(q-1)$, то, очевидно що d буде розв’язком системи порівнянь

$$\begin{cases} ed \equiv 1 (\mathrm{mod}\, p-1), \\ ed \equiv 1 (\mathrm{mod}\, q-1). \end{cases}$$

За умовою задачі ця система набуває вигляду

$$\begin{cases} 139d \equiv 1 (\mathrm{mod}\, 3306), \\ 139d \equiv 1 (\mathrm{mod}\, 4408). \end{cases}$$

Розв’язавши обидва порівняння відносно d, маємо

$$\begin{cases} d \equiv 1213 (\mathrm{mod}\, 3306), \\ d \equiv 2315 (\mathrm{mod}\, 4408). \end{cases}$$

Оскільки відображення $Z_n^* \simeq Z_p^* \times Z_q^*$ є ізоморфізмом, то

$$Z_{3307}^* \times Z_{4409}^* \simeq Z_{3306} \times Z_{4408} \simeq Z_6 \times Z_{551} \times Z_8 \times Z_{551}.$$

Тоді

$$\begin{cases} d \equiv 1213 (\mathrm{mod}\, 6), \\ d \equiv 1213 (\mathrm{mod}\, 551), \\ d \equiv 2315 (\mathrm{mod}\, 8), \\ d \equiv 2315 (\mathrm{mod}\, 551) \end{cases} \Rightarrow \begin{cases} \begin{cases} d \equiv 1 (\mathrm{mod}\, 6), \\ d \equiv 3 (\mathrm{mod}\, 8), \end{cases} \\ d \equiv 111 (\mathrm{mod}\, 551) \end{cases} \Rightarrow \begin{cases} d \equiv -5 (\mathrm{mod}\, 24), \\ d \equiv 111 (\mathrm{mod}\, 551). \end{cases}$$

Закрита експонента буде розв'язком останньої системи порівнянь.

Задача 6. Для утворення модуля криптосистеми RSA вибрано випадкове число $p < 2^{1000}$ і число $q = 3 \cdot 2^k - 1$, де $1 < k < 1000$. Як можна атакувати таку криптосистему?

Р о з в' я з а н н я. Оскільки $n = pq$, то можна знайти НСД$(3 \cdot 2^k - 1, n)$ для $k = 1, 2, ..., 1000$, що дозволить факторизувати модуль та зламати систему.

Задача 7. Знайдіть ймовірність того, що відкритий текст M, що шифрується за допомогою криптосистеми RSA з відкритим ключем $(n = pq,\ e)$, виявиться не взаємно простим з модулем криптосистеми. Чому дорівнюватиме ця ймовірність, якщо множники p і q будуть більші, ніж 10^{100}?

Р о з в' я з а н н я. Значення функції Ейлера $\varphi(n)$ дорівнює кількості натуральних чисел, менших за n і взаємно простих з n. А відтак, решта цілих чисел з проміжку $(1, n)$ – не взаємно прості з n. Їх кількість

$$n - \varphi(n) = n - (p-1)(q-1) = n - pq + p + q - 1 = p + q - 1.$$

Отже, ймовірність того, що відкритий текст M не взаємно простий з модулем криптосистеми складає

$$P = \frac{p+q-1}{n} = \frac{p+q-1}{pq} = \frac{1}{q} + \frac{1}{p} - \frac{1}{pq}.$$

При $p, q \sim 10^{100}$ ця ймовірність становить

$$P = 10^{-100} + 10^{-100} - 10^{-200} < 10^{-99}.$$

Задача 8. Нехай $n = pq$ – модуль криптосистеми RSA, N – кількість файлів, що підлягають шифруванню, $e_1, e_2, ..., e_N$ – взаємно прості цілі числа, які також взаємно прості із значенням $\varphi(n) = (p-1)(q-1)$, тобто

$$\text{НСД}(e_i, e_j) = 1; \quad \text{НСД}\ (e_i, \varphi(n)) = 1, \quad i \neq j.$$

Числа $e_1, e_2, ..., e_N$ є відкритими ключами. З групи Z_n^* вибрано випадкове число r та зашифровано кожен файл F_i на ключі $K_i = r^{1/e^i}$. Припустимо також, що користувач U дізнався значення $K_U = r^{1/b}$, де $b = \prod_{i \in S_U} e_i$. Покажіть, що він може дешифрувати будь-який файл $i \in S_U$, де множина $S_U \subseteq \{1, 2, ..., N\}$.

Р о з в' я з а н н я. Користувач U, отримавши $K_U = r^{1/b}$, щоб знайти $K_i = 1/e^i$ має обчислити $(K_U)^\gamma$, де $\gamma = \prod_{i \neq j;\ j \in S_U} e_i$. За побудовою, якщо $i \in S_U$, то $\gamma = b/e_i$, звідки випливає $(K_U)^\gamma = r^{(1/b)(b/e_i)} = r^{1/e_i}$.

Задача 9. Чи можна для криптосистеми RSA у якості модуля вибрати добуток трьох різних простих чисел $n = pqr$? Як має працювати криптосистема у цьому випадку? Які співвідношення мають задовольнити відкрита та закрита експоненти? Чи підвищує це безпечність шифрування?

Р о з в' я з а н н я.

Генерація ключів: 1). Вибрати три різних простих числа p, q і r та обчислити модуль $n = pqr$;

2). Вибрати відкриту експоненту e так щоб,

$$\text{НСД}((p-1)(q-1)(r-1), e) = 1.$$

3) Визначити закриту експоненту d з рівності

$$de \equiv 1 (\text{mod}(p-1)(q-1)(r-1)).$$

p, q і r і d – закриті параметри; n і e – відкриті параметри.

Рівняння шифрування: $C = M^e (\text{mod}\, n)$.

Рівняння розшифрування: $M = C^d (\text{mod}\, n)$.

Доведення коректності шифрування: значення функції Ейлера $\varphi(n) = (p-1)(q-1)(r-1)$. За малою теоремою Ферма для будь-якого простого числа p і $M \not\equiv 0 \bmod p$ справедливе порівняння $M^{p-1} \equiv 1 (\text{mod}\, p)$. Якщо $M \equiv 0 \bmod n$, то очевидно, розшифрування діє

коректно. Оскільки d – обернений елемент до числа e за модулем $\varphi(n)$, тобто $ed \equiv 1(\mathrm{mod}\,\varphi(n))$, то для деякого цілого числа k буде виконано рівність $ed = 1 + k\varphi(n)$. А відтак, при $M \not\equiv 0 \bmod p$ матимемо

$$C^d = (M^e)^d = M^{ed} = M^{k\varphi(n)+1} = M^{k(p-1)(q-1)(r-1)+1} \equiv$$
$$\equiv M \cdot M^{k(p-1)(q-1)(r-1)}(\mathrm{mod}\,p) \equiv M \cdot M^{\lambda(p-1)} \equiv M(\mathrm{mod}\,p),$$

тобто $C^d - M$ ділиться на p. Аналогічно можна показати, що $C^d - M$ ділиться на q і r. Тоді $C^d - M \equiv 0(\mathrm{mod}\,pqr)$, $C^d \equiv M(\mathrm{mod}\,n)$.

Використання добутку трьох простих чисел не надає криптосистемі додаткової стійкості, бо в основі алгоритму RSA лежить складність факторизації великих чисел. Час такої факторизації залежить від розмірів простих чисел, що утворюють добуток, а не від їх кількості.

Задача 10. Припустимо, що у мережі два абоненти використовують для зв'язку криптосистему RSA. Їхні модулі різні та відповідно дорівнюють n_1 і n_2 ($n_1 \neq n_2$). Як можна зламати криптосистему за умови, що модулі не є взаємно простими?

Р о з в' я з а н н я. Покладемо для зручності $n_1 > n_2$, $n_1 = p_1 q_1$, де p_1 та q_1 – прості. $\Rightarrow$ Можливі множники числа n_1 – це $1; p_1; q_1; n_1$. З умови задачі НСД$(n_1, n_2) > 1$, а за припущенням $n_1 > n_2$, тому НСД$(n_1, n_2) \neq n_1$. Отже, або НСД$(n_1, n_2) = p_1$, або НСД$(n_1, n_2) = q_1$.

Розглянемо випадок НСД$(n_1, n_2) = p_1$. Тоді $p_1 \mid n_2$, що означає, що p_1 – один з простих множників числа n_2. Тобто $n_2 = p_1 q_2$, де q_2 – просте. Таким чином, визначивши НСД(n_1, n_2), ми будемо знати p_1. Тоді $q_1 = \dfrac{n_1}{p_1}$; $q_2 = \dfrac{n_2}{p_1}$ – секретні ключі обох абонентів стають відомими. Випадок НСД$(n_1, n_2) = q_1$ аналогічний.

Задача 11. Нехай відкритий текст M зашифровано за допомогою криптосистеми RSA на відкритому ключі (n, e) і отримано шифрований текст C. Криптоаналітик умовив власника закритого ключа послідовно виконати розшифровування шифротексту $C_1 = 2^e C(\mathrm{mod}\,n)$ стільки

разів, поки не виникне текст C. Як криптоаналітик зможе за цією інформацією розкрити відкритий текст M?

Р о з в' я з а н н я. Криптоаналітик має відкриті ключі n, e, шифротекст $C_1 = 2^e C (\mathrm{mod}\, n)$ та відкритий текст M_1, який відповідає шифротексту C_1.

$$M_1 \equiv C_1^d (\mathrm{mod}\, n) \equiv (2^e C)^d (\mathrm{mod}\, n) \equiv 2^{ed} C^d (\mathrm{mod}\, n) \equiv 2^{ed} M (\mathrm{mod}\, n).$$

Оскільки $ed \equiv 1 (\mathrm{mod}\, \varphi(n))$, $\varphi(n)$ – функція Ейлера, то $ed = 1 + k\varphi(n)$, $k \in Z$. Тоді

$M_1 \equiv 2^{1+k\varphi(n)} M (\mathrm{mod}\, n) \equiv 2M (2^{\varphi(n)})^k (\mathrm{mod}\, n) \equiv 2M$ (використано теорему Ейлера). Отже $M \equiv 2^{-1} \cdot M_1$.

Задача 12. Нехай p і q – прості числа, $p \neq q$ і $(n = pq,\ e)$ відкритий ключ криптосистеми RSA. Повідомлення M, для якого при зашифруванні матиме місце $M^e \equiv M (\mathrm{mod}\, n)$, називається нерухомим блоком (або фіксованою точкою). Скільки нерухомих блоків існує у групі Z_n^*?

Р о з в' я з а н н я. Оскільки елемент M є оборотним у групі Z_n^*, то порівняння $M^e \equiv M (\mathrm{mod}\, n)$ еквівалентно порівнянню $M^{e-1} \equiv 1 (\mathrm{mod}\, n)$. Це означає, що $M^{e-1} = 1 + kn = 1 + kpq$, де $k \in Z$. Тоді

$$\begin{cases} M^{e-1} \equiv 1 \bmod p, \\ M^{e-1} \equiv 1 \bmod q. \end{cases}$$

Очевидно, НСД$(p, q) = 1$, тому отриману систему можна розв'язати за китайською теоремою про остачі. Якщо S_p і S_q – множини розв'язків першого і другого порівнянь системи відповідно, то потужність цих множин

$$\left|S_p\right| = \text{НСД}(e-1, p-1), \quad \left|S_q\right| = \text{НСД}(e-1, q-1).$$

Тоді

$$\begin{cases} M \equiv s_p \bmod p, \\ M \equiv s_q \bmod q, \end{cases}$$

де $s_p \in S_p$, $s_q \in S_q$. За китайською теоремою про остачі кількість розв'язків $M \in Z_n^*$ системи порівнянь визначається добутком

$$\left|S_p\right|\left|S_q\right| = \text{НСД}(e-1, p-1)\cdot \text{НСД}(e-1, q-1).$$

Задача 13. Нехай у криптосистемі RSA відкритий ключ – модуль $n = 667$ і відкрита експонента $e = 83$, закритий ключ – прості числа $p = 23$ і $q = 29$ та закрита експонента $d = 475$. Визначте усі нерухомі блоки при такому виборі ключів (див. умови попередньої задачі).

Р о з в' я з а н н я. Умова нерухомості блока $M^{83} \equiv M (\text{mod}\, 667)$ рівносильна системі

$$\begin{cases} M^{83} \equiv M (\text{mod}\, 23), \\ M^{83} \equiv M (\text{mod}\, 29) \end{cases}$$

або

$$\begin{cases} \left[\begin{array}{l} M^{83} \equiv 0 (\text{mod}\, 23), \\ M^{82} \equiv 1 (\text{mod}\, 23); \end{array}\right. \\ \left[\begin{array}{l} M^{83} \equiv 0 (\text{mod}\, 29), \\ M^{82} \equiv 1 (\text{mod}\, 29). \end{array}\right. \end{cases}$$

За малою теоремою Ферма якщо $M \not\equiv 0 (\text{mod}\, 23)$, то $M^{22} \equiv 1 (\text{mod}\, 23)$. Оскільки порядки чисел є дільниками $p-1$, то з умов $M^{82} \equiv 1 (\text{mod}\, 23)$, $M^{22} \equiv 1 (\text{mod}\, 23)$ випливає, що

$$M^A \equiv 1 (\text{mod}\, 23) = M^2 \equiv 1 (\text{mod}\, 23),$$

де $ord_{23} M$ ділить $A = \text{НСД}(82, 22) = 2$. Тому $ord_{23} M = 2$ і нам не потрібно випробовувати інші дільники числа A.

Аналогічно отримаємо $M^B = M^2 \equiv 1 (\text{mod}\, 29)$ при $B = \text{НСД}(82, 28) = 2$. Звідси

$$\begin{cases} \left[\begin{array}{l} M \equiv 0 (\mathrm{mod}\, 23), \\ M^2 \equiv 1 (\mathrm{mod}\, 23); \end{array}\right. \\ \left[\begin{array}{l} M \equiv 0 (\mathrm{mod}\, 29), \\ M^2 \equiv 1 (\mathrm{mod}\, 29) \end{array}\right. \end{cases}$$

або

$$\begin{cases} M \in \{0,1,-1\} (\mathrm{mod}\, 23), \\ M \in \{0,1,-1\} (\mathrm{mod}\, 29). \end{cases}$$

Розв'язок системи порівнянь $\begin{cases} M \equiv a (\mathrm{mod}\, 23), \\ M \equiv b (\mathrm{mod}\, 29) \end{cases}$ легко визначимо за китайською теоремою про остачі у вигляді $M = 116a + 552b \bmod 667$. При $a \in \{0,1,-1\}$, $b = \in \{0,1,-1\}$ дістанемо таку ж сукупність нерухомих блоків, як і при розв'язанні за першим способом: 0, 1, 115, 116, 231, 436, 551, 552, 666.

Задача 14. $(n,e) = (70457950271,\ 65355599089)$ – відкриті ключ криптосистеми RSA, де $n = pq$. Виявилось, що число $e-1$ ділиться без остачі на $p-1$. Використавши цю інформацію, факторизуйте модуль криптосистеми.

Р о з в' я з а н н я. Оскільки $p-1$ є множником числа $e-1$, то $M^e \equiv M \bmod p$ для всіх M і $M^{e-1} \equiv 1 \bmod p$ для всіх M, що не діляться на p. Обчислимо при $M = 2$ вираз $Y = M^{e-1} (\mathrm{mod}\, n)$:

$$Y = 2^{65355599088} (\mathrm{mod}\, 70457950271) = 51432365529.$$

Тоді, визначивши

$$\text{НСД}(Y-1, n) = \text{НСД}(51432365528, 70457950271) = 223549,$$

факторизуємо модуль криптосистеми

$$70457950271 = 223549 \cdot 315179.$$

Задача 15. Зловмисник перехопив шифрований текст C, надісланий користувачеві криптосистеми RSA з відкритим ключем (n,e).

Як він може дешифрувати перехоплений шифротекст, провівши атаку на основі: а) вибраного шифротексту; б) вибраного відкритого тексту?

Р о з в' я з а н н я. За схемою RSA має місце $C = M^e \bmod n$; $M = C^d \bmod n$, де d – закритий ключ.

а) Зловмисник довільно вибирає значення $C_1 \in Z_n$ та умовляє законного користувача розшифрувати C_1. Нехай значенню C_1 відповідає відкрите повідомлення M_1. Далі зловмисник просить користувача розшифрувати текст $C_2 = C \cdot C_1^{-1}$ та отримує відкритий текст M_2. Тепер

$$M_1 \cdot M_2 = C_1^{\,d} \cdot C_2^{\,d} = C_1^{\,d} \cdot C^d \cdot C_1^{\,-d} = C^d = M^{ed} = M \bmod n;$$

б) Зловмисник спочатку довільно вибирає відкритий текст $M_1 \in Z_n$ і шифрує його на відкритому ключі користувача $C_1 = M_1^{\,e} \bmod n$, а потім пропонує користувачеві розшифрувати значення $C_2 = C \cdot C_1^{-1}$ та надіслати йому результат розшифрування текст M_2. Відкритий текст M відновлюється таким чином

$$M_1 \cdot M_2 = M_1 \cdot C_2^{\,d} = M_1 \cdot C^d \cdot C_1^{\,-d} = M_1 \cdot C^d \cdot M_1^{\,-1} = (M^e)^d = M \bmod n.$$

Задача 16. Однакове повідомлення надіслано двом користувачам криптосистеми RSA, які мають відкриті ключі $(32967409;\ 65537)$ та $(32967409;\ 4125)$ відповідно. Перший користувач отримав шифротекст $C_1 = 19746863$, а другий – шифротекст $C_2 = 6219526$. Прочитайте відкрите повідомлення за умови, що перехоплені обидві криптограми (абетка українська).

Р о з в ' я з а н н я. Модуль однаковий $n = 32967409$, а відкриті експоненти різні: $e_1 = 65537$, $e_2 = 4125$. Очевидно, що

$$\text{НСД}(e_1, e_2) = 1.$$

Обчисливши обернений елемент

$$t_1 \equiv e_1^{\,-1} \bmod e_2 \equiv 65537^{-1} \bmod 4125 \equiv 98 \bmod 4125,$$

визначимо число $t_2 = \dfrac{t_1 e_1 - 1}{e_2} = \dfrac{98 \cdot 65537 - 1}{4125} = 1557$. Тоді

$$C_1^{t_1} C_2^{-t_2} (\mathrm{mod}\, n) \equiv (M^{e_1})^{t_1} (M^{e_2})^{-t_2} \equiv M^{e_1 t_1} M^{-e_2 t_2} \equiv$$

$$\equiv M^{1+e_2 t_2} M^{-e_2 t_2} \equiv M .$$

Отже, за формулою $M \equiv C_1^{t_1} C_2^{-t_2} (\mathrm{mod}\, n)$ відновлюємо відкритий текст:

$$M \equiv 19746863^{98} \cdot 6219526^{-1557} (\mathrm{mod}\, 32967409) \equiv$$

$$\equiv 27183900 \cdot 11435013^{15557} \bmod 32967409 \equiv 3001600 .$$

Розшифрованому цифровому запису відкритого повідомлення 3001600 (або $03\ \ 00\ 16\ \ 00$) відповідає слово ГАМА.

Задача 17. Уявіть, що Ви послали одне й те саме відкрите повідомлення $m = 175$ трьом користувачам криптосистеми RSA, зашифрувавши його за допомогою їх відкритих ключів: $(n_1, 3) = (8383, 3); (n_2, 3) = (8453, 3);\ \ (n_3, 3) = (8549, 3)$. Криптоаналітик перехопив надіслані Вами відповідні шифровані тексти $C_1 = 2638$; $C_2 = 173$; $C_3 = 7701$ та відшукав ціле число $M = 605794954951$, яке задовольняє нерівність $M < 8383 \cdot 8453 \cdot 8549$ і порівняння

$$M = 2638 \bmod 8383;\ \ M = 173 \bmod 8453;\ \ M = 7701 \bmod 8549 .$$

Будучи впевненим, що $\sqrt[3]{M}$ має бути відкритим текстом, він обчислює $\sqrt[3]{M} \approx 1940{,}24$ і розуміє, що число M не є кубом. Чому атака не вдалася? Запропонуйте іншу базисну атаку, яка дозволить криптоаналітику відновити відкритий текст.

Р о з в’ я з а н н я. Модулі n_1, n_2 і n_3 – попарно не взаємно прості, тому атака на основі використання спільної невеликої відкритої експоненти безпосередньо не розкриває відкритого тексту. Побачивши такий результат, криптоаналітик має знайти найбільший спільний дільник кожної пари модулів, що дозволить йому факторизувати модулі і далі визначити секретну експоненту d. Дійсно, НСД$(n_1, n_3) = 83$.

Задача 18. $(n = 400271,\ e = 117353)$ – відкриті ключі криптосистеми RSA. За допомогою атаки Вінера визначте закриту експоненту d і значення функції Ейлера $\varphi(n)$ та факторизуйте модуль криптосистеми.

Р о з в’ я з а н н я. Коли у криптосистемі RSA закрита експонента $d < \frac{1}{3}\sqrt[4]{n}$, то за відкритим ключем (n, e) можна визначити закриту експоненту d, провівши атаку Вінера за схемою: 1) розкласти число $\frac{e}{n}$ у ланцюговий дріб; 2) знайти всі підхідні дроби P_i / Q_i для ланцюгового дробу; 3) з підхідних дробів послідовним випробуванням знайти той, для якого вираз $eQ_i - 1$ ділиться без остачі на P_i. Тоді $Q_i = d$ – закрита експонента криптосистеми, а $P_i = k$ – таке ціле число, для якого $ed - k\varphi(n) = 1$, де $\varphi(n)$ – значення функції Ейлера.

Отже, починаємо з розкладання дробу $\frac{e}{n}$ у ланцюговий дріб:

$$\frac{e}{n} = \frac{117353}{400271} = \frac{1}{\frac{400271}{117353}} = \frac{1}{3 + \frac{48212}{117353}} = \frac{1}{3 + \frac{1}{2 + \frac{20929}{48212}}} = \ldots =$$

$$= \cfrac{1}{3 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{3 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{11 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \frac{1}{2}}}}}}}}}}}}}.$$

$$\frac{e}{n} = \frac{117353}{400271} = \left[0; \frac{1}{3}, \frac{1}{2}, \frac{1}{2}, \frac{1}{3}, \frac{1}{3}, \frac{1}{2}, \frac{1}{2}, \frac{1}{11}, \frac{1}{1}, \frac{1}{1}, \frac{1}{1}, \frac{1}{4}, \frac{1}{2}\right].$$

Послідовно знайдемо підхідні дроби:

i	-1	0	1	2	3	4	5	6	7	8	9	10	11	12	13
b_i			1	1	1	1	1	1	1	1	1	1	1	1	1
a_i		0	3	2	2	3	3	2	2	11	1	1	1	4	2
P_i	1	0	1	2	5	...									
Q_i	0	1	3	7	17	...									

$$\frac{P_1}{Q_1}=\frac{1}{3};\ \frac{P_2}{Q_2}=\frac{2}{7};\ \frac{P_3}{Q_3}=\frac{5}{17}\ldots$$

Для третього підхідного дробу різниця

$$e\cdot Q_3-1=117353\cdot 17-1=1995000.$$

ділиться націло на $P_3=5$. Покладемо $d=Q_3=17$ – закриту експоненту знайдено. Підставивши у рівняння $ed-k\varphi(n)=1$ значення e, k і d, обчислимо значення функції Ейлера $\varphi(n)=399000$. Щоб знайти множники p і q, на які розкладається модуль криптосистеми, залишається розв'язати систему рівнянь:

$$\begin{cases} n=pq, \\ \varphi(n)=(p-1)(q-1) \end{cases} \Rightarrow \begin{cases} pq=400271, \\ (p-1)(q-1)=399000 \end{cases} \Rightarrow \begin{cases} p=701, \\ q=571. \end{cases}$$

Задача 19. Шифротекст $C=2342$ отримано за допомогою криптосистеми RSA з відкритим ключем $n=2773$, $e=17$. Відновіть відкритий текст, використавши метод безключового читання.

Р о з в' я з а н н я. Припустимо, що відкрита експонента e криптосистеми RSA має порядок r за модулем $\varphi(n)$, де $\varphi(n)$ – значення функції Ейлера. За визначенням порядку це означає, що r – найменше натуральне число, для якого $e^r=1\bmod\varphi(n)$, $1\le e\le\varphi(n)$, НСД$(e,\varphi(n))=1$. Очевидно, у цьому випадку $M^{e^r}=M\bmod n$. Тож необхідно побудувати послідовність шифрувань $M^{e^k}\bmod n$ при $k=1,2,3,...$, поки не виникне даний шифротекст:

$$2342^{17}\bmod 2773\equiv 2365,\ 2365^{17}\bmod 2773\equiv 1157 \text{ і т.д.}$$

У результаті остаточно отримаємо:

2365 1157 2018 985 1421 2101 1664 2047 1539 980

1310 1104 1893 1629 2608 218 1185 1039 602 513

772 744 720 2755 890 2160 2549 926 536 449

2667 2578 182 2278 248 454 1480 1393 2313 2637

2247 1688 1900 2342.

$\downarrow \quad \downarrow$

$M \quad C$

Дійсно, 1900 – відкритий текст, бо $1900^{17} \bmod 2773 \equiv 2342$.

Задача 20. Згенеруйте ключі для криптосистеми RSA-CRT і зашифруйте повідомлення $M = 5$. Проведіть процедуру розшифрування.

Р о з в я' з а н н я. Виберемо $p = 7$ і $q = 11$, НСД$(p-1, q-1) = 2$,

$$n = pq = 77,\ \varphi(n) = (p-1)(q-1) = 60.$$

Нехай $d_p = 5$; НСД$(d_p, p-1) =$ НСД$(5,6) = 1$;

$$d_q = 3;\ \text{НСД}(d_q, q-1) = (3,10) = 1,$$

$$d_p \equiv d_q \bmod 2.$$

Закриту експоненту d визначимо із системи порівнянь $\begin{cases} d \equiv 5 \bmod 6; \\ d \equiv 3 \bmod 10 \end{cases}$. Оскільки НСД$(6,10) \neq 1$, то безпосередньо застосувати китайську теорему про остачі до розв'язання системи неможливо. Тому перепишемо систему у вигляді $\begin{cases} d-1 \equiv 5-1 \bmod 6; \\ d-1 \equiv 3-1 \bmod 10 \end{cases}$ і скоротимо усі частини порівнянь і модуль на 2:

$$\begin{cases} d' \equiv 2 \bmod 3; \\ d' \equiv 2 \bmod 5 \end{cases},\ \text{де } d' = \frac{d-1}{2}.$$

Тоді за китайською теоремою про остачі дістаємо $d' \equiv 11 \bmod 15$, звідки $d = 23$, а відтак, $e \equiv d^{-1} (\bmod \varphi(n)) \Rightarrow e \equiv 23^{-1} \bmod 60 \equiv 47$.

Відкритий ключ – $(77;\ 47)$, секретний ключ – $(7;11;5;\ 3)$.

Шифруємо повідомлення $M = 5$:

$$C \equiv M^e \bmod(n) \equiv 5^{47} \bmod(77) \equiv 3.$$

Розшифрування: $M_p \equiv C^d \bmod p \equiv 3^5 \bmod 7 \equiv 5;$

$$M_q \equiv C^d \bmod(q) \equiv 3^3 \bmod 11 \equiv 5;$$

$$\begin{cases} M \equiv 5 \bmod 7; \\ M \equiv 5 \bmod 11. \end{cases}$$

Знову застосувавши до розв'язання китайську теорему про остачі, отримаємо $M \equiv 5(\bmod 77)$.

Задача 21. Відкриті ключі криптосистеми RSA – $(n = 323,\ e = 5)$, секретна експонента $d = 173$. Для зашифрування використано схему RSA-OAEP:

- довжина відкритого (не поповненого) повідомлення – 3 біти;
- параметри $k_1 = 2$, $k_0 = 4$;
- $G(x_1x_2x_3x_4) = x_1x_2x_3x_4x_1$ для $x_i \in \{0,1\}$, $i = 1,2,3,4$;
- $H(x_1x_2x_3x_4x_5) = (x_1 \oplus x_2)(x_2 \oplus x_3)(x_3 \oplus x_4)(x_4 \oplus x_5)$, де $x_i \in \{0,1\}$, $i = 1,2,3,4,5$.

У чому полягає процес зашифрування/розшифрування? Знайдіть оригінальне трибітове повідомлення, що відповідає шифротексту $C = 116$.

Р о з в' я з а н н я. Схема оптимізованого асиметричного поповнення шифрування (OAEP) може використовуватися з будь-якою однобічною функцією з секретом. Коли її застосовують разом з криптосистемою RSA, то процес зашифрування виглядає так:

- фіксують два параметри схеми – числа $k_0, k_1 > 128$;
- вибирають модуль N криптосистеми довжиною $n = 1024$ бітів;
- вибирають дві криптографічні хеш-функції G і H;
- відкритий текст m – це число у двійковій системі числення, довжиною $(n - k_0 - k_1)$ бітів;

При зашифруванні:

1). Праворуч до відкритого тексту приписують k_1 нулів (число набуває вигляду $m \,||\, 0^{k_1}$, його довжина $n - k_0$ бітів);

2). Генерують рядок r із k_0 випадкових бітів.

3). Рядок r подають на вхід хеш-функції G (хеш-образ $G(r)$ має довжину $n-k_0$ бітів);

4). Обчислюють $X = m00...0 \oplus G(r)$;

5). Рядок X подають на вхід хеш-функції H, яка скорочує довжину рядка до k_0 бітів;

6). Обчислюють $Y = r \oplus H(X)$, де $H(X)$ – хеш-образ рядка X;

7). Шифротекст утворює конкатенація $C = X \| Y$ рядків X і Y.

Для розшифрування потрібно:

1).Знайти $r = Y \oplus H(X)$;

2). Обчислити $m00...0 = X \oplus G(r)$, відділити від зайвих нулів число m.

За умовою задачі $M = C^d \pmod n = 116^{173} \pmod{323} = 243$.

$n = 323_{10} = 101000011_2$, тобто довжина модуля 9 бітів.

$M = 243_{10} = 011110011_2$. Перші п'ять бітів утворюють рядок $X = 01111$, решта чотири біти – рядок $Y = 0011$.

$$H(X) = H(01111) = (1 \oplus 0)(0 \oplus 0)(0 \oplus 0)(0 \oplus 0) = 1000;$$

$$r = H(X) \oplus Y = 1000 \oplus 0011 = 1011;$$

$$X \oplus G(r) = 01111 \oplus 10111 = 11000 = m0^2.$$

Два останніх нулі – це доповнення, тому повідомлення $m = 110_2 = 6_{10}$.

Задача 22. Перевірити за допомогою тесту Міллера – Рабіна простоту числа $n = 104513$, вибравши свідком простоти $a = 3$.

Р о з в' я з а н н я. $n-1 = 2^k \cdot q = 2^6 \cdot 1633 \Rightarrow k = 6,\ q = 1633$.

Обчислимо послідовності $a^{q \cdot 2^i} \mod n,\ i = 0,1,...,k-1$:

$$3^{1633} \equiv 88958 \bmod 104513;$$
$$3^{2 \cdot 1633} \equiv 88958^2 \equiv 10430 \bmod 104513;$$
$$3^{2^2 \cdot 1633} \equiv 10430^2 \equiv 91380 \bmod 104513;$$
$$3^{2^3 \cdot 1633} \equiv 91380^2 \equiv 29239 \bmod 104513;$$
$$3^{2^4 \cdot 1633} \equiv 29239^2 \equiv 2781 \bmod 104513;$$
$$3^{2^5 \cdot 1633} \equiv 2781^2 \equiv -1 \bmod 104513.$$

Наявність у останньому порівнянні (-1) свідчить, що число тест пройшло і $n = 104513$ – імовірно просте число.

Задача 23. Нижче наведено декілька правильних порівнянь

1) $34733^{274656} \equiv 1 (\mathrm{mod}\, 274657)$;

2) $34734^{274656} \equiv 60108 (\mathrm{mod}\, 274657)$;

3) $53013^{274656} \equiv 1 (\mathrm{mod}\, 274657)$;

4) $87745^{274656} \equiv 1 (\mathrm{mod}\, 274657)$;

5) $34733^{69265} \equiv 71394 (\mathrm{mod}\, 277061)$;

6) $34733^{138530} \equiv 12019 (\mathrm{mod}\, 277061)$;

7) $53013^{72015} \equiv 182831 (\mathrm{mod}\, 288061)$;

8) $53013^{144030} \equiv 288060 (\mathrm{mod}\, 288061)$.

Визначте простоту числа 274657 за даними порівнянь 1) – 4), числа 277061 за даними порівнянь 5) і 6) та числа 288061 за даними порівнянь 7) і 8).

Р о з в' я з а н н я. Порівняння 1) – 4) є результатом обчислення $a^{n-1} (\mathrm{mod}\, n)$ при різних значеннях a і модулі $n = 274657$. Оскільки у другому порівнянні

$$34734^{274656} \equiv 60108 (\mathrm{mod}\, 274657) \not\equiv 1 (\mathrm{mod}\, 274657),$$

то число 274657 не проходить тест Ферма на простоту і є складеним.

Якщо $n = 277061$, то $n - 1 = 277060 = 2^2 \cdot 69265$. При тестуванні простоти чисел за допомогою тесту Міллера – Рабіна потрібно обчислити $a^{69265} (\mathrm{mod}\, n)$ і $a^{2 \cdot 69265} (\mathrm{mod}\, n) \equiv a^{138530} (\mathrm{mod}\, n)$ для випадково вибраного числа a. Тож коли $a = 34733$, ми отримаємо відповідно порівняння 5) і 6). Оскільки

$$a^{69265} \not\equiv \pm 1 (\mathrm{mod}\, 277061) \text{ і } a^{138530} \not\equiv -1 (\mathrm{mod}\, 277061),$$

робимо висновок, що 277061 – складене.

При $n = 288061$ матимемо: $n - 1 = 288060 = 2^2 \cdot 72015$. Використана в тесті Міллера – Рабіна послідовність порівнянь містить $a^{72015} (\mathrm{mod}\, n)$ і $a^{2 \cdot 72015} (\mathrm{mod}\, n) \equiv a^{144030} (\mathrm{mod}\, n)$ при випадково вибраному числі a. Очевидно, коли $a = 53013$, ці порівняння збігатимуться з порівняннями 7) і 8) із умові. А тому

$$a^{72015} \not\equiv \pm 1 (\mathrm{mod}\, n), \quad a^{144030} \equiv -1 (\mathrm{mod}\, n).$$

Результати тесту не дають зрозуміти, чи є число 288061 простим. Крім того, $53013^{288060} \equiv 1 (\mathrm{mod}\, 288061)$ і за допомогою тесту Ферма питання щодо простоти числа 288061 також прояснити не вдається.

Задача 24. Припустимо, що при факторизації числа $n = 10981$ за допомогою квадратичного решета було визначено

$$91^2 - n = -2700; \quad 98^2 - n = -1377; \quad 105^2 - n = 44;$$
$$107^2 - n = 468; \quad 115^2 - n = 2244; \quad 116^2 - n = 2475.$$

На основі цієї інформації факторизуйте число n.

Р о з в’ я з а н н я. Розкладемо на множники числа

$$-2700 = -2^2 \cdot 3^3 \cdot 5^2; \quad -1377 = -3^4 \cdot 17; \quad 44 = 2^2 \cdot 11;$$
$$468 = 2^2 \cdot 3^2 \cdot 13; \quad 2244 = 2^2 \cdot 3 \cdot 11 \cdot 17; \quad 2475 = 3^2 \cdot 5^2 \cdot 11.$$

Тоді

$$91^2 \equiv -2^2 \cdot 3^3 \cdot 5^2 \bmod 10981; \quad 98^2 \equiv -3^4 \cdot 17 \bmod 10981;$$
$$105^2 \equiv 2^2 \cdot 11 \bmod 10981; \quad 107^2 \equiv 2^2 \cdot 3^2 \cdot 13 \bmod 10981;$$
$$115^2 \equiv 2^2 \cdot 3 \cdot 11 \cdot 17 \bmod 10981; \quad 116^2 \equiv 3^2 \cdot 5^2 \cdot 11 \bmod 10981.$$

Для даної множини чисел виявимо таку підмножину, щоб перемноживши з цієї підмножини числа, отримати з обох сторін порівняння точний квадрат. Наприклад,

$$105^2 \cdot 116^2 = 2^2 \cdot 3^2 \cdot 5^2 \cdot 11^2 \bmod 10981.$$

Звідси випливає

$$x = 105 \cdot 116 = 12180; \quad y = 2 \cdot 3 \cdot 5 \cdot 11 = 330.$$

Оскільки $x \not\equiv \pm y \bmod 10981$, то факторизація можлива. $x - y \equiv 869 \bmod 10981$. Далі шукаємо НСД$(x - y, n)$ або НСД$(x + y, n)$. (це легко зробити за алгоритмом Евкліда):

$$\text{НСД}(x - y, n) = \text{НСД}(869, 10981) = 79.$$

Тепер число n можна розкласти на множники $10981 = 79 \cdot 139$.

Задача 25. Часова складність двох алгоритмів факторизації чисел визначена як $O(a \cdot n^{1000})$ і $O(b \cdot n^{100})$, де n – кількість цифр у десятковому записі числа. Який з алгоритмів швидше факторизує 100-цифрове десяткове число, якщо

а) $a = 1;\ b = 10^{1000000000000000000000000}$;

б) $a = 10^{1000000000000000000000000};\ b = 1$?

Р о з в' я з а н н я. $n = 100$.

а) $a \cdot n^{1000} = 100^{1000}$;

$$b \cdot n^{100} = 10^{1000000000000000000000000} \cdot 100^{100} =$$

$$= 100^{500000000000000000000000} \cdot 100^{100} =$$

$$= 100^{500000000000000000000002}.$$

$$a \cdot n^{1000} < b \cdot n^{1000}.$$

Отже, алгоритм з часовою складністю $O(a \cdot n^{1000})$ швидше закінчить факторизацію.

б) $a \cdot n^{1000} = 10^{1000000000000000000000000} \cdot 100^{1000} =$

$= 100^{500000000000000000000003}$.

$b \cdot n^{100} = 100^{100}$.

При таких значення констант $a \cdot n^{1000} > b \cdot n^{1000}$ і тому вигідніше проводити факторизацію алгоритмом із складністю $O(b \cdot n^{100})$.

Задача 26. Користуючись асимптотичним законом розподілу простих чисел, знайдіть приблизну імовірність, що навмання вибране 512-бітних число буде простим (мається на увазі, що старший 512-ий біт числа одиничний).

Р о з в' я з а н н я. За асимптотичним законом розподілу простих чисел кількість $\pi(n)$ простих чисел на відрізку від 1 до n зростає з ростом n як $\frac{n}{\ln n}$. Найменше 512-бітне число – 2^{511}, найбільше – $2^{512} - 1$. Тому нас цікавитиме приблизна кількість простих чисел у діапазоні від $n_1 = 2^{511}$ до $n_2 = 2^{512}$.

$$\pi(n_2) - \pi(n_1) = \frac{n_2}{\ln n_2} - \frac{n_1}{\ln n_1} = \frac{2^{512}}{\ln 2^{512}} - \frac{2^{511}}{\ln 2^{511}} =$$

$$= \frac{2^{511}}{\ln 2}\left(\frac{1}{256} - \frac{1}{511}\right) = \frac{2^{511} \cdot 255}{256 \cdot 511 \cdot \ln 2}.$$

Тоді імовірність P при випадковому пошуку у заданому діапазону вибрати просте число дорівнює

$$P = \frac{\pi(n_2) - \pi(n_1)}{n_2 - n_1} = \frac{2^{511} \cdot 255}{256 \cdot 511 \cdot \ln 2 \cdot 2^{511}} \approx \frac{1}{356}.$$

Задача 27. Нехай $q = 7541$ і $p = 2q + 1 = 15083$ – прості числа; G – група, що складається з тих елементів групи Z_p^*, порядок яких ділить q; $a = 604$ і $b = 3791$ – елементи групи G і

$$a^{7431} b^{5564} \equiv a^{1459} b^{954} \bmod p.$$

Покажіть безпосередньо, що a і b мають порядок q у групі Z_p^* і є генераторами групи G. Обчисліть дискретний логарифм $\log_{604} 3791$.

Р о з в' я з а н н я. $q = 7541$ – просте і

$$a^q = 604^{7541} \equiv 1 (\bmod p); \quad b^q = 3791^{7541} \equiv 1 (\bmod p).$$

Отже,

$$ord\ \ a = ord\ \ b = 7541 = q,$$

і оскільки група Z_p^* нараховує $p - 1 = 2q$ елементів, то $\langle a \rangle = \langle b \rangle = G$.

Із умови $604^{7431} 3791^{5564} \equiv 604^{1459} 3791^{954} \bmod p$ випливає

$$604^{7431-1459} \equiv 3791^{954-5564} \bmod p \ \Rightarrow$$

$$604^{5972} \equiv 3791^{-4610} \bmod p.$$

$-4610 \equiv 2931 \bmod 7541$, тому $604^{5972} \equiv 3791^{2931} \bmod p$. За означенням дискретного логарифма $\log_{604} 3791 = x$ і $604^x \equiv 3791 \bmod p$.

Тоді $604^{5972} \equiv (604^x)^{2931} \bmod p$ або

$$5972 \equiv 2931 x \bmod q.$$

Звідси

$$x \equiv 5972 \cdot 2931^{-1} \bmod 7541.$$

Таким чином, задача зведена до пошуку оберненого елемента

$$2931^{-1} \equiv 4680 \bmod 7541.$$

$$x \equiv 5972 \cdot 4680 \bmod 7541 \equiv 2014.$$

Задача 28. Яка ймовірність того, що навмання вибране число буде генератором мультиплікативної групи $GF^*(p)$, де $p = 25061977$? Покажіть, що число 2 не є її генератором, а число 5 є. Якщо використати групу $GF^*(p)$ з генератором 5 для побудови криптосистеми Ель-Гамаля з секретним ключем $a = 10676070$, то яким має бути відповідний

відкритий ключ? Зашифруйте за допомогою такої криптосистеми відкрите повідомлення $M = 12345678$ і покажіть, як власник секретного ключа може його розшифрувати.

Р о з в' я з а н н я. У мультиплікативні групі $GF^*(p)$ існує $\varphi(p-1)$ різних генераторів, де φ – функція Ейлера.

$$\varphi(p-1) = \varphi(25061976) = \varphi(2^3 \cdot 3^2 \cdot 348083) = 8353968.$$

Ймовірність того, що навмання вибране число є генератором групи, дорівнюватиме частці від ділення кількості генераторів на загальну кількість елементів групи, тобто

$$\frac{8353968}{25061976} = 0{,}33333237570...$$

Якщо число a не є генератором групи, то має існувати такий показник $k < p-1$, для якого $a^k \equiv 1 \bmod p$. Дійсно,

$$2^{(p-1)/2} \equiv 2^{12530988} \equiv 1 \bmod 25061977.$$

Фактично, елемент 2 має порядок $(p-1)/2$.

Якщо $p-1 = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ – канонічний розклад числа $p-1$, то число g буде генератором групи $GF^*(p)$ лише за умови, що

$$g^{\frac{p-1}{p_1}} \not\equiv 1(\bmod p),\ g^{\frac{p-1}{p_2}} \not\equiv 1(\bmod p),...,\ g^{\frac{p-1}{p_k}} \not\equiv 1(\bmod p).$$

Для числа $g = 5$ перевірка дає $25061977 - 1 = 2^3 \cdot 3^2 \cdot 348083$;

$$5^{\frac{p-1}{2}} \equiv -1(\bmod p);\ 5^{\frac{p-1}{3}} \equiv 1859846(\bmod p);$$

$$5^{\frac{p-1}{348083}} \equiv 12764146(\bmod p).$$

Отже, число 5 – генератор групи $GF^*(p)$.

Перейдемо до генерування відкритого ключа h, що відповідатиме секретному ключу $a = 10676070$:

$$h = g^a (\bmod p) = 5^{10676070} (\bmod 25061977) = 23140629.$$

Із відрізка $[1, p-1]$ виберемо рандомізатор $r = 129$ і зашифруємо текст $M = 12345678$:

$$C_1 = g^r \pmod p \equiv 5^{129} \pmod{25061977} \equiv 12830244;$$

$$C_2 = M \cdot h^r \pmod p \equiv$$

$$= 12345678 \cdot 23140629^{129} \pmod{25061977} \equiv 9969600.$$

Шифротекст – це $(C_1, C_2) = (12830244, 9969600)$.

За допомогою секретного ключа розшифруємо

$$C_2 \cdot (C_1^a)^{-1} \bmod p = 9969600 \cdot (12830244^{10676070})^{-1} \bmod 25061977 \equiv$$

$$\equiv 12345678 = M.$$

Задача 23. Для протоколу Діффі – Хеллмана відкритого розподілу ключів вибрано групу Z_{19}^* та генератор $g = 2$. Припустимо, після першого кроку протоколу Ви перехопили з мережі два значення: від першого абонента $g^a = 11 (\mathrm{mod} 19)$, а від другого абонента $g^b = 13 (\mathrm{mod} 19)$. Знайдіть за цими даними секретний спільний ключ, який буде створено наприкінці алгоритму.

Р о з в я' з а н н я. Обчислюємо степені генератора за $\mathrm{mod} 19$:

$$2^2 \equiv 4;\ 2^3 \equiv 8;\ 2^4 \equiv 16;\ \underline{2^5 \equiv 32 \equiv 13};\ 2^6 \equiv 64 \equiv 7;\ 2^7 \equiv 14;\ 2^8 \equiv 28 \equiv 9;$$

$$2^9 \equiv 18 \equiv -1;\ 2^{10} \equiv -2 \equiv 17;\ 2^{11} \equiv -4 \equiv 15;\ \underline{2^{12} \equiv -8 \equiv 11.}$$

Якщо $2^a = 11 (\mathrm{mod} 19)$, то $a = 12$, а якщо $2^b = 13 (\mathrm{mod} 19)$, то $2^b = 13 (\mathrm{mod} 19)$, то $b = 5$. Спільний ключ – це

$$(2^a)^b = (2^{12})^5 \bmod 19 \equiv 11^5 \bmod 19 \equiv 7 \bmod 19.$$

Задача 24. Доведіть, що побудована на основі методу повного перебору атака на алгоритм Діффі – Хеллмана розподілу ключів має експоненціальну часову складність.

Р о з в' я з а н н я. Нехай для протоколу Діффі – Хеллмана вибрано k-бітове просте число p, (тобто $2^k \le p \le 2^{k+1}$) і g – примітивний корінь за модулем p. Учасники протоколу можуть вибирати для своїх секретних ключів будь-яке ціле число з інтервалу $(1, p-1)$. Отже, при повному переборі ключів криптоаналітик має перевірити усі числа з

цього інтервалу. Оскільки p містить k бітів, то потенційно існуватиме 2^k двійкових чисел, що підлягають перевірці. Тому проблема, як мінімум, має складність $O(2^k)$, тобто є експоненційною. Якщо ж врахувати перевірку двійкових чисел, довжина яких менша за k бітів, то складність атаки становитиме $O(2^1 + 2^2 + ... + 2^{k-1} + 2^k)$. Очевидно, що $2^i < 2^k$ при $i < k$, тому

$$O(2^1 + 2^2 + ... + 2^{k-1} + 2^k) = O(2^k + 2^k + ... + 2^k + 2^k) = O(k2^k).$$

Це не зменшує складності атаки і вона залишається експоненційною.

Задача 25. Покажіть, чому для криптосистем, основаних на складності задачі дискретного логарифмування, небезпечний вибір у якості модуля криптосистеми простих чисел вигляду $p = 2^k + 1$, $k \in N$. Вважайте, що g – генератор групи Z_p^*.

Р о з в' я з а н н я. При невідомому x у порівнянні $y = g^x \bmod p$ ми знаємо, що y є квадратичним лишком тоді і тільки тоді, коли x – парне. Крім того, за критерієм Ейлера y – квадратичний лишок тільки за умови, що $y^{(p-1)/2} \equiv 1 \bmod p$. Тому коли ця умова виконується, то x – парне і найменший значущий біт цього числа нульовий. Якщо ж $y^{(p-1)/2} \not\equiv 1 \bmod p$, то x – непарне число і, очевидно, тоді найменший значущий біт дорівнює одиниці.

У свою чергу, при парному x число $g^{x/2}$ – квадратичний лишок, якщо $x/2$ – парне. При цьому за критерієм Ейлера

$$\left(g^{x/2}\right)^{(p-1)/2} = y^{(p-1)/4} \equiv 1 \bmod p,$$

що знову дає змогу визначити другий значущий біт числа x.

У загальному випадку якщо $b_n, b_{n-1}, ..., b_1$ – біти показника x, то їх можна знайти, виконуючи такі дії:

1⁰. Покласти $i = 1$;

2⁰. Поки $y \neq 1$

2.1. Якщо $y^{(p-1)/2^i} \equiv 1 \bmod p$, то $b_i = 0$, інакше $b_i = 1$;

2.2. $y = y \Big/ g^{b_i 2^{i-1}}$;

2.3. $i = i + 1$.

Задача 26. За алгоритмом Шенкса («крок немовляти – крок велетня») розв'яжіть задачу дискретного логарифмування $821^x \equiv 288 \bmod 2009$, врахувавши, що порядок елемента $a = 821$ у мультиплікативній групі Z^*_{2005} дорівнює 21 і елемент $b = 288$ належіть до циклічної підгрупи $\langle a \rangle$ групи Z^*_{2009}.

Р о з в' я з а н н я. Циклічна підгрупа мультиплікативної групи Z^*_{2005} генерується елементом $a = 821$, порядок якого $n = 21$, тому за алгоритмом Шенкса спочатку визначимо найменше ціле число m, для якого $m^2 \geq n$:

$$n = 21 < 25 = 5^2 = m^2 \quad \Rightarrow \quad m = 5.$$

Далі для $j = 0,...,m-1$ знайдемо значення $a^{j \cdot m}$ і з пар $(j,\ a^{j \cdot m})$ сформуємо перший список, а для $i = 0,...,m-1$ визначимо значення $a^{-i} \cdot b$ і з пар $(i, a^{-i} \cdot b)$ створимо другий список. Для цих розрахунків зручно виконати попередні обчислення: $821^5 \bmod 2009 = 1313$ і $821^{-1} \bmod 2009 = 739$.

j	$(a^m)^j = (821^5)^j$
1	1313
2	247
3	862
4	739

i	$(a^{-1})^i \cdot b = (821^{-1})^i \cdot 288$
1	$739 \cdot 288 = 1887$
2	$739^2 \cdot 288 = 247$
3	…
4	…

При $j = 2$, $i = 2$ обчислені значення збігаються, тому

$$\log_a b = (m \cdot j + i) \bmod n = (5 \cdot 2 + 2) \bmod 2009 = 12.$$

Задача 27. Яке з наступних простих чисел p_1 чи p_2 Ви рекомендували б в якості параметра для криптосистеми Ель-Гамаля, якщо

$p_1 = 2 \cdot m \cdot n^2 + 1$, де m і n – числа довжиною 1024 біти;

$p_2 = 2 \cdot k \cdot l + 1$, де k і l – числа довжиною 100 і 1000 бітів відповідно.

Р о з в’ я з а н н я. Довжина чисел p_1 і p_2 – приблизно 3073 и 1101 бітів відповідно. Через алгоритм Сільвера – Поліга – Хеллмана виникає загроза ефективного проведення дискретного логарифмування: тому у криптосистеми Ель-Гамаля, побудованій у мультиплікативній групі $GF^*(p_1)$, рівень безпеки падає до рівня криптосистеми, побудованої за допомогою сильно простого числа довжиною усього 1025 бітів. Аналогічні міркування щодо групи $GF^*(p_2)$ дають рівень безпеки, еквівалентний рівню, що матиме шифр з сильно простим числом у 1001 біт. Проте слід відзначити суттєве збільшення часу виконання арифметичних модульних операцій у групі $GF^*(p_1)$ порівняно з групою $GF^*(p_2)$, оскільки довжини модулів p_1 і p_2 відрізняються за довжиною майже втричі. Отже, при компромісі «безпека шифрування – ефективність обчислень» слід вибрати криптосистему у групі $GF^*(p_2)$.

Задача 28. Яким є протокол відкритого розподілу ключів між трьома користувачами A, B і C, аналогічний протоколу Діффі – Хеллмана?

Р о з в’ я з а н н я. Вибираємо спільні для всіх користувачів циклічну групу G, порядок якої є просте число, та примітивний елемент g.

1. Користувач **A** вибирає випадкове число x, обчислює g^x та відсилає його користувачу **B**.

2. Користувач **B** вибирає випадкове число y, обчислює g^y та відсилає його користувачу **C**.

3. Користувач **C** вибирає випадкове число z, обчислює g^z та відсилає його користувачу **A**.

4. Користувач **A** обчислює g^{xz} та відсилає його **B**.

5. Користувач **B** обчислює g^{xy} та відсилає його **C**.

6. Користувач **C** обчислює g^{yz} та відсилає його **A**.

7. Користувач **A** обчислює спільний ключ g^{yzx}.

8. Користувач **B** обчислює спільний ключ g^{zxy}.

9. Користувач **C** обчислює спільний ключ g^{xyz}.

Задача 29. Нехай p – велике просте число. Абонент **A** хоче надіслати абоненту **B** шифроване повідомлення M $(1 \le M \le p-1)$.

Для цього **A** і **B** таємно вибирають відповідно по одному цілому числу a і b, що є взаємно простими з числом $p-1$. Абонент **A** обчислює $c \equiv M^a \pmod p$ і надсилає це значення абоненту **B**. Той обчислює $d \equiv c^b \pmod p$ і повертає значення d абонентові **A**. Оскільки той знає число a, він знаходить a_1 з умови $a a_1 \equiv 1 \pmod{p-1}$, обчислює $e = d^{a_1} \pmod p$ та повертає число e абоненту **B**. Як абонент **B** може тепер знайти M? Доведіть, чому таке зашифрування коректне.

Р о з в' я з а н н я. Абонент **B** повинен знайти b_1 з умови $bb_1 \equiv 1 \pmod{p-1}$ та обчислити $e^{b_1} \pmod p \equiv M \pmod p$. Доведемо коректність шифрування

$$e \equiv d^{a_1} \pmod p \equiv (c^b)^{a_1} \pmod p \equiv ((m^a)^b)^{a_1} \pmod p \equiv M^b \pmod p \Rightarrow$$

$$\Rightarrow e^{b_1} \equiv M^{b_1 b} \pmod p \equiv M .$$

Задача 30. У деякому алгоритмі шифрування відкритий ключ утворюється за процедурою:

1) вибирають прості числа p, q і $g \in Z_p^*$, де g – генератор підгрупи G_q;

2) вибирають випадкові числа x і y із множини $\{0,1,...,q-1\}$;

3) обчислюють значення $h_1 = g^x \bmod p$ і $h_2 = g^y \bmod p$;

4) відкритий ключ – (G_q, p, g, h_1, h_2), секретний ключ – (x, y).

Для зашифрування повідомлення M виконують такі операції:

1) перевіряють умову $M \in G_q$;

2) вибірають випадкове число $z \in \{0,1,...,q-1\}$ та обчислюють $C_1 = g^z \bmod p$ і $C_2 = M \cdot h_1^{-z} h_2^z \bmod p$;

3) шифрований текст – пара $C = (C_1; C_2)$.

Розробіть відповідний алгоритм розшифрування для наведеної криптосистеми та продемонструйте коректність її роботи.

Р о з в' я з а н н я. Відновити відкритий текст власник секретного ключа може згідно з рівнянням $M = C_1^{x-y} C_2 \bmod p$. Коректність такого розшифрування підтверджують такі розрахунки:

$$C_1^{x-y}C_2 \bmod p = C_1^{x}C_1^{-y}C_2 \bmod p = (g^z)^{-y}(g^z)^x(M\cdot h_1^{-z}h_2^{z}) \bmod p =$$
$$= g^{-zy}g^{zx}\cdot(M\cdot(g^x)^{-z}(g^y)^z) \bmod p = g^{-zy}g^{zx}\cdot M\cdot g^{xz}g^{yz} \bmod p = M\,.$$

Задача 31. За умовою попередньої задачі розшифруйте шифротекст $C=(3;4)$, якщо параметри шифру $p=23;\ q=11;$ $G_{11}=\langle 6\rangle;\ x=9;\ y=8;\ z=7$.

Р о з в' я з а н н я. Підгрупа $\langle 6\rangle=\{3,9,4,12,13,16,2,6,18,8,1\}$.

$$M = C_1^{x-y}C_2 \bmod p = 3^{9-8}\cdot 4 \bmod 23 \equiv 12 \in \langle 6\rangle.$$

Задача 32. PIN-код зарплатної банківської картки у зашифрованому вигляді було двічі надіслано від абонента **A** до абонента **B**. Для зашифрування використано шифр Ель-Гамаля, $(7,30)$ і $(49,139)$ – надіслані шифротексти. Розкрийте PIN-код за умови, що перша частина відкритого ключа $p=10007$.

Р о з в' я з а н н я. Нехай $(p=10007,\ g,\ h)$ – відкритий ключ криптосистеми, r_1, r_2 – рандомізатори, задіяні для зашифрування у перший та другий рази. У криптосистемі Ель-Гамаля шифротекст (C_1,C_2) повідомлення M утворюється згідно з рівняннями:

$$C_1 = g^r \bmod p;\ C_2 = M\cdot h^r \bmod p\,.$$

Тому за умовою задачі

$$(C_1',C_2') = (g^{r_1} \bmod p,\ M\cdot h^{r_1} \bmod p) = (7,30);$$

$$(C_1'',C_2'') = (g^{r_2} \bmod p,\ M\cdot h^{r_2} \bmod p) = (49,139).$$

Оскільки $7^2=49$, то $r_2=2r_1$. Отже,

$$C_2''\cdot(C_2')^{-1} = M\cdot h^{r_2}(M\cdot h^{r_1})^{-1} \bmod p =$$
$$= h^{2r_1}\cdot h^{-r_1} \bmod p = h^{r_1} \bmod p = 139\cdot 30^{-1} \bmod 10007\,.$$

Із виразу $C_2' = M\cdot h^{r_1} \bmod p$ дістаємо

$$M = C_2'\cdot h^{-r_1} \bmod p = 30\cdot(139\cdot 30^{-1})^{-1} \bmod 10007 =$$

$$= 30 \cdot 30 \cdot 139^{-1} \bmod 10007 \equiv 900 \cdot 72 \bmod 10007 \equiv 4758.$$

Задача 33. Уявіть, що менеджер страхової компанії надіслав шефу нешифрований запит, чи купувати йому акції. За домовленістю шеф у відповідь може надіслати одне з двох повідомлень «ТАК» або «НІ», а для збереження таємниці відповіді вони шифрують своє листування за допомогою криптосистеми Ель-Гамаля у групі $GF(23801)$. Відомо, що відповіді перед зашифруванням кодуються: «ТАК» $=18915$, «НІ» $=4886$ або навпаки. Припустимо, що шеф надіслав менеджеру шифротекст $(4457,1979)$. Як криптоаналітик, не обчислюючи дискретних логарифмів, може змінити шифротекст на альтернативний (щоб при розшифруванні менеджер отримав замість «ТАК» відповідь «НІ» і навпаки)?

Р о з в' я з а н н я. У криптосистемі Ель-Гамаля відкритому тексту M відповідає шифротекст $(g^r \bmod p,\ M \cdot g^{ar} \bmod p)$, де g – примітивний корінь за модулем p, a – секретний ключ абонента, r – рандомізатор. Перехопивши шифрований текст, його можна модифікувати двома шляхами: або помножити на додатковий множник тільки його другу частину $(g^r \bmod p,\ \lambda M \cdot g^{ar} \bmod p)$, або піднести обидві його частини до деякого степеня. Наприклад, розшифрування шифротексту $(g^{r\mu} \bmod p,\ M^{\mu} \cdot g^{ar\mu} \bmod p)$ дає відкритий текст M^{μ}.

Отже, у першому випадку криптоаналітик має відшукати число λ з умовами: $\lambda \cdot 4886 \equiv 18915 \bmod 23801$ і $\lambda \cdot 18915 \equiv 4886 \bmod 23801$. Перемножимо почленно ці порівняння: $\lambda^2 \equiv 1 \bmod 23801$, звідки $\lambda \equiv \pm 1 \bmod 23801$. Оскільки для вибраних кодів відповідей виконується рівність $18915 + 4886 = 23801 = p$, то криптоаналітик може підмінити шифротекст на $(4457, -1979 \bmod 23801)$ або $(4457,\ 21822 \bmod 23801)$.

У другому випадку криптоаналітику потрібно підібрати таке число μ, для якого $4886^{\mu} \equiv 18915 \bmod 23801$ і $18915^{\mu} \equiv 4886 \bmod 23801$. Злогарифмувавши порівняння, дістанемо

$$\mu \cdot \log 4886 \equiv \log 18915 \bmod 23800;$$

$$\mu \cdot \log 18915 \equiv \log 4886 \bmod 23800,$$

звідки $\mu^2 \equiv 1 \bmod 23800$, $\mu \equiv \pm 1 \bmod 23800$. Перевірка нетривіального значення дає $4886^{-1} \not\equiv 18915 \bmod 23801$, тому другий підхід з вибраним кодуванням реалізувати неможливо.

Задача 34. Для криптосистеми Ель-Гамаля вибрано поле $GF(2^4)$ з многочленом x^4+x+1 та примітивний елемент $g=0010=x$. Секретний ключ $a=7$. Завершіть формування ключів та розшифруйте шифротекст $(C_1, C_2)=(0100, 1110)$.

Р о з в' я з а н н я. Для формування відкритого ключа визначимо:

$$h=g^a=x^7=x^3x^4=x^3(x+1)=x^4+x^3=x^3+x+1=1011$$

(усі розрахунки у полі $GF(2)$). Отже, відкритий ключ криптосистеми – трійка $(GF(2^4), 0010, 1011)$.

Переходимо до розшифрування даного шифротексту.

У криптосистемі Ель-Гамаля згідно з рівнянням розшифрування

$$M=C_2\cdot(C_1^a)^{-1},\ \text{де}\ C_1=0100=x^2;\quad C_2=1110=x^3+x^2+x.$$

$$C_1^a=(x^2)^7=(x^7)^2=(x^3+x+1)^2=x^6+x^2+1=$$

$$=x^4\cdot x^2+x^2+1=(x+1)\cdot x^2+x^2+1=x^3+1.$$

$$(C_1^a)^{-1}=(x^3+1)^{-1}.$$

Оскільки у даному полі $x^4+x\equiv 1 \bmod x^4+x+1$, то

$$x(x^3+1)\equiv 1 \bmod x^4+x+1 \Rightarrow\ (x^3+1)^{-1}\equiv x \bmod x^4+x+1.$$

Отже, $(C_1^a)^{-1}=(x^3+1)^{-1}=x$ і

$$M=C_2\cdot(C_1^a)^{-1}=(x^3+x^2+x)x=x^4+x^3+x^2=$$

$$=(x+1)+x^3+x^2 \bmod x^4+x+1=1111.$$

Задача 35. Еліптична крива $y^2=x^3+x+27$ визначена над простим полем $GF(p)$, де $p=2^{127}-1$. Доведіть безпосередньо, що точка $Q=(p-1,\ 5)$ належіть кривій.

Р о з в' я з а н н я. При $x=p-1=2^{127}-2,\ y=5$ отримаємо

$$25\equiv(2^{127}-2)^3+(2^{127}-2)+27(\bmod 2^{127}-1)\equiv$$

$$\equiv((2^{127}-1)-1)^3+(2^{127}-1)-1+27(\bmod 2^{127}-1)\equiv$$

$$\equiv(2^{127}-1)^3-3(2^{127}-1)^2+3(2^{127}-1)-1+26(\bmod 2^{127}-1)\equiv 25\ \Rightarrow$$

точка $Q=(p-1,\ 5)$ належіть кривій $y^2=x^3+x+27(\mathrm{mod}\,2^{127}-1)$.

Задача 36. Покажіть, що еліптична крива $y^2=x^3-x$ над полем $GF(p)$ має $p+1$ точку, коли $p>3$ – просте і $p\equiv 3(\mathrm{mod}\,4)$.

Р о з в' я з а н н я. У полі $GF(p)$ за властивостями символу Лежандра

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=-1.$$

$$\left(\frac{(-x)^3-(-x)}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{x^3-x}{p}\right)=-\left(\frac{x^3-x}{p}\right).$$

За простим модулем добуток двох квадратичних лишків є квадратичним лишком. Тому залежно від того, чи є вираз x^3-x квадратичним лишком чи квадратичним нелишком, кожна пара $\{x,-x\}$, де $x\neq 0$, дає дві точки:

$$(x,\,(x^3-x)^{1/2}),\quad (x,\,-(x^3-x)^{1/2})$$

або

$$(x,\,(-x^3-x)^{1/2}),\quad (x,\,-(-x^3-x)^{1/2}).$$

Оскільки $\left(\frac{0}{p}\right)=0$, то $\sum\limits_{x\in GF(p)}\left(\frac{x^3-x}{p}\right)=0$. Таким чином, кількість $|E|$ точок на кривій складає

$$|E|=1+\sum_{x\in GF(p)}\left(1+\left(\frac{x^3-x}{p}\right)\right)=1+p+\sum_{x\in GF(p)}\left(\frac{x^3-x}{p}\right)=1+p$$

(враховано нескінченно віддалену точку O і те, що рівняння $x^3-x=0(\mathrm{mod}\,p)$ має тільки один розв'язок).

Задача 37. Покажіть, що еліптична крива $y^2=x^3-1$ над полем $GF(p)$ має $p+1$ точку, коли $p>3$ – просте, і $p\equiv 2(\mathrm{mod}\,3)$.

Р о з в’ я з а н н я. У полі $GF(p)$ кубічний корінь завжди існує та однозначно визначений. Отже, для кожного значення y на кривій існуватиме лише одна точка $((y^2+1)^{1/3}, y)$. Оскільки просте поле $GF(p)$ нараховує p елементів, то, беручи до уваги нескінченно віддалену точку O, усього матимемо $p+1$ точку на кривій.

Задача 38. Відомо, що на еліптичній кривій $y^2 = x^3 + 59x + 23$ над полем $GF(347)$ існує точка $M = (345, 217)$, для якої $113M = O$. Яким є порядок групи точок цієї кривої? Доведіть, що точка $Q = (38, 24)$ – генератор групи.

Р о з в’ я з а н н я. За умовою $113M = O$, тому порядок точки має ділити число 113. Це число просте, отже порядок точки $M(345, 217)$ має дорівнювати 113. Тоді за теоремою Лагранжа порядок N_E групи точок еліптичної кривої обов’язково кратний 113. Також за теоремою Хассе $p+1-2\sqrt{p} \le N_E \le p+1+2\sqrt{p}$. У нашому випадку $310 \le N_E \le 385$ і єдине число з відрізку $[310; 385]$, яке ділитиметься на 113, – це 339. Таким чином, порядок групи точок $N_E = 339$.

$N_E = 339 = 3 \cdot 113$. Отже, аби довести, що точка $Q = (38, 24)$ – генератор групи, достатньо показати, що порядок точки Q не є ані 3, ані 113. Дійсно, $3Q = (345, 217) \ne O$, $113Q = (67, 272) \ne O \Rightarrow$ точка Q – генератор групи.

Задача 39. Нехай $m_0 > 0$ – найменший розв’язок рівняння $Q = mP$, що зв’язує дві точки P і Q еліптичної кривої E над полем $GF(p)$. Доведіть, що при деякому цілому j будь-який інший розв’язок цього рівняння матиме вигляд $m = m_0 + jk$, де k – порядок точки P.

Р о з в’ я з а н н я. Покладемо $m = jk + l$, де l – ціле з проміжку $[0; k)$. Оскільки $kP = O$ (за визначенням порядку точки), то

$$Q = mP = (jk + l)P = j(kP) + lP = jO + lP = lP.$$

За умовою $m_0 P$ є найменшим скалярним добутком точки P, який дорівнює Q, тому $l \ge m_0$. Припустимо, що $l > m_0$. Тоді

$$O = Q - Q = lP - m_0 P = (l - m_0)P,$$

Як порядок точки, k – найменше з можливих ненульових цілих

чисел, для якого $kP = O$, а відтак, $l - m_0 \geq k$, що суперечить припущенню $l > m_0$. Таким чином, $l = m_0$ і $m = m_0 + jk$.

Задача 40. Покажіть, що для відновлення точки $P(x_0, y_0)$ еліптичної кривої $E_p(a,b)$ абоненту достатньо передати тільки абсцису x_0 точки та один біт l, що визначається умовою

$$l = \begin{cases} 0, & 0 \leq y < p/2; \\ 1, & p/2 < y < p. \end{cases}$$

Якщо вибрати криву $E_{1123}(54,87)$, то яка точка кривої буде відновлена абонентом у разі отримання ним даних: а) $x_0 = 14;\ l = 0;$ б) $x_0 = 14;\ l = 1$?

Р о з в' я з а н н я. Якщо β – квадратичний лишок за модулем p, то порівняння $\alpha^2 \equiv \beta \bmod p$ має два корені $\alpha \bmod p$ та $-\alpha \equiv p - \alpha \bmod p$. Отримавши абсцису x_0 точки $P(x_0, y_0)$ еліптичної кривої $y^2 = x^3 + ax + b \bmod p$, абонент обчислить ${y_0}^2 = {x_0}^3 + ax_0 + b \bmod p$. З цього числа можна добути два корені y_0 та $-y_0 \equiv p - y_0 \bmod p$, один з яких лежатиме в проміжку від 0 до $p/2$, а інший в інтервалі від $p/2$ до p. Вибрати одну з цих точок можна, додатково вказавши значення біта l.

У разі отримання абсциси $x_0 = 14$ обчислимо

$${y_0}^2 \equiv 14^3 + 54 \cdot 14 + 87 \bmod 1123 \equiv 218 \bmod 1123.$$

При простому модулі вигляду $p = 4k + 3$, де k – ціле, корені порівняння $\alpha^2 \equiv \beta \bmod p$ визначаються за формулою $\alpha \equiv \pm\beta^{k+1} \bmod p$. За умовою

$$p = 1123 = 280 \cdot 4 + 3 \Rightarrow\ k = 280. \Rightarrow$$

$$y_0 \equiv \pm 218^{281} \bmod 1123 \equiv \pm 619 \bmod 1123.$$

Це дає дві точки на кривій – $(14, 619)$ і $(14, 504)$, бо $-619 \equiv 504 \bmod 1123$. $p/2 = 561{,}5$. Тому:

а) якщо $l = 0$, то передано точку $(14, 504)$;

б) якщо $l = 1$, то передано точку $(14, 619)$.

Задача 41. Нехай M – тризначне ціле число вигляду $21m$, де останній знак $m \in \{0,1,2,...,9\}$ – невідомий. Знайдіть таке значення m, при якому абсциса точка (x, y) еліптичної кривої $y^2 \equiv x^3 + 7x + 15 \bmod 593$ дорівнюватиме числу M.

Р о з в' я з а н н я. Спочатку обчислимо значення виразу $x^3 + 7x + 15 \bmod 593$ при всіх значеннях x з множини

$$\{210 + 0,\ 210 + 1,...,\ 210 + 9\}.$$

x	210	211	212	213	214	215	216	217	218	219
$x^3 + 7x + 15 \bmod 593$	418	524	117	389	160	29	2	85	284	12.

Очевидно, точка (x, y), де $y \in GF(593)$, належатиме еліптичній кривій тоді і тільки тоді, коли $x^3 + 7x + 15$ матиме квадратні корені за модулем 593. У цьому разі символ Лежандра $\left(\frac{x^3 + 7x + 15}{593}\right)$ дорівнюватиме $+1$. Отже, залишається визначити десять значень символу Лежанжра:

x	210	211	212	213	214	215	216	217	218	219
$\left(\frac{x^3 + 7x + 15}{593}\right)$	-1	-1	-1	-1	-1	1	1	-1	1	-1

Таким чином, точки з абсцисами $215, 216$ і 218 належать даній кривій і $m \in \{5, 6, 8\}$.

Задача 42. Точка $A(10,2)$ є генератором групи E точок еліптичної кривої $y^2 = x^3 + 2x + 19$ над полем $GF(23)$:

i	1	2	3	4	5	6	7	8	9	10	11
iP	(10,2)	(5,19)	(3,11)	(14,13)	(8,15)	(7,13)	(22,19)	(20,3)	(19,4)	(2,10)	(12,0)
i	12	13	14	15	16	17	18	19	20	21	22
iP	(2,13)	(19,19)	(20,20)	(22,4)	(7,10)	(8,8)	(14,10)	(3,12)	(5,4)	(10,21)	O

Для криптосистеми Ель-Гамаля вибрано у групі E циклічну підгрупу $G = \langle P \rangle$, де $P = (20,20) = 14A$. Яким буде відкритий ключ користувача, якщо його секретний ключ $a = 4$? Використавши

рандомізатор $k=5$ та визначений секретний ключ, знайдіть шифротекст для відкритого тексту, закодованого за допомогою точки $M=(2,10)$.

Р о з в' я з а н н я. Відкритий ключ користувача – це точка

$$Q=aP=4(14A)=56A=(2\cdot 22+12)A=O+12A=12A=(2,13).$$

Відкритий текст $M=(2,10)=10A$.

Шифротекст, відповідний точці M, складається з пари точок $(kP;\ R)$, де $k=5$ – рандомізатор, $R=M+kQ$.

$$kP=5P=5\cdot 14A=70A=4A=(14,13);$$

$$R=M+kQ=10A+5\cdot 12A=70A=4A=(14,13).$$

Шифротекст – $((14,13);\ (14,13))$.

Задача 43. Два абоненти **A** і **B** обмінюються ключами за схемою Діффі – Хеллмана, вибравши групу точок еліптичної кривої $y^2=x^3+x+6$ над полем $GF(11)$ і базову точку $P=(2,7)$, порядок якої дорівнює 13. Визначте спільний секретний ключ користувачів за умови, що перший абонент вибрав секретний параметр $n_A=2$, а другий – секретний параметр $n_B=13^{100}+1$.

Р о з в' я з а н н я. Оскільки порядок базової точки P дорівнює 13, то $13P=O$. Спільний ключ абонентів обчислимо як

$$n_A\cdot n_B(2,7)=2\cdot(13^{100}+1)(2,7)=2\cdot(13^{100}(2,7)+(2,7))=$$
$$=2\cdot(O+(2,7))=2\cdot(2,7).$$

За формулами для подвоєння точки еліптичної кривої дістанемо

$$\lambda=\frac{3x_1{}^2+a}{2y_1}=\frac{3\cdot 4+1}{2\cdot 7}=13\cdot 14^{-1}\equiv 2\cdot 3^{-1}=2\cdot 4\equiv 8(\mathrm{mod}11);$$

$$x=\lambda^2-2x_1=64-2\cdot 2\equiv 5(\mathrm{mod}11);$$

$$y=\lambda(x_1-x)-y_1=8(2-5)-7\equiv -31(\mathrm{mod}11)\equiv 2;$$

$2(2,7)=(5,2)$. Ця точка й буде спільним ключем абонентів.

Задача 44. Криптосистема Ель-Гамаля побудована на еліптичній кривій $y^2=x^3+77x+28$ над полем $GF(157)$, базова точка $P(9,115)$. Відкритий ключ користувача – точка $Q=(89,144)$. Зашифруйте текст, якому відповідає точка $M=(20,73)$, вибравши рандомізатор $k=3$.

Р о з в' я з а н н я. $kP=3P=3(9,115)=(22,81)$,

$$R = M + kQ = (20,73) + 3 \cdot (89,144) = (140,137).$$

Шифротекст – пара точок $(kP,\ R) = ((22,81),\ (140,137))$.

Задача 45. Криптосистема Ель-Гамаля побудована на еліптичній кривій $y^2 = x^3 + 77x + 28$ над полем $GF(157)$, базова точка $P(9,115)$. Перед шифруванням букви відкритого тексту кодуються точками еліптичної кривої $y^2 = x^3 + 77x + 28$ над полем $GF(157)$:

А	(2, 87)	І	(20,73)	Т	(35, 15)
Б	(17, 21)	Ї	(42,109)	У	(78, 154)
В	(36, 156)	Й	(68, 94)	Ф	(96, 32)
Г	(66, 127)	К	(82, 108)	Х	(74, 9)
Ґ	(81,83)	Л	(1, 48)	Ц	(51, 4)
Д	(1, 109)	М	(44, 44)	Ч	(28, 30)
Е	(17, 136)	Н	(83, 17)	Ш	(78, 3)
Є	(42,48)	О	(8, 34)	Щ	(44,113)
Ж	(2, 70)	П	(9, 42)	Ь	(49, 106)
З	(82, 49)	Р	(4, 20)	Ю	(99, 25)
И	(68, 63)	С	(29, 66)	Я	(53, 15)

Розшифруйте шифротекст

$$((27,81),\ (26,74)),\ ((68,63),\ (126,52)),\ ((108,76),\ (88,50)),$$

отриманий за допомогою криптосистеми Ель-Гамаля на вказаній еліптичній кривій, базова точка $P(9,115)$, відкритий ключ користувача – точка $Q = (89,144)$, його секретний ключ $a = 7$.

Р о з в’ я з а н н я. За допомогою секретного ключа користувача послідовно розшифровуємо

$$M_1 = R_1 - a k_1 \cdot P = (26,74) - 7 \cdot (27,81) = (4,20) = \text{«Р»};$$

$$M_2 = R_2 - a k_2 \cdot P = (126,52) - 7 \cdot (68,63) = (2,70) = \text{«Ж»};$$

$$M_3 = R_3 - a k_3 \cdot P = (88,50) - 7 \cdot (108,76) = (2,87) = \text{«А»}.$$

Отже, зашифровано слово РЖА.

Задача 46. Генератор групи точок еліптичної кривої $y^2 = x^3 + 2x + 1$ над полем $GF(41)$– точка $P = (0,\ 1)$. За допомогою алгоритму «крок немовляти – крок велетня» розв’яжіть задачу дискретного логарифмування $Q = kP$, де $Q = (23,\ 18)$.

Р о з в’ я з а н н я. Наша задача – визначити множник k у рівнянні $Q = kP$. За алгоритмом «крок немовляти – крок велетня» потрібно

1. Визначити $m = \left\lceil \sqrt{q+1+2\sqrt{q}} \right\rceil$ (округлення у бік більшого, q – кількість елементів поля);

2. Побудувати дві послідовності точок:

- iP, де $i = 1,...,m-1$;
- $Q - jmP$, де $j = 0,1,...,m-1$;

3. знайти такі значення i і j, при яких точка з першою послідовності збігатиметься з точкою другої послідовності;

4. $k = i + jm \bmod n$, де n – порядок підгрупи, генерованої точкою P.

У нашому випадку

$$m = \left\lceil \sqrt{q+1+2\sqrt{q}} \right\rceil = \left\lceil \sqrt{41+1+2\sqrt{41}} \right\rceil = \lceil 7,40 \rceil = 8.$$

Відповідні значення скалярного множення векторів записуємо у таблиці:

i	1	2	3	4	5	6	7
iP	(0,1)	**(1,39)**	(8,23)	(38,38)	(23,23)	(20,28)	(26,9)

j	0	1	2	3	4	5	6	7
$Q-8jP$	(23,18)	(13,16)	(28,19)	(40,11)	**(1,39)**			

Подальші обчислення припиняємо, бо при $i = 2$, $j = 4$ виявляється збіг точок: $2P = Q - 8 \cdot 4 \cdot P$. Таким чином,

$$k = i + jm \bmod n = 2 + 4 \cdot 8 = 34.$$

Дійсно, за перевіркою $34(0, 1) = (23, 18)$.

Задача 47. Найкращий алгоритм для розв’язання задачі дискретного логарифмування у групі точок еліптичної кривої над полем $GF(p)$ має часову складність $O(\sqrt{p})$, а часова складність найкращого метода решета числового поля для розв’язання цієї задачі у мультиплікативній групі точок простого поля $GF^*(p)$ складає

$$e^{1,92(\ln p)^{1/3}(\ln \ln p)^{2/3}}.$$

Визначте порядки полів, в яких час розв’язання задачі дискретного логарифмування обома алгоритмами однаковий і дорівнює 2^{56}, 2^{80}, 2^{112}, 2^{128}, 2^{192}, 2^{256} ? Порядки полів укажіть у вигляді 2^n.

Р о з в’ я з а н н я. Порядком скінченного поля називають кількість його елементів. Якщо час розв’язання задачі дорівнює 2^{56}, то при дискретному логарифмуванні:

1) у групі точок еліптичної кривої над полем $GF(p)$

$$\sqrt{p} \approx 2^{56} \Rightarrow \ p \approx 2^{112};$$

2) у мультиплікативній групі точок простого поля $GF^*(p)$ при $p = 2^n$

$$e^{1,92(\ln p)^{1/3}(\ln\ln p)^{2/3}} \approx 2^{56} \quad \Rightarrow$$

$$1,92(\ln 2^n)^{1/3}(\ln\ln 2^n)^{2/3} \approx 56 \cdot \ln 2 \ \Rightarrow n \approx 383 \Rightarrow p \approx 2^{383}.$$

Аналогічно отриммаємо й інші результати:

Час, необхідний для розв’язання задачі дискретного логарифмування	Розмір поля $GF(p)$, над яким визначена еліптична крива	Порядок поля $GF(p)$ для групи $GF^*(p)$
2^{56}	2^{112}	2^{383}
2^{80}	2^{160}	2^{853}
2^{112}	2^{224}	2^{1859}
2^{128}	2^{256}	2^{2547}
2^{192}	2^{384}	2^{6732}
2^{256}	2^{512}	2^{13599}

Дані, наведені у таблиці, пояснюють причини поширення криптосистем на основі еліптичних кривих – значно коротший ключ в таких системах може забезпечити той самий рівень безпеки, що й криптосистеми, які побудовані на мультиплікативній групі простого поля $GF(p)$.

Задача 48 . Криптосистема NTRU визначена над кільцем усічених многочленів $\dfrac{Z[x]}{x^N - 1}$, елементами якого є многочлени степеня $N-1$, зведені за модулем $x^N - 1$. У цьому кільці добуток многочленів визначається не як звичайне множення, а як згортка (позначається $*$) . Під згорткою розуміють множення многочленів з умовою $x^N = 1$

(очевидно, при цьому $x^{N+1}=x$ і т. д.). Дії над многочленами у кільці $R_q=\frac{Z_q[x]}{x^N-1}$ визначаються так саме, як і у кільці $R=\frac{Z[x]}{x^N-1}$ з тією різницею, що операції над коефіцієнтами многочленів виконуються за $\bmod q$.

Генерація ключів. Необхідні параметри криптосистеми – це числа (N,p,q,d), де N,p – прості; НСД $(p,q)=$ НСД$(N,q)=1$, $q>(6d+1)p$. Секретний ключ користувача **A** утворюють два многочлени f і g, оборотні у кільцях R_q і R_p, причому:

- серед коефіцієнтів многочлена f є $(d+1)$ коефіцієнтів $(+1)$, d коефіцієнтів (-1), а решта нулі;
- у многочлена g кількість коефіцієнтів $(+1)$ і (-1) однакова і також дорівнює d (решта – нулі).

Далі користувач обчислює обернені многочлени f_q^{-1} і f_p^{-1} у кільцях R_q і R_p і визначає відкритий ключ $h=f_q^{-1}*g(\bmod q)$.

Зашифрування. Користувач **B**, що надсилає повідомлення $m\in R_p$, спочатку вибирає многочлен r, який має по d коефіцієнтів $(+1)$ і (-1), обчислює шифротекст $e=pr*h+m\,(\bmod q)$ і надсилає його користувачеві **A**.

Розшифрування. На своєму секретному ключі користувач **A** обчислює $a=f*e(\bmod q)$. Коефіцієнти цього многочлена він вибирає так, щоб вони належали проміжку $(-q/2;\,q/2)$. Далі коефіцієнти многочлена a зводяться за $\bmod p$ і обчислюється значення $f_p^{-1}*a(\bmod p)\equiv m$.

Припустимо, що параметри криптосистеми NTRU – $(N,p,q,d)=(7,\,2,\,37,1)$, а користувач **A** отримав шифроване повідомлення

$$e=35x^6+x^5+4x^4+4x^3+3x^2+3x+1.$$

Яким буде розшифрований текст, якщо до складу секретного ключа користувача входить многочлен $f=x^6+x^3+x$ і відомо, що $f_p^{-1}=x^6+x^5+x^4+x+1$? (зауваження: при виборі коефіцієнтів многочлена f враховано, що $-1\equiv 1\bmod 2$).

Р о з в' я з а н н я. Спершу користувач **A** обчислює

$$a = f * e = (x^6 + x^3 + x) * (35x^6 + x^5 + 4x^4 + 4x^3 + 3x^2 + 3x + 1) \bmod 37 \equiv$$
$$\equiv 35x^{12} + x^{11} + 4x^{10} + 2x^9 + 4x^8 + 5x^7 + 6x^6 + 7x^5 + 7x^4 + 4x^3 + 3x^2 + x \bmod 37.$$

Враховуючи, що при обчисленні згортки у кільці $R_{37} = \dfrac{Z_{37}[x]}{x^7 - 1}$ виконуються рівності

$$x^{12} \equiv x^5;\ \ x^{11} \equiv x^4;\ \ x^{10} \equiv x^3;\ x^9 \equiv x^2;\ x^8 \equiv x;\ \ x^7 \equiv 1,$$

отримаємо

$$a = 35x^5 + x^4 + 4x^3 + 2x^2 + 4x + 5 + 6x^6 + 7x^5 + 7x^4 + 4x^3 + 3x^2 + x \bmod 37 \equiv$$
$$\equiv 6x^6 + 5x^5 + 8x^4 + 8x^3 + 5x^2 + 5x + 5 \bmod 37.$$

Отже, при розшифруванні матимемо

$$m \equiv f_p^{-1} * a \,(\bmod\, p) =$$
$$= (x^6 + x^5 + x^4 + x + 1) * (6x^6 + 5x^5 + 8x^4 + 8x^3 + 5x^2 + 5x + 5) \bmod 2 =$$
$$= x^{11} + x^{10} + x^9 + x^8 + x^5 + x^4 + x^3 + 1 \equiv x^5 + x^2 + x + 1.$$

Задача 49. Зашифруйте відкритий текст $m = x^5 + 1$ за допомогою криптосистеми NTRU з параметрами $(N, p, q, d) = (7, 2, 29, 2)$, якщо відкритий ключ отримувача

$$h = 23x^6 + 24x^5 + 23x^4 + 24x^3 + 23x^2 + 23x + 23.$$

Як отримувач зможе розшифрувати надісланий йому шифротекст, якщо його секретний ключ $f = x^5 + x^4 + x^2 + x + 1$ і $f_p^{-1} = x^6 + x^5 + 1$?

Р о з в' я з а н н я. Виберемо многочлен над кільцем R_2:

$$r = x^6 + x^3 + x + 1.$$

Тоді шифротекст виглядатиме так:

$$e = p\,r * h + m \,(\bmod\, q) =$$
$$= 2(x^6 + x^3 + x + 1) * (23x^6 + 24x^5 + 23x^4 + 24x^3 + 23x^2 + 23x + 23) +$$
$$+ x^5 + 1 (\bmod 29) \equiv 14x^6 + 13x^5 + 14x^4 + 12x^3 + 12x^2 + 12x + 11 (\bmod 29).$$

Для розшифрування отримувачу знадобиться обернений многочлен до многочлена $f = x^5 + x^4 + x^2 + x + 1$ у кільці R_2. За алгоритмом Евкліда

$$x^7 - 1 \equiv x^7 + 1 = (x^5 + x^4 + x^2 + x + 1)(x^2 + x + 1) + x^2;$$

$$x^5 + x^4 + x^2 + x + 1 = x^2(x^3 + x^2 + 1) + x + 1;$$

$$x^2 = (x+1)(x+1) + 1 \qquad \Rightarrow$$

$$1 = x^2 + (x+1)^2 = x^2 + (x+1)[(x^5 + x^4 + x^2 + x + 1) + x^2(x^3 + x^2 + 1)] =$$

$$= x^2(x^4 + x^2 + x) + (x+1)(x^5 + x^4 + x^2 + x + 1)] =$$

$$= (x^5 + x^4 + x^2 + x + 1)(x^6 + x^5 + 1) + (x^4 + x^2 + x)(x^7 + 1) \quad \Rightarrow$$

Обернений многочлен $f_2^{-1} = x^6 + x^5 + 1$ (усі розрахунки за $\bmod 2$).

Тепер обчислюємо згортки

$$a = f * e (\bmod q) =$$

$$= (x^5 + x^4 + x^2 + x + 1) * (14x^6 + 13x^5 + 14x^4 + 12x^3 + 12x^2 + 12x + 11) \bmod 29 \equiv$$

$$\equiv 7x^6 + 4x^5 + 5x^4 + 5x^3 + 4x^2 + 5x + 4 \bmod 29;$$

$$f_2^{-1} * a (\bmod p) = (x^6 + x^5 + 1) * (7x^6 + 4x^5 + 5x^4 + 5x^3 + 4x^2 + 5x + 4) \bmod 2 \equiv$$

$$\equiv 16x^6 + 15x^5 + 16x^4 + 14x^3 + 14x^2 + 14x + 13 \bmod 2 \equiv x^5 + 1,$$

що збігається з заданим відкритим текстом.

Задача 50. Пара $(N, a) = (9991, 5)$ – відкритий ключ криптосистеми Голдвассер – Мікалі. За допомогою цієї системи зашифруйте чотири біти 1001. У якості випадкових параметрів виберіть $r_1 = 2427$, $r_2 = 8093$, $r_3 = 793$ і $r_4 = 3280$ відповідно.

Р о з в’ я з а н н я. Для зашифрування біта $m \in \{0,1\}$ за допомогою криптосистеми Голдвассер – Мікалі з відкритим ключем (N, a) потрібно вибрати випадкове ціле число $r \in \{1, 2, ..., N\}$ і обчислити шифротекст

$$c = \begin{cases} r^2 \bmod N, & \text{якщо } m = 0; \\ a\, r^2 \bmod N, & \text{якщо } m = 1. \end{cases}$$

$$m_1=1 \;\Rightarrow\; c_1 \equiv a r_1^2 \bmod n \equiv 5\cdot 2427^2 \bmod 9991 \equiv 8168;$$

$$m_2=0 \;\Rightarrow\; c_2 \equiv r_2^2 \bmod n \equiv 8093^2 \bmod 9991 \equiv 5644.$$

$$m_3=0 \;\Rightarrow\; c_3 \equiv r_3^2 \bmod n \equiv 793^2 \bmod 9991 \equiv 9407;$$

$$m_4=1 \;\Rightarrow\; c_4 \equiv a r_4^2 \bmod n \equiv 5\cdot 3280^2 \bmod 9991 \equiv 456.$$

Увесь шифротекст складається з чотирьох значень

$$(8168,\ 5644,\ 9407,\ 456).$$

Задача 51. Знайдіть біти відкритого тексту, що відповідають шифротексту $(21, 76, 68, 86)$, зашифрованому за допомогою криптосистеми Голдвассер – Мікалі, якщо секретний ключ криптосистеми $(89, 113)$.

Р о з в' я з а н н я. Для розшифрування визначимо, чи будуть числа $21, 76, 68, 86$ квадратичними лишками у кільці Z_{pq}, де $p=89, q=113$ – прості числа. Якщо це так, то відповідний елемент шифротексту розшифровується як нульовий біт, у противному випадку – як одиничний біт. Доказом того, що число $a \in Z_{pq}$ є квадратичним лишком, є виконання умови $\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=1$, де $\left(\frac{a}{p}\right)$ і $\left(\frac{a}{q}\right)$– символи Лежандра. Якщо число a не є кратним простому числу p, то ця арифметична функція визначається як

$$\left(\frac{a}{p}\right)=\begin{cases}+1, & \text{якщо } a \text{ – квадратичний лишок за } \bmod p;\\ -1, & \text{якщо } a \text{ – квадратичний нелишок за } \bmod p.\end{cases}$$

$$\left(\frac{21}{89}\right)=\left(\frac{3}{89}\right)\left(\frac{7}{89}\right)=(-1)^{\frac{(7-1)(89-1)}{4}}\left(\frac{89\bmod 3}{3}\right)(-1)^{\frac{(7-1)(89-1)}{4}}\left(\frac{89\bmod 7}{7}\right)=$$

$$=\left(\frac{2}{3}\right)\left(\frac{5}{7}\right)=(-1)^{\frac{3^2-1}{8}}\left(\frac{5}{7}\right)=-\left(\frac{5}{7}\right)=-(-1)^{\frac{(5-1)(7-1)}{4}}\left(\frac{7\bmod 5}{5}\right)=-\left(\frac{2}{5}\right)=$$

$$=-(-1)^{\frac{5^2-1}{8}}=1.$$

Отже, 21 – квадратичний лишок за $\bmod 89$. За аналогічними розрахунками отримаємо

$$\left(\frac{21}{113}\right)=-1;\quad \left(\frac{76}{89}\right)=-1;\quad \left(\frac{76}{113}\right)=1;$$

$$\left(\frac{68}{89}\right)=1;\quad \left(\frac{68}{113}\right)=-1;\quad \left(\frac{86}{89}\right)=1;\quad \left(\frac{86}{113}\right)=-1.$$

Це дозволяє визначити біти відкритого тексту: 11111.

ТЕСТИ

1. Які шифри використовують два типи ключів та однобічні функції з лазівкою?

   а) симетричні; б) блокові; в) потокові; г) асиметричні.

2. Дайте визначення однобічної функції $y=F(x)$, що здійснює відображення $X\to Y$, де X,Y – довільні множини.

   а) існує поліноміальний алгоритм обчислення значень функції $F(x)$ для всіх аргументів $x\in X$, але не існує поліноміального алгоритму обчислення значень оберненої функції $x=F^{-1}(y)$;

   б) існують поліноміальні алгоритми обчислення як значень функції $F(x)$, так і значень оберненої функції $x=F^{-1}(y)$ для всіх $x\in X$ і $y\in Y$;

   в) обчислити значення функції $F(x)$ для деяких аргументів $x\in X$ можна лише за експоненціальний час;

   г) існують експоненціальні алгоритми обчислення значень функції $F(x)$ для всіх $x\in X$ і поліноміальний алгоритм для обчислення значень оберненої функції $x=F^{-1}(y)$ для всіх $y\in Y$.

3. Функція належить до однобічних функцій з лазівкою, якщо

   а) для неї не існує оберненої;

   б) за будь-яких умов алгоритм обчислення значень її оберненої функції має поліноміальну складність;

   в) вона є однобічною коли невідома додаткова інформація;

   г) алгоритм обчислення значень її оберненої функції має поліноміальну складність за умови, що відома додаткова інформація.

4. Однобічною функція з лазівкою $y=F(x,k)$ здійснює відображення $X\to Y$, $k\in K$ – параметр, де X,Y,K – довільні множини. Укажіть, яка часова складність нижченаведених алгоритмів:

i – алгоритм обчислення значень функції $y = F(x,k)$ для всіх аргументів $x \in X$ і всіх значень параметрів $k \in K$;

ii – алгоритм обчислення значень оберненої функції $x = F^{-1}(y,k)$ для всіх аргументів $x \in X$ без знання значення параметра $k \in K$;

iii – алгоритм обчислення значень оберненої функції $x = F^{-1}(y,k)$ для всіх аргументів $x \in X$ при відомому значенні параметра $k \in K$.

а) **i** – експоненціальна; **ii** – поліноміальна; **iii** – експоненціальна;
б) **i** – експоненціальна; **ii** – експоненціальна; **iii** – експоненціальна;
в) **i** – поліноміальна; **ii** – експоненціальна; **iii** – експоненціальна;
г) **i** – поліноміальна; **ii** – експоненціальна; **iii** – поліноміальна.

5. Наведені нижче пари функцій задають час роботи деяких алгоритмів. Визначте, які алгоритми матимуть однаковий порядок зростання складності.

а) $n(n+2)$ і $2000n^2$; б) $1000n^2$ і $0,001n^3$;

в) $\log_2 n$ і $\ln n$; г) 2^{n-1} і 2^{n+1}.

6. Для розв'язання задачі маємо два алгоритми, перший із яких з часовою складністю $O(4^n)$, а другий – $O(n^4)$. При якій довжині n вхідних даних другий алгоритм має переваги над першим?

а) $n = 2$; б) $n \geq 2$; в) $n > 4$; г) при будь-якій.

7. У скільки разів довше буде розв'язуватися задача за допомогою алгоритму з часовою складністю $T(n) = O(n^3)$, якщо розмір вхідних даних подвоїти?

а) 2; б) 4; в) 6; г) 8; д) 64.

8. Нижче наведено часову складність $T = O(f(n))$ алгоритмів розв'язання деяких задач. Які з них належать до класу P-задач?

а) $f(n) = n^2$; б) $f(n) = 5n$; в) $f(n) = n^2 + 2n$;

г) $f(n) = n!$; д) $f(n) = 4^n$; е) $f(n) = n \cdot \lg n$.

9. Часова складність $O(f(n))$ деяких алгоритмів описується функціями:

$f(n) = n^n$; $\exp\sqrt{\log_2 n \log_2 \log_2 n}$; 1; $\log_2 \log_2 n$; n^c; n^ε; $n^{\log_2 n}$; $\log_2 n$,

де ε і c – константи, для яких $0<\varepsilon<1<c$. Впорядкуйте ці функції за зростанням їх темпів асимптотичного зростання.

а)1; $\log_2 n$; $\log_2\log_2 n$; n^{ε}; n^{c}; $\exp\sqrt{\log_2 n \log_2\log_2 n}$; $n^{\log_2 n}$; n^{n};

б)1; $\log_2\log_2 n$; $\log_2 n$; n^{ε}; n^{c}; $\exp\sqrt{\log_2 n \log_2\log_2 n}$; $n^{\log_2 n}$; n^{n};

в)1; $\log_2\log_2 n$; $\log_2 n$; n^{ε}; $\exp\sqrt{\log_2 n \log_2\log_2 n}$; n^{c}; $n^{\log_2 n}$; n^{n};

г)$\log_2\log_2 n$; 1; $\log_2 n$; n^{c}; $\exp\sqrt{\log_2 n \log_2\log_2 n}$; n^{ε}; $n^{\log_2 n}$; n^{n};

д)1; $\log_2\log_2 n$; $\log_2 n$; n^{c}; n^{ε}; $n^{\log_2 n}$; $\exp\sqrt{\log_2 n \log_2\log_2 n}$; n^{n}.

10. Для розв'язання яких з нижченаведених задач існують ефективні алгоритми з поліноміальною складністю?

а) факторизація великих чисел;
б) обчислення значення функції Ейлера великого числа;
в) визначення секретного параметра d криптосистеми RSA за відомим відкритим ключем (n,e);
г) шифрування $C=M^{e}(\mathrm{mod}\, n)$ відкритого тексту M за допомогою криптосистеми RSA;
д) обчислення ЕЦП RSA $M^{d}(\mathrm{mod}\, n)$ для документа M за відомим відкритим ключем (n,e).

11. Часову складність алгоритмів часто описують функцією $L(t,v,\lambda)=\exp(\lambda t^{v}(\log t)^{1-v})$, де $0\le v\le 1$, $\lambda>0$, $t=\lceil \log_2 n \rceil$ – довжина у бітах вхідного числа. Яке з наведених тверджень щодо складності алгоритмів *правильне*?

а) при $v=0$ функція $L(t,0,\lambda)$ описує експоненціальну складність;
б) при $v=1$ функція $L(t,1,\lambda)$ описує поліноміальну складність;
в) при $0<v<1$ функція $L(t,v,\lambda)$ описує субекспоненціальну складність;
г) усі твердження а) – в) правильні.

12. У криптографії з відкритим ключем

а) як зашифрування, так і розшифрування виконується тільки за допомогою відкритого ключа;
б) як зашифрування, так і розшифрування виконується тільки за допомогою секретного ключа;
в) для зашифрування використовується відкритий ключ, а для розшифрування – секретний;

г) для електронного цифрового підпису використовується секретний ключ, а для його верифікації – відкритий.

13. За даними РИА Новости у 2011 р. у всьому світі було зафіксовано ~2,1 мільярда користувачів Інтернету. Якби всі вони вирішили обмінятися між собою інформацією, зашифрованою за допомогою симетричного шифру, то потрібно було б згенерувати і розподілити між ними приблизно

а) $\sim 2{,}1 \cdot 10^{9}$ ключів; б) $\sim 2{,}205 \cdot 10^{18}$ ключів;

в) $\sim 4{,}2 \cdot 10^{12}$ ключів; г) $\sim 4{,}2 \cdot 10^{18}$ ключів.

14. Криптосистеми з відкритим ключем можна використовувати

а) як засіб аутентифікації користувачів;
б) як засіб для захищеного розподілу ключів;
в) безпосередньо для зашифрування і передачі інформації невеликого об'єму;
г) для зашифрування інформаційних потоків великого об'єму у реальному часі.

15. Стійкість усіх криптосистем з відкритим ключем базується на

а) можливості отримання верхніх оцінок складності задач, що покладено в основу криптосистеми;
б) припущенні про ймовірнісний характер шифрування;
в) припущенні існування однобічних функцій;
г) гіпотезі $P \neq NP$;
д) існуванні нетривіального статистичного розподілу символів одночасно у відкритому тексті та шифротексті.

16. Які переваги асиметричних шифрів над симетричними?

а) непотрібно передавати секретний ключ надійним безпечним каналом зв'язку;
б) за умови забезпечення одного й того самого рівня безпеки довжини ключів, що використовуються у асиметричних шифрах, будуть меншими, ніж довжини ключів симетричних шифрів.
в) швидкість шифрування асиметричних шифрів вище за швидкість симетричних;
г) спрощення керування ключами у великій мережі.

17. Що не відноситься до недоліків асиметричних шифрів?

а) за умови забезпечення одного й того самого рівня безпеки довжини ключів, що використовуються у асиметричних шифрах, більші, ніж довжини ключів симетричних шифрів;
б) ускладнюється процес керування ключами у мережі з великою кількістю абонентів;
в) швидкість шифрування асиметричних шифрів вище за швидкість симетричних;
г) процеси зашифрування і розшифрування потребують великих обчислювальних ресурсів.

18. Чому криптосистеми з відкритим ключем використовують лише для захисту даних невеликого об'єму?

а) ключі криптосистем з відкритим ключем повинні бути фіксованої довжини;
б) відкриті ключі мають зберігатися у секреті;
в) відповідні алгоритми дуже повільно працюють;
г) відкриті ключі мають дуже часто змінюватися.

19. У гібридній криптографічній системі зазвичай

а) зашифрування відкритих текстів здійснюють за допомогою асиметричного шифру на відкритому ключі;
б) секретний сеансовий ключ використовується для зашифрування відкритих текстів;
в) ні відкритий ключ, ні секретний ключі асиметричного шифру не застосовують;
г) не використовується цифровий сертифікат;
д) секретний сеансовий ключ передається у зашифрованому за допомогою криптосистеми з відкритим ключем вигляді.

20. Серед наведених тверджень щодо криптоалгоритму RSA два *неправильні*. Які?

а) криптоалгоритм був затверджений як національний стандарт шифрування;
б) криптоалгоритм RSA використовується як для шифрування масивів даних, так і для створення електронного цифрового підпису;
в) криптоалгоритм RSA застосовується для розподілу ключів між користувачами;
г) назва криптоалгоритму RSA походить від перших букв прізвищ його розробників.

21. Виберіть криптосистеми, що основані на задачі факторизації великих чисел.

а) RSA; б) Ель-Гамаля; в) DES; г) Рабіна.

22. Криптографічна стійкість алгоритму RSA базується на складності

а) обчислення дискретного логарифма у скінченних полях;
б) операції множення двох великих чисел;
в) факторизації великих чисел;
г) перевірки простоти великих простих чисел.

23. Доведення коректності шифрування за допомогою алгоритму RSA основане на

а) теоремі Ейлера;
б) теоремі про існування первісних коренів за модулем великого числа;
в) властивостях символу Лежандра;
г) розширеному алгоритмі Евкліда.

24. Модуль криптоалгоритму RSA являє собою

а) добуток двох великих простих чисел;
б) квадрат великого простого числа;
в) частку від ділення великого простого числа на менше просте число;
г) результат обчислення степеня числа з великим показником.

25. Тільки одне з наведених нижче тверджень про криптоалгоритм RSA є *правильним*. Яке?

а) криптоалгоритм RSA дозволяє виконувати зашифрування набагато швидше, ніж криптоалгоритм DES;
б) криптоалгоритм RSA використовується для захисту корпоративних даних у середовищі з високою пропускною здатністю і низькою латентністю (з низьким рівнем затримання);
в) RSA – симетричний криптоалгоритм;
г) RSA з ключами довжиною у 512 бітів можна задіяти для більш швидкого зашифрування, а з ключами довжиною 2048 бітів – для збільшення безпеки шифрування.

26. Якщо n – модуль криптосистеми RSA, e – її відкрита експонента, то яка з нижченаведених задач називається задачею RSA?

а) для числа $1 < C < n$ знайти число M, для якого $C \equiv M^e \bmod n$;
б) знайти прості дільники p і q числа n;

в) визначити, чи буде число $1 < C < n$ квадратичним лишком за модулем n;

г) за даним числом $1 < C < n$ знайти таке значення M, для якого $M \equiv C^e \bmod p$.

27. Якщо користувач криптосистеми RSA вибрав для генерації модуля два числа $p = 11$, $q = 47$, то як відкриту експоненту серед чисел $12; 33; 125; 513$ він може вибрати

а) 12; б) 33; в) 125; г) 513.

28. Згенеруйте другу частину відкритого ключа та секретний ключ абонента криптосистеми RSA, якщо відомо, що він вибрав $p = 5$, $q = 11$, $e = 13$.

а) $n = 16$; $d = 23$; б) $n = 55$; $d = 37$; в) $n = 55$; $d = 2$;
г) $n = 16$; $d = 17$; д) $n = 55$; $d = 17$.

29. Зашифруйте відкрите повідомлення $M = 100$ за допомогою криптосистеми RSA, відкритий ключ якої $(n, e) = (517, 3)$.

а) $C = 12$; б) $C = 21$; в) $C = 122$; г) $C = 221$; д) $C = 212$.

30. Розшифруйте повідомлення 1552 – 352, отримане при зашифруванні за допомогою криптосистеми RSA, модуль якої $n = 1739$, а закрита експонента $d = 5$ (абетка українська).

а) ДОБА; б) ОДЯГ; в) РЯД; г) КІТ.

31. Яке з нижченаведених простих чисел недоцільно вибирати як відкриту експоненту криптоалгоритму RSA?

а) 32771; б) 32801; в) 32833; г) 32749.

32. Чому не вибирають парне число як відкриту експоненту e криптоалгоритму RSA?

а) шифрування потребує піднесення до степеня з показником e, а така операція триває значно довше, якщо показник парний;

б) при парній відкритій експоненті закрита експонента обов'язково непарна, а тоді дешифрувати текст неможливо;

в) якщо відкрита експонента парна, то НСД$(e, \varphi(n)) \neq 1$ і тоді неможливо знайти закриту експоненту d з порівняння $ed \equiv 1 (\bmod \varphi(n))$ і, відповідно, дешифрувати закритий текст.

33. За яких умов число p називається сильним псевдопростим?

а) p – велике просте число;

б) p – добуток двох великих простих чисел;

в) число $p-1$ має достатньо великий простий дільник q_1, а число q_1-1, у свою чергу, має достатньо великий простий дільник q_2;

г) p – складене, НОД $(a,p)=1$, $a^{p-1}\equiv 1(\mathrm{mod}\, p)$;

д) число $p+1$ має великі прості дільники;

34. Зашифрування відкритого тексту $M=1$ за допомогою криптосистеми RSA на будь якому ключі породжує шифротекст $C=1$. Тому коли супротивник побачить такий шифротекст, він може легко здогадатися, що шифрували відкритий текст $M=1$. Як у реальності долають цю проблему?

а) у цифрових еквівалентах відкритих текстів завжди викреслюють усі одиничні блоки;

б) повідомлення перед шифруванням кодується, наприклад, за допомогою OAEP кодування;

в) додатково шифрують вектор ініціалізації і здійснюють конкатенацію шифрованого тексту та шифрованого вектора ініціалізації, що приховує структуру тексту;

г) у цифрових еквівалентах відкритих текстів замінюють усі одиничні блоки на блоки вигляду 101, 1001, …, 10..01.

35. Якщо (n,e) – відкритий ключ криптоалгоритму RSA, (p,q,d) – його закритий ключ, то атака на криптоалгоритм може зводитися до задачі факторизації числа

а) q; б) p; в) n; г) $\varphi(n)$; д) e; е) d.

36. Яка слабкість притаманна шифруванню за допомогою криптоалгоритму RSA? Вважайте, що $E(M)$ – функція зашифрування, n – модуль криптосистеми.

а) $E(-M)=-E(M)\bmod n$;

б) $E(M_1)+E(M_2)=E(M_1+M_2)\bmod n$;

в) $E(M_1)-E(M_2)=E(M_1-M_2)\bmod n$;

г) $E(M_1)\cdot E(M_2)=E(M_1\cdot M_2)\bmod n$;

д) $E(M)^k=E(M^k)\bmod n$, де k – ціле.

37. Перехопивши криптограму повідомлення $M \in Z_n$, для якого НСД$(M,n)>1$, криптоаналітик отримує нетривіальний дільник модуля n криптоалгоритму RSA. Якщо e – відкрита експонента, (p,q,d) – закритий ключ криптоалгоритму, то скільки існує таких відкритих повідомлень?

а) $p+q$; б) $p+q-1$; в) $p+q-d$; г) $p+q+e$; д) $pe+qd$.

38. Яка атака на криптоалгоритм RSA базується на властивості мультиплікативності цього алгоритму?

а) зустріч посередині; б) чоловік посередині;
в) безключове читання; г) Вінера.

39. Якщо перехоплено деякий шифротекст C, отриманий за допомогою криптоалгоритму RSA з відкритим ключем (n,e), то при проведенні атаки безключового читання, потрібно виконувати послідовні шифрування на відкритому ключі:

$$C^e(\mathrm{mod}\, n)\equiv C_1;\ \ C_1{}^e(\mathrm{mod}\, n)\equiv C_2,\ \ \ C_2{}^e(\mathrm{mod}\, n)\equiv C_3,\ldots$$

доти, поки не виникне

а) вихідний шифротекст C;
б) будь-яке просте число;
в) одиниця;
г) нуль;
д) відрізок ключа.

40. Криптоаналітик намагається застосувати метод безключового читання до шифротексту $C=2342$, отриманого при зашифруванні деякого тексту за допомогою криптосистеми RSA з відкритим ключем $(2773,17)$. Скільки посладовних зашифрувань йому доведеться здійснити, щоб отримати вихідний шифротекст?

а) 16; б) 17; в) 43; г) 44; д) 2772.

41. (n,e) – відкритий ключ криптоалгоритму RSA. У разі малого порядку відкритої експоненти за модулем $\varphi(n)$ криптоалгоритм піддається атаці

а) «зустріч посередині»; б) «чоловік посередині»;
в) безключового читання; г) Вінера.

42. (n,e) – відкритий ключ криптоалгоритму RSA, (p,q,d) – його закритий ключ. За якої умови криптоалгоритм не може встояти перед атакою Вінера?

а) $d \ge \frac{1}{3}\sqrt[4]{n}+e$; б) $d < \frac{1}{2}\sqrt[3]{ne}$; в) $d < \frac{1}{4}\sqrt[3]{n}$; г) $d < \frac{1}{3}\sqrt[4]{n}$;

д) $d < \frac{1}{3}\sqrt[4]{p+q}$; е) $p+q < \frac{1}{3}\sqrt[4]{n}$; є) $p+q \ge \frac{1}{4}\sqrt[n]{n}$.

43. Атака Вінера на криптоалгоритм RSA з відкритим ключем (n,e) базується на зображенні ланцюговим дробом числа

а) $\frac{e}{n}$; б) $\frac{n}{e}$; в) $\frac{e}{n}+\frac{n}{e}$; г) $\frac{n}{e^2}$; д) $\frac{n}{3e}$; е) $\frac{n+e}{e-1}$.

44. Криптоаналітик намагається провести атаку Вінера і розкрити закриту експоненту d криптосистеми RSA з відкритими ключами

$$(n,\ e) = (6852403,\ 3651823).$$

Він знаходить перші п'ять підхідних дробів для числа $\frac{3651823}{6852403}$:

$$\frac{0}{1}, \frac{1}{1}, \frac{1}{2}, \frac{8}{15}, \frac{81}{152},$$

звідки випливає, що $d \in \{1; 2; 15; 152\}$. Серед наступних тверджень виберіть ті, з якими Ви згодні.

а) $d \ne 2$, бо d має бути взаємно простим із значенням функції Ейлера $\varphi(n)$, яке завжди є парним;

б) $d \ne 152$, оскільки $152 > \frac{1}{3}\sqrt[4]{n} \approx 17,0545$;

в) d може бути тільки парним числом, тому $d \ne 15$;

г) $\varphi(n) = \frac{ed-1}{8} = \frac{3651823 \cdot 15 - 1}{8}$.

45. Одне відкрите повідомлення зашифроване і надіслано двом користувачам криптосистеми RSA, які мають відкриті ключі $(n;\ e_1)$ та $(n; e_2)$ відповідно. Як криптоаналітик, перехопивши обидва надіслані шифротексти C_1 і C_2, може прочитати відкрите повідомлення M?

а) $M = C_2^{t_1} C_1^{-t_2} (\mathrm{mod}\, n)$, де $t_1 \equiv e_1^{-1} (\mathrm{mod}\, e_2)$, $t_2 = (t_1 e_1 + 1)/e_2$;

б) $M = C_1^{t_1} C_2^{-t_2} (\mathrm{mod}\, n)$, де $t_1 \equiv e_1^{-1} (\mathrm{mod}\, e_2)$, $t_2 = (t_1 e_1 - 1)/e_2$;

в) $M = (C_1 C_2)^{t_1 - t_2} (\mathrm{mod}\, n)$, де $t_1 \equiv e_1^{-1} (\mathrm{mod}\, e_2)$, $t_2 = (t_1 e_1 - 1)/e_2$;

г) $M = (C_1 C_2)^{t_1 + t_2} (\mathrm{mod}\, n)$, де $t_1 \equiv e_2^{-1} (\mathrm{mod}\, e_1)$, $t_2 = (t_1 e_2 - 1)/e_1$.

46. Нехай абоненти **A**, **B** і **C** криптосистеми RSA мають відповідно відкриті ключі $(n_1, 3)$, $(n_2, 3)$ та $(n_3, 3)$. Дехто надсилає кожному з них однакове відкрите повідомлення, зашифроване за допомогою цих ключів. Як криптоаналітик, перехопивши три надіслані шифротексти C_1, C_2 і C_3, зможе відновити відкритий текст M ?

а) $M = (C_1 C_2 C_3)^3 \bmod (n_1 + n_2 + n_3)$;

б) $M = (C_1 + C_2 + C_3)^3 \bmod n_1 n_2 n_3$;

в) $M = 3m$, де m – розв'язок системи $\begin{cases} m \equiv C_1 (\mathrm{mod}\, n_1), \\ m \equiv C_2 (\mathrm{mod}\, n_2), \\ m \equiv C_3 (\mathrm{mod}\, n_3); \end{cases}$

г) $M = \sqrt[3]{m}$, де m – розв'язок системи $\begin{cases} m \equiv C_1 (\mathrm{mod}\, n_1), \\ m \equiv C_2 (\mathrm{mod}\, n_2), \\ m \equiv C_3 (\mathrm{mod}\, n_3). \end{cases}$

47. Порівняйте швидкості шифрування за допомогою алгоритмів DES, AES і RSA-1024. Що з нижченаведеного є правдою?

а) AES швидший за RSA-1024, який швидший за DES;
б) RSA-1024 швидший за AES і DES;
в) AES швидший за DES, який швидший за RSA-1024;
г) DES швидший за AES, який швидший за RSA-1024.

48. Якщо $C = M^e (\mathrm{mod}\, n)$ і $M = C^d (\mathrm{mod}\, n)$ – рівняння зашифрування і розшифрування криптосистеми RSA відповідно, то її стійкість визначається

а) розміром модуля;
б) тільки розміром відкритої експоненти;

в) тільки розміром закритої експоненти;
г) розміром відкритого тексту.

49. $C = 42$ – шифртекст, отриманий за допомогою криптосистеми RSA з відкритими ключами $(n, e) = (247,17)$. Відповідна закрита експонента криптосистеми $d = 89$. Розшифрування за допомогою RSA-CRT зводиться до системи порівнянь

а) $\begin{cases} M = 42^5 \bmod 19, \\ M = 42^{17} \bmod 13 \end{cases}$; б) $\begin{cases} M = 42^5 \bmod 247, \\ M = 42^{17} \bmod 216 \end{cases}$;

в) $\begin{cases} M = 42^5 \bmod 13, \\ M = 42^{17} \bmod 19 \end{cases}$; г) $\begin{cases} M = 42^{89} \bmod 17, \\ M = 42^{17} \bmod 89. \end{cases}$

50. Яку мінімальну кількість множень за модулем потрібно виконати, щоб обчислити значення $a^{75} (\bmod m)$ за методом квадратів і множень (двійкового потенціювання)?

а) відповідь залежіть від значення чисел a і m;
б) 8; в) 9; г) 10; д) 74; е) 75.

51. Яка часова складність обчислення значення $a^k (\bmod m)$ за методом квадратів і множень (двійкового потенціювання)?

а) $O(k)$; б) $O(\log_2 \sqrt{a})$; в) $O(\log_2 m)$;
г) $O(\log_2 k)$; д) $O(m)$;
е) відповідь залежіть від значення чисел a, k і m.

52. Яка ймовірність помилково визнати складене число n за просте у разі перевірки його простоти за допомогою тесту Соловея – Штрассена k разів?

а) $(3/4)^{-k}$; б) 2^{-k}; в) 4^{-k}; г) 4^{-nk}; д) 2^{-n}; е) $(3/4)^{-n}$.

53. У разі k-разового застосування тесту Міллера – Рабіна для перевірки простоти числа n імовірність помилково визнати складене число за просте дорівнює

а) $(3/4)^{-k}$; б) 2^{-k}; в) 4^{-k}; г) 4^{-nk}; д) 2^{-n}; е) $(3/4)^{-n}$.

54. Яку мінімальну кількість разів потрібно застосувати тест Міллера – Рабіна для перевірки простоти числа n, щоб імовірність помилково визнати складене число за просте не перевищила 2^{-80}?

а) 2; б)4; в) 20; г) 30; д) 40; е) інша відповідь.

55. В основу тесту Міллера – Рабіна перевірки простоти чисел покладено

а) малу теорема Ферма;
б) обчислення символу Якобі;
в) умову: непарне число n буде складеним, якщо воно є повним квадратом або існують такі числа $x, y \in N$, що $x \not\equiv \pm y \bmod n$, $x^2 \equiv y^2 \bmod n$;
г) критерій Ейлера.

56. Уявіть, що за допомогою алгоритму Міллера – Рабіна ви перевіряєте простоту множників для модуля криптосистеми RSA і вибрали для перевірки число $n = 1000000000039 = 10^{12} + 39$. У першій серій досліджень жодне з чисел $i = 2,3,...,100$ не стало свідком непростоти числа n. У другій серії досліджень Ви за допомогою того самого тесту встановили, що усі числа $i = 2,3,...,0,3 \cdot 10^6$ не вказують на можливість факторизувати число n. Яке з наступних тверджень *неправильне*?

а) тест Міллера – Рабіна відноситься до ймовірнісних;
б) якщо число n було складеним, то принаймні 75 % перевірених свідків засвідчили б непростоту числа;
в) ймовірність того, що за результатами другої серії досліджень число n визнане простим помилково, складає $4^{-300\,000} \approx 0$.
г) ймовірність того, що за результатами другої серії досліджень число n визнане простим правильно, складає 2^{-100}.

57. Який з нижченаведених тестів перевірки на простоту не розпізнає непростоту чисел Кармайкла?

а) Ферма; б) Соловея – Штрассена;
в) Міллера; г) Міллера – Рабіна.

58. При перевірці числа Кармайкла $n = 561 = 3 \cdot 11 \cdot 17$ за допомогою імовірнісного тесту Ферма кількість баз a $(1 \le a \le n)$, при кожній з яких буде отримано результат «ймовірно просте число», дорівнює

а) 1; б) 241; в) 320; г) 560; д) 561; е) інша відповідь.

59. Упорядкуйте наведені тести на простоту чисел за спаданням імовірності помилки у найгіршому випадку (тобто помилково визнати складене число за просте або «ймовірно просте»).
    1 – простий алгоритм Ленстри тестування простоти (ECPP);
    2 – п'ять проходів тесту Міллера – Рабіна;
    3 – п'ять проходів тесту Соловея – Штрасеена;
    4 – п'ять проходів тесту на основі малої теореми Ферма.

    а) 2,1,3 = 4; б) 1,2, 3 = 4; в) 1,2,4,3; г) 3,2,4,1; д) 2,4=3, 1.

60. Щоб ускладнити факторизацію модуля криптосистеми RSA, на вибір множників p і q накладають умови

    а) p чи q має бути числом Мерсенна або числом Ферма;
    б) p і q обов'язково є числами-близнюками;
    в) $p = 1 \bmod k$ або $q = 1 \bmod l$ при деяких великих цілих k, l;
    г) p і q – великі сильно прості числа.

61. Якщо не брати до уваги довжину далі використаних чисел і, врахувавши, що усі вони прості, визначте, який з поданих добутків доцільно вибрати як модуль криптосистеми RSA?

    а) $n = 10007 \cdot 10009$;
    б) $n = \left(2^{13} - 1\right)\left(2^{2^4} + 1\right) = 8191 \cdot 65537$;
    в) $n = \left(2^7 - 1\right)\left(2^{17} - 1\right) = 127 \cdot 131071$;
    г) $n = 101 \cdot 10000019$;
    д) будь-яке з наведених у пунктах а) – г);
    е) жодного.

62. У якому разі числа p і q називаються сильними простими числами?

    а) коли вони є числами-близнюками ($p - q = 2$);
    б) коли різниця $p - q$ є великою;
    в) за умови, що $p \not\equiv 1 \pmod r$, $r \not\equiv 1 \pmod t$, де p, r, t – прості числа;
    г) за умови, що $p - 1 \equiv 0 \pmod r$, $p + 1 \equiv 0 \pmod s$, $r \equiv 1 \pmod t$, де p, r, s, t – великі прості числа.

63. Які обмеження у криптосистемі RSA накладають на вибір множників p і q, щоб модуль криптосистеми не був вразливим до факторизації чисел за методом Ферма?

а) числа $p-1$ и $q-1$ повинні мати великий простий дільник;
б) числа $p+1$ и $q+1$ повинні мати малий простий дільник;
в) добуток pq має бути псевдопростим ;
г) різниця $p-q$ має бути великою.

64. ρ-метод Полларда для факторизації чисел використовує

а) парадокс днів народження;
б) алгоритм Флойда;
в) простоту чисел, за модулем яких виконуються обчислення;
г) істинно випадкову числову послідовність.

65. Нехай $n=pq$, де множник p є таким, що число $p-1$ – гладке. Припустимо, що усі множники числа $p-1$ менші, ніж 30. Тоді для запуску $(p-1)$- алгоритму Полларда показник k при обчисленні виразу $a \equiv a^k \bmod n$ (при деякому a) має бути
а) $k=2\cdot3\cdot5\cdot7\cdot11\cdot13\cdot17\cdot19\cdot23\cdot29$ (добуток усіх простих чисел, менших тридцяти);
б) $k=2\cdot4\cdot6\cdot\ldots\cdot30$ (добуток усіх парних чисел, менших тридцяти);
в) $k=30^2-1$;
г) $k=\left\lceil\sqrt{30}-1\right\rceil$.

66. При факторизації модуля n криптосистеми RSA за методом неперервних дробів знаходять підхідні дроби до звичайного неперервного дробу, що відповідає числу
а) $\frac{1}{\sqrt{n}}$; б) $\frac{1}{n}$; в) $\frac{1}{n^2}$; г) e^{-n}; д) $\sqrt{n}$.

67. В алгоритмі квадратичного решета при факторизації модуля n криптосистеми RSA для просіяних чисел обчислюють значення функції $f(x)$ і перевіряють гладкість цих значень. Укажіть цю функцію.

а) $f(x)=(x+[\sqrt{n}])^2-n$; б) $f(x)=(x-[\sqrt{n}])^2-n$;
в) $f(x)=[\sqrt{n}]-x^2$; г) $f(x)=(n-[\sqrt{n}])^2+x$.

68. Часова складність алгоритму решета числового поля для факторизації чисел описується функцією

$$L(N) = 2^{1,9229 \cdot N^{1/3} \cdot (\log_2 N)^{2/3}},$$

де N – довжина числа. Скільки операцій потрібно виконати алгоритму, аби розкласти на множники число довжиною 1024 біти?

а) 2^{43}; б) 2^{66}; в) 2^{89}; г) 2^{129}; д) 2^{256}.

69. Якщо p, q – два великих простих множники, то які з нижченаведених задач поліноміально еквівалентні задачі факторизації великих чисел?

а) визначення закритої експоненти криптоалгоритма RSA за відомими значеннями модуля і відкритої експоненти;
б) обчислення функції Ейлера від числа $n = pq$;
в) обчислення степеня $M^e \pmod n$, де модуль $n = pq$;
г) визначення дискретного логарифма числа за великим модулем;
д) добування квадратних коренів за модулем числа $n = pq$.

70. П. Шор для розробки свого квантового алгоритму факторизації чисел використав

а) квантовий варіант лінійного криптоаналізу S-боксів криптоалгоритму RSA;
б) квантове перетворення Фур'є для визначення періоду функції;
в) розв'язання NP-проблеми за допомогою квантової імітації відпалу;
г) квантове розфарбування графа.

71. Який асиметричний криптоалгоритм, використовуючи 160-бітові ключі, має стійкість, близьку до стійкості алгоритму RSA-1024?

а) Ель-Гамаля; б) 3-DES;
в) криптосистема на еліптичних кривих; г)Діффі – Хеллмана.

72. Нехай абонент **B** криптосистеми RSA вибрав для зашифрування модуль n і дві відкриті експоненти e_1 і e_2 та умовив абонента **A** спочатку зашифрувати своє повідомлення M на ключі e_1, а далі до отриманого шифротексту C_1 знову застосувати криптоалгоритм RSA, але на ключі e_2. Виберіть *правильне* твердження щодо стійкості такого подвійного зашифрування, припустивши, що криптоаналітик перехопив шифротексти C_1 і C_2.

а) стійкість шифрування збільшується порівняно з однократним використанням RSA;

б) стійкість шифрування не зростає, оскільки, якщо криптоаналітик розкриє закритий ключ d_1, відповідний відкритому ключу e_1, то він зможе факторизувати модуль криптосистеми, знайти закритий ключ d_2 і далі прочитати відкритий текст;

в) стійкість шифрування зростає, оскільки, навіть, якщо криптоаналітик розкриє закритий ключ d_1, відповідний відкритому ключу e_1, то він не зможе факторизувати модуль криптосистеми;

г) стійкість шифрування не збільшується порівняно з однократним використання RSA, бо криптоаналітик легко зможе застосувати частотний аналіз.

73. Порівняно з криптоалгоритмом RSA застосування алгоритму RSA-OAEP дає змогу протистояти атакам

а) суперзашифрування;
б) на основі зашифрування множини подібних шифрів за допомогою відкритого ключа и порівняння їх з перехопленим шифротекстом;
в) факторизації модуля RSA за допомогою методу числового решета;
г) на основі використання спільної відкритої експоненти $e = 3$ кількома користувачами;
д) факторизації модуля RSA за допомогою $(p-1)$-алгоритму Полларда.

74. Криптографічна стійкість алгоритму Ель-Гамаля базується на складності

а) обчислення дискретного логарифма у скінченних полях;
б) операції піднесення до степеня за модулем;
в) факторизації великих чисел;
г) обчислення символу Лежандра.

75. Чому криптосистему Ель-Гамаля можна віднести до схеми ймовірнісного шифрування?

а) через подвоєння довжини шифротексту порівняно з довжиною відкритого тексту;
б) через використання відкритих і секретних ключів;
в) через уведення у процес шифрування рандомізатора;
г) через складність задачі дискретного логарифмування, покладеної в основу криптосистеми.

76. Нехай $p = 17$, $g = 3$ – відкриті параметри криптосистеми Ель-Гамаля, спільні для декількох користувачів, $a = 7$ – секретний ключ одного з них. Завершіть формування його відкритих ключів.

а) $h=10$; б) $h=11$; в) $h=12$; г) $h=3$; д) $h=4$; е) $h=5$.

77. (p,g,h) – відкритий ключ, a – секретний ключ криптосистеми Ель-Гамаля, r – рандомізатор, вибраний для зашифрування відкритого повідомлення M. Як знайти шифротекст?

а) $(h^r \bmod p,\ M\cdot g^r \bmod p)$; б) $(g^r \bmod p,\ M+h^r \bmod p)$;

в) $(g^r \bmod p,\ M\cdot h^r \bmod p)$; г) $(M\cdot g^{-r} \bmod p,\ h^r \bmod p)$;

д) $(M\cdot g^r \bmod p,\ h^{-r} \bmod p)$; е) $(g^a \bmod p,\ M\cdot h^a \bmod p)$.

78. (p,g,h) – відкритий ключ, a – секретний ключ криптосистеми Ель-Гамаля, (C_1,C_2) – отриманий шифротекст, отриманий у результаті зашифрування відкритого повідомлення M. Як провести розшифрування?

а) $M=C_2(C_1{}^a)^{-1} \bmod p$; б) $M=C_1(C_2{}^a)^{-1} \bmod p$;

в) $M=(C_1{}^aC_2)^{-1} \bmod p$; г) $M=(C_1C_2{}^a)^{-1} \bmod p$;

д) $M=C_1{}^aC_2h \bmod p$; е) $M=C_1C_2{}^ah \bmod p$.

79. $p=23$, $g=5$, $h=21$ – відкриті параметри користувача у криптосистемі Ель-Гамаля. Дехто хоче надіслати йому повідомлення $M=15$, вибравши рандомізатор $r=7$. Знайдіть шифротекст.

а) (13, 8); б) (14, 9); в) (14, 17);
г) (16, 12); д) (12, 15); е) (17, 12).

80. Відкритому тексту M відповідає шифротекст $(C_1, C_2)=(3,5)$, отриманий за допомогою криптосистеми Ель-Гамаля. Відновіть цей текст, якщо секретний ключ $a=4$, доменний параметр $p=7$.

а) 2; б) 3; в) 4; г) 5; д) 6.

81. Розшифруйте повідомлення $(119827, 100638)$, отримане при зашифруванні за допомогою криптосистеми Ель-Гамаля, відкритий ключ якої $(150607, 2, 16)$, а секретний ключ $a=4$ (алфавіт український).

а) РОМБ; б) КІНО; в) ГЕН; г) ЛАН.

82. Два різних повідомлення M_1 і M_2 зашифровані за допомогою криптосистеми Ель-Гамаля на одному й тому самому ключі (p,g,h). Відповідні шифротексти: $(5,10)$ і $(5,9)$. Якщо при цьому $M_1 = 4$, $p = 17$, то $M_2 = ...$

а) 3; б) 5; в) 7; г)10; д)13.

83. Нехай (p,g,h) – відкриті ключі, a – секретний ключ криптосистеми Ель-Гамаля, результатом зашифрування відкритого повідомлення $M < p$ з рандомізатором r є шифротекст $C = (C_1, C_2)$. Укажіть *перший* етап у доведенні коректності роботи криптосистеми, на якому допущено помилку:

$$D(C) \underset{\uparrow}{=} C_2 (C_1{}^a)^{-1} \bmod p \underset{\uparrow}{=} M^r h (g^{ra})^{-1} \bmod p \underset{\uparrow}{=} M^r h M^{-r+1} h^{-1} \bmod p \underset{\uparrow}{=} M$$

а) б) в) г)

84. Які з наведених алгоритмів дискретного логарифмування у мультиплікативній групі простих скінченних полів мають субекспоненціальну складність?

а) алгоритми «index calculus», що використовують факторну базу;
б) алгоритм Сілвера – Поліга – Хеллмана;
в) алгоритм Шенкса;
г) алгоритм решета числового поля.

85. Які з наведених алгоритмів дискретного логарифмування у мультиплікативній групі простих скінченних полів мають експоненціальну складність?

а) алгоритми index calculus, що використовують факторну базу;
б) алгоритм Сілвера – Поліга – Хеллмана;
в) алгоритм Адлемана;
г) ρ-метод Полларда.

86. Для розв'язку задачі дискретного логарифмування $g^x \equiv h (\bmod n)$ використовується алгоритм Шенкса. Скільки значень міститиме перший список $\{e, g, g^2, ...\}$ за умови, що порядок числа g дорівнює 10000?

а) 10000; б) 10001; в) 101; г) 100; д) 200.

87. Один з важливих кроків при розв'язанні задачі дискретного логарифмування у групі $GF^*(p)$ за допомогою алгоритмів index

calculus – вибір границі гладкості B числа p. Запишіть вигляд функції, що апроксимує значення B.

а) $\exp(const \cdot \sqrt{\log_2 p + \log_2 \log_2 p})$;

б) $\exp(const \cdot \sqrt{\log_2 p} + \log_2 \log_2 p)$;

в) $\exp(const \cdot \sqrt{(\log_2 p) \log_2 \log_2 p})$;

г) $\exp(const \cdot \sqrt{\log_2 \log_2 p})$.

88. Припустимо, що для листування вибрано дві криптосистеми Ель-Гамаля у групі $GF^*(p_1)$ і групі $GF^*(p_2)$, де $p_1 = 48947$ і $p_2 = 15502033$ – прості, $p_1 - 1 = 2 \cdot 24473$, $p_2 - 1 = 2^4 \cdot 3^2 \cdot 7^2 \cdot 13^3$. З погляду на те, що криптоаналітик намагатиметься розв'язати задачу дискретного логарифмування за допомогою алгоритму Сільвера – Поліга – Хеллмана, визначте якій системі логічно надати перевагу.

а) першій, оскільки часова складність алгоритму $O(\sqrt{q})$, де q – найбільший простий дільник модуля;

б) другій, оскільки часова складність алгоритму $O(\sqrt{p})$;

в) жоден алгоритм не має переваг;

г) недостатньо інформації.

89. Часова складність алгоритму решета числового поля для дискретного логарифмування у групі $GF^*(p)$ описується функцією

$$L(p) = 2^{1,992 \cdot (\log_2 p \cdot (\log_2 \log_2 p)^2)^{1/3}}.$$

Скільки операцій потрібно виконати алгоритму, якщо $p \sim 2^{1024}$?

а) 2^{43}; б) 2^{66}; в) 2^{86}; г) 2^{129}; д) 2^{256}.

90. Заповніть порожні клітини таблиці, перший стовпець якої містить перелік задач, важливих для криптографії, другий стовпець – алгоритми їх розв'язання, третій – асимптотичну часову складність алгоритму (залежно від розміру вхідних даних).

Задача	Алгоритм	Асимптотична часова складність
Визначення НСД	???	Поліноміальна
???	Index calculus	???
Факторизація чисел	Квадратичне решето	???

???	Агравала – Каяла – Саксени	???
Дискретне логарифмування у групі точок еліптичної кривої	???	Експоненціальна

91. Алгоритм Діффі – Хеллмана забезпечує:

    а) безумовно безпечний обмін загальним секретом абонентам мережі;
    б) безпечний обмін загальним секретом двом абонентам мережі за умови аутентифікації сторін;
    в) електронний цифровий підпис повідомлень;
    г) надійне зашифрування повідомлень.

92. Навіщо в протоколі Діффі – Хеллмана доцільно передбачати аутентифікацію абонентів?

    а) без аутентифікації можливо зламати задачу дискретного логарифмування;
    б) без аутентифікації можливо зламати задачу факторизації великих чисел;
    в) без аутентифікації супротивник може замінити своїм ключем відкритий ключ одного з абонентів, який той надсилає законному користувачеві;
    г) завдяки аутентифікації неможливо провести атаку на основі «парадоксу днів народження» абонентів.

93. Які з нижченаведених асиметричних шифрів або алгоритмів електронного цифрового підпису використовують операції, подібні тим, що задіяні в протоколі Діффі – Хеллмана?

    а) криптосистема RSA; б) ЕЦП RSA;
    в) криптосистема Ель-Гамаля; г) ЕЦП Ель-Гамаля.

94. За допомогою якого алгоритму можливо розподілити ключі, але неможливо реалізувати стійке шифрування та гарантувати невідмову від авторства?

    а) RSA; б) Діффі – Хеллмана;
    в) ECC (Elliptic Curve Cryptosystem) ; г) Ель-Гамаля.

95. 50 користувачів встановили секретний зв'язок на основі симетричного шифру так, що листування кожних двох недоступне для інших. У скільки разів зменшиться кількість потрібних ключів, якщо вони перейдуть на шифрування за допомогою асиметричної криптосистеми?

    а) у 50; б) у 2450; в) у 24,5; г) у 49; д) у 2500.

96. За протоколом Діффі – Хеллмана розподілу ключів

а) виробляється ключ симетричного шифру;
б) виробляється ключ асиметричного шифру;
в) використовується електронний цифровий підпис;
г) виробляється рандомізатор.

97. Для обміну ключами за схемою Діффі – Хеллмана вибрано скінчене поле $GF(37)$ і первісний корінь $g = 5$ за модулем 37. Які числа розкриваються користувачами, якщо їх закриті ключі $x_A = 4$ і $x_B = 3$?

а) 31 і 12; б) 32 і 13; в) 33 і 14; г) 34 і 15; д) 35 і 16.

98. Для обміну ключами за схемою Діффі – Хеллмана вибрано скінчене поле $GF(37)$ і первісний корінь $g = 2$ за модулем 37. Визначте спільний секретний ключ користувачів, якщо їх закриті ключі $x_A = 15$ і $x_B = 20$.

а) 29; б) 28; в) 27; г) 26; д) 25.

99. Як формулюється задача розкриття експоненційного обміну ключів за протоколом Діффі – Хеллмана?

а) дано: $p, g, a \in N$, де $1 < g < p - 1$. Знайти: x, для якого $a \equiv g^x \bmod p$;

б) дано: $p, g, a, b \in N$, де $1 < g < p - 1$; $a = g^x \bmod p$; $b = g^y \bmod p$. Знайти: $g^{xy} \bmod p$;

в) дано: $p, g, a, b, c \in N$, де $1 < g < p - 1$; $a = g^x \bmod p$; $b = g^y \bmod p$; $c = g^z \bmod p$. З'ясувати, чи виконується рівність $z = xy$;

г) дано: $p, g, x \in N$, де $1 < g < p - 1$. Знайти: $g^x \bmod p$.

100. Яким є спільний секретний ключ, визначений за протоколом відкритого розподілу ключів між трьома абонентів **A**, **B** і **C**, аналогічним протоколу Діффі – Хеллмана для двох абонентів, якщо G – спільна для всіх користувачів скінченна циклічна група, g – її генератор, a, b, c – секретні ключі користувачів **A**, **B** і **C** і відповідно.

а) g^{abc}; б) g^{ab+c}; в) g^{a+b+c}; г) $g^{ab}c$; д) $g^{c}ab$.

101. Нехай g – генератор такої скінченної циклічної групи $GF^*(p)$, в якій значення функції Діффі – Хеллмана $f(g^a, g^b) = g^{ab}$ є важко обчислювальними. Які з нижченаведених функцій також будуть важко обчислювальними?

а) $f(g^a, g^b) = (g^2)^{a+b}$; б) $f(g^a, g^b) = g^{a(b+1)}$;
в) $f(g^a, g^b) = g^{ab+a+b+1}$; г) $f(g^a, g^b) = (\sqrt{g})^{a+b}$.

102. Якщо p – просте, то скільки генераторів є в групі $GF^*(p)$?

а) $(p-1)/2$; б) $\varphi(p)$; в) $\varphi(p-1)$; г) $(p+1)/2$; д) $p-1$.

103. Припустимо, що за протоколом Діффі – Хеллмана, як завжди, користувач **A** вибирає секретний ключ $a \in \{1, 2, ...p-1\}$ і надсилає користувачу **B** значення $X = g^a$. Той, у свою чергу, визначає свій таємний ключ $b \in \{1, 2, ...p-1\}$ та посилає користувачу **A** число $Y = g^{1/b}$. Яким буде спільний ключ та які обчислення вони мають зробити?

	а)	б)	в)	г)
Ключ	$K = g^{ab}$	$K = g^{ab}$	$K = g^{a/b}$	$K = g^{a/b}$
Обчислення користувача **A**	Y^a	$Y^{1/a}$	$Y^{1/a}$	Y^a
Обчислення користувача **B**	X^b	X^b	X^b	$X^{1/b}$

104. Для обміну ключами за схемою Діффі – Хеллмана вибрано скінченну циклічну групу $GF^*(p)$, де p – просте число, і g – твірний елемент. Які рекомендації щодо вибору чисел p і g для реальних умов Ви можете надати?

а) число p слід вибирати так, щоб число $p-1$ мало простий множник $q > 2^{160}$;

б) абонентам слід перевіряти умови: $g^x \not\equiv y \bmod p$ і $g^y \not\equiv x \bmod p$, де x, y – їх секретні ключі;

в) достатньо, щоб число g було твірним елементом підгрупи групи $GF^*(p)$, яка б мала достатньо великий порядок (наприклад, 2^{160});

г) число g обов'язково має бути твірним елементом групи $GF^*(p)$.

105. Проміжні результати $g^x \bmod p$ і $g^y \bmod p$ за протоколом Діффі – Хеллмана використовуються для

а) захисту від атаки «людина посередині»;
б) захисту від атаки відтворення;
в) для забезпечення аутентифікації учасників протоколу;
г) для передачі один одному.

106. У яких алгебраїчних структурах можна використовувати протокол Діффі – Хеллмана?

а) у будь-якій комутативній скінченній групі;
б) у нескінченних групах;
в) у групі перестановок;
г) у групі невироджених квадратних матриць порядку n.

107. Як називається атака, діаграма якої схематично подана на рис. 5.1?

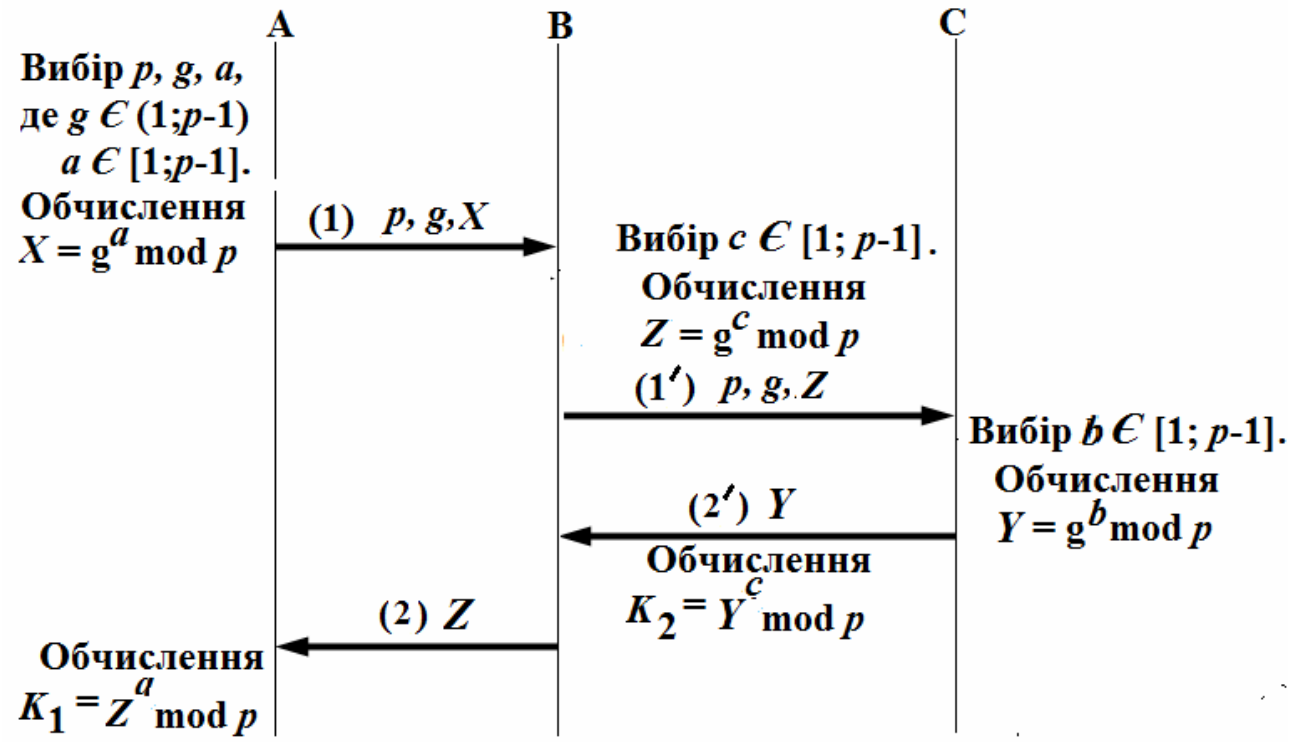


Рис. 5.1

а) атака на основі «парадоксу днів народження»;
б) атака повторенням;
в) атака «зустріч посередині»
г) атака «людина посередині»;
д) атака з повторною передачею повідомлення.

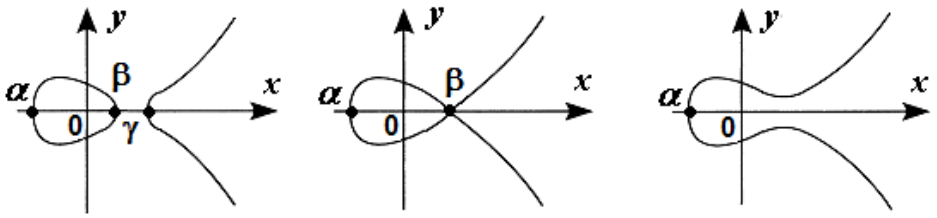
108. Якщо $E_p(a,b)$ – еліптична крива над полем $GF(p)$, характеристика якого $p \neq 2;3$, то рівнянням Вейєрштрасса цієї кривої є

а) $y^2 + y \equiv x^3 + ax + b (\mathrm{mod}\, p)$; б) $y^2 + xy \equiv x^3 + ax^2 + b (\mathrm{mod}\, p)$;
в) $y^2 \equiv x^3 + ax + b (\mathrm{mod}\, p)$; г) $y^2 \equiv x^3 + ax^2 + bx + c (\mathrm{mod}\, p)$.

109. Нехай кубічний многочлен $x^3 + ax + b$ над полем $GF(p)$ розкладено на множники $x^3 + ax + b = (x-\alpha)(x-\beta)(x-\gamma)$, де $\alpha, \beta, \gamma \in GF(p)$. За якої умови дискримінант $D = 4a^3 + 27b^2 (\mathrm{mod}\, p)$ дорівнює нулю?

а) $\alpha = \gamma, \alpha \neq \beta$; б) $\alpha \neq \beta, \alpha \neq \gamma, \beta \neq \gamma$;
в) $\alpha = \beta = \gamma$; г) $D \neq 0$ за жодних умов.

110. Яка з еліптичних кривих, поданих на рис. 5.2, є сингулярною?



а) б) в)

Рис. 5.2

111. Яка з нижченаведених еліптичних кривих $E_p(a,b)$ над полем $GF(p)$ буде несингулярною?

а) $y^2 = x^3 - 35x - 9$ над полем $GF(883)$;
б) $y^2 = x^3 + 41x - 89$ над полем $GF(101)$;
в) $y^2 = x^3 + 28x + 49$ над полем $GF(67)$;

г) $y^2 = x^3 - 22x + 2$ над полем $GF(43)$.

112. У групі точок еліптичної кривої $E_p(a,b)$ над скінченним полем $GF(p)$ груповою операцією є

а) додавання точок; б) інверсія точки;
в) множення точок; г) з'єднання точок.

113. Еліптичній кривій $y^2 = x^3 + 4x + 1$ над полем $GF(7)$ належіть точка

а) $(1,1)$; б) $(2,6)$; в) $(6,3)$; г) $(3,4)$; д) $(4,5)$.

114. Якщо $P = (3,2)$ – точка еліптичної кривої $y^2 = x^3 - 2x - 3$ над полем $GF(7)$, то точка $2P$ має координати

а) $(4,2)$; б) $(2,6)$; в) $(0,5)$; г) $(2,1)$; д) $(3,5)$.

115. Яке з нижченаведених співвідношень щодо точок еліптичної кривої $y^2 = x^3 + 2x + 7$ над $GF(11)$ помилкове?

а) $-(7,1) = (-7,-1)$; б) $-(10,2) = (10,-2)$;
в) $-(7,1) = (7,10)$; г) $-(6,2) = (6,9)$.

116. У якому випадку *правильно* додані точки кривої $y^2 = x^3 + 2x + 7$ над полем $GF(11)$?

а) $(6,2) + (6,9) = O$; б) $(6,2) + O = (6,2)$;
в) $O + O = 2 \cdot O$; г) $(6,2) + (10,2) = O$.

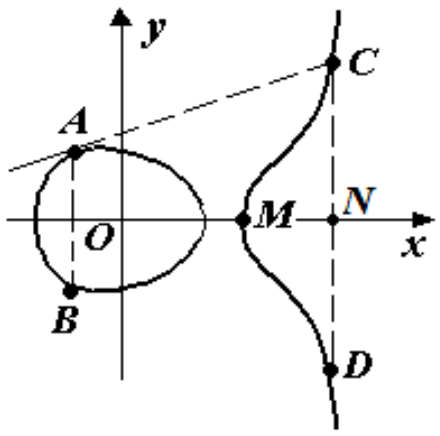


Рис. 5.3

117. Яка з позначених точок еліптичної кривої, зображеної на рис. 5.3, дорівнює точці $2A$?

а) B; б) C;
в) D; г) M;
д) N.

118. Укажіть таку пару чисел a і b, щоб для точок $(5,a)$ і $(5,b)$ еліптичної кривої $y^2 = x^3 + 5x + 2$ над $GF(11)$ справджувалась рівність $(5,a) + (5,b) = O$.

а) $a = -5,\ b = -5$; б) $a = 8,\ b = 3$;
в) $a = 8,\ b = 8$; г) $a = 2,\ b = -2$.

119. Яка з позначених точок еліптичної кривої, зображеної на рис. 5.4, дорівнює точці $R + Q$?

а) M; б) N;
в) P; г) S;
д) T.

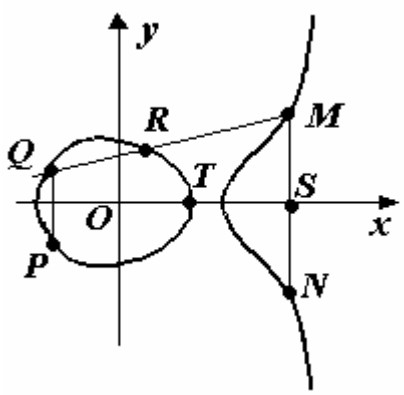


Рис. 5.4

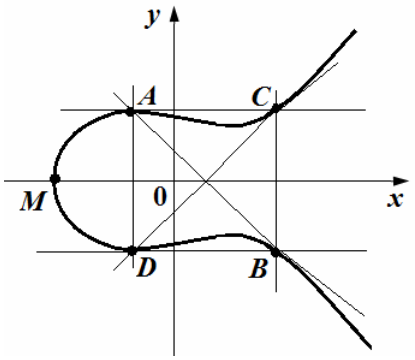


Рис. 5.5

120. За даними рис. 5.5, на якому зображено деяку еліптичну криву, укажіть, які скалярні добутки визначено *неправильно*.

а) $2A = B$; б) $3A = D$; в) $4A = C$;
г) $5A = O$; д) $6A = A$.

121. За даними рис. 5.5, на якому подано деяку еліптичну криву, знайдіть порядок точки A.

а) 2; б) 3; в) 4; г) 5; д) 6.

122. За даними рис. 5.5, на якому подано деяку еліптичну криву, визначте, яка сума точок обчислена *неправильно*.

а) $A + A = B$; б) $B + A = C$;
в) $C + A = O$; г) $D + A = O$.

123. Що називається порядком групи точок еліптичної кривої $E_p(a,b)$ над полем $GF(p)$?

а) кількість точок кривої;

б) число $D = 4a^3 + 27b^2 \bmod p$;

в) найменше натуральне число n, при якому скалярний добуток $nG = G$, де G – генератор групи;

г) сума $a + b$.

124. Наведена на рис. 5.6 діаграма відображає результати скалярного множення точки $P = (3,3)$ еліптичної кривої $y^2 = x^3 + x$ над полем $GF(7)$. За допомогою діаграми знайдіть скалярний добуток $P = 2(5,5)$.

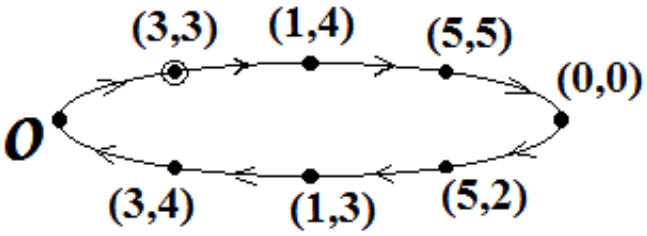


Рис. 5.6

а) $(1,3)$; б) $(5,2)$; в) $(3,4)$; г) O; д) $(1,4)$.

125. При якому значенні C точка $(4,2)$ належіть кривій $y^2 \equiv x^3 + 3x + C (\bmod 7)$?

а) $C = 1$; б) $C = 2$; в) $C = 3$;
г) $C = 4$; д) $C = 5$; е) $C = 6$.

126. Якщо точки P, Q і R еліптичної кривої лежать на одній прямій, заданій рівнянням $y^2 \equiv x^3 + ax + b (\bmod p)$, то

а) $P + Q + R = O$; б) $P + Q = R$;
в) $P = Q + R$; г) $P = Q - R$.

127. Як зв'язані між собою кількість N точок еліптичної кривої $E_p(a,b)$ над полем $GF(p)$ і характеристика p поля?

а) $(\sqrt{p} - 1)^2 \le N \le (\sqrt{p} + 1)^2$;

б) $(\sqrt{p} - a)^2 \le N \le (\sqrt{p} + a)^2$;

в) $(\sqrt{p} - a)^2 \le N \le (\sqrt{p} + b)^2$;

г) $p-\sqrt{ab} \le N \le p+\sqrt{ab}$.

128. Якщо Q – точка еліптичної кривої $E_p(a,b)$ над полем $GF(p)$, то найменше натуральне число n з умовою $nQ=O$ називають

а) порядком кривої;
б) дискримінантом точки;
в) порядком точки;
г) скалярним добутком точки;
д) дискретним логарифмом точки.

129. За умови, що порядок N групи точок еліптичної кривої $E_p(a,b)$ є простим числом, *неправильним* є твердження

а) будь-яка точка еліптичної кривої, крім точки O, є генератором усіх точок кривої;
б) якщо точка $Q \in E_p(a,b)$, то точки $Q,2Q,3Q,...,NQ,O$ складають усю множину точок кривої;
в) через три точки Q, αQ і $-(\alpha+1)Q$, $\alpha = 1,2,...,N$, можна провести одну пряму;
г) $(p-1)^2 \le N \le (p+1)^2$.

130. За допомогою наведених нижче результатів додавання точок еліптичної кривої $y^2 = x^3 + x + 1$ над полем $GF(5)$, визначте порядок точки $(3,1)$.

	$(0,1)$	$(0,4)$	$(2,1)$	$(2,4)$	$(3,1)$	$(3,4)$	$(4,2)$	$(4,3)$	O
$(0,1)$	$(4,2)$	O	$(3,4)$	$(4,3)$	$(2,4)$	$(3,1)$	$(2,1)$	$(0,4)$	$(0,1)$
$(0,4)$	O	$(4,3)$	$(4,2)$	$(3,1)$	$(3,4)$	$(2,1)$	$(0,1)$	$(2,4)$	$(0,4)$
$(2,1)$	$(3,4)$	$(4,2)$	$(2,4)$	O	$(0,4)$	$(4,3)$	$(3,1)$	$(0,1)$	$(2,1)$
$(2,4)$	$(4,3)$	$(3,1)$	O	$(2,1)$	$(4,2)$	$(0,1)$	$(0,4)$	$(3,4)$	$(2,4)$
$(3,1)$	$(2,4)$	$(3,4)$	$(0,4)$	$(4,2)$	$(0,1)$	O	$(4,3)$	$(2,1)$	$(3,1)$
$(3,4)$	$(3,1)$	$(2,1)$	$(4,3)$	$(0,1)$	O	$(0,4)$	$(2,4)$	$(4,2)$	$(3,4)$
$(4,2)$	$(2,1)$	$(0,1)$	$(3,1)$	$(0,4)$	$(4,3)$	$(2,4)$	$(3,4)$	O	$(4,2)$
$(4,3)$	$(0,4)$	$(2,4)$	$(0,1)$	$(3,4)$	$(2,1)$	$(4,2)$	O	$(3,1)$	$(4,3)$
O	$(0,1)$	$(0,4)$	$(2,1)$	$(2,4)$	$(3,1)$	$(3,4)$	$(4,2)$	$(4,3)$	O

а) 2; б)3; в) 4; г) 6; д) 8; е) 9; є) 12.

131. Якщо група E точок еліптичної кривої має порядок 6557, а порядок точки $P \in E$ дорівнює n, то можливі значення n – це

а) $\{1, 79, 83, 6557\}$; б) $\{1, 2, 84, 6556\}$;

в) $\{2, 4, 16, 256, ..., 6144\}$; г) $\{1, 6556\}$.

132. Задача дискретного логарифмування у групі точок еліптичної кривої $E_p(a,b)$ над полем $GF(p)$ формулюється так: за даними точками P і Q кривої знайти число k, для якого

а) $|PQ| = k$; б) $Q + P = (k,k)$;

в) $Q^k = P$; г) $Q = kP$.

133. Яка математична проблема забезпечує стійкість криптосистем, побудованих на еліптичних кривих?

а) визначення точок на кривій, координати яких були б надзвичайно великими числами;

б) пошук на еліптичній кривій точок $P(x, y)$, в яких $x > y$;

в) дискретне логарифмування на еліптичній кривій;

г) пошук двох точок кривої, які мали б однакові абсциси, а їх ординати відрізнялись знаками.

134. Установіть відповідність між параметрами і операціями криптоалгоритмів над простим скінченним полем та на еліптичній кривій.

№	Криптоалгоритм над $GF(p)$	Криптоалгоритм на базі еліптичної кривої над $GF(p)$
I	Група	
II	Групова операція	
III	Обернений елемент	
IV	Піднесення до степеня	

а) додавання точок; б) $E_p(a,b)$; в) Z_p^*;

г) множення точок за модулем, д) g^{-1}, е) $(-P)$;

ж) скалярне множення; з) віднімання точок.

135. Яку мінімальну кількість подвоєнь і додавань точок потрібно виконати, щоб знайти на еліптичній кривій за даною точкою P скалярний добуток $397P$?

а) 4 подвоєння та 8 додавань;
б) 8 подвоєнь та 4 додавання;
в) 198 подвоєнь та одне додавання;
г) 16 подвоєнь та 8 додавань;
д) 8 подвоєнь та 16 додавань;
е) залежіть від рівняння кривої.

136. Для обміну ключами за схемою Діффі – Хеллмана вибрано групу точок еліптичної кривої $y^2 = x^3 + x + 1$ над полем $GF(23)$ і базову точку $P = (0,1)$. $x_A = 9$ і $x_B = 2$ – секретні ключі користувачів. Використавши таблицю скалярного множення точки P, визначте, яким буде спільний секретний ключ за умови, що він збігатиметься з абсцисою згенерованої точки.

$P = (0,1)$	$2P = (6,4)$	$3P = (3,10)$	$4P = (10,7)$
$5P = (5,3)$	$P = 6(7,11)$	$7P = (11,3)$	$8P = (5,4)$
$9P = (4,5)$	$10P = (12,14)$	$11P = (1,7)$	$12P = (6,3)$
$13P = (9,7)$	$14P = (4,10)$	$15P = (9,7)$	$16P = (6,3)$
$17P = (1,7)$	$18P = (12,4)$	$19P = (4,5)$	$20P = (5,4)$
$21P = (11,3)$	$22P = (7,11)$	$23P = (5,3)$	$24P = (10,7)$
$25P = (3,10)$	$26P = (6,4)$	$27P = (0,1)$	$28P = O$

а) 12; б) 11; в) 10; г) 9; д) 7; е) 6; ж) 5; з) 4.

137. Для обміну ключами за схемою Діффі – Хеллмана вибрано групу точок еліптичної кривої $y^2 = x^3 + 5x + 2$ над полем $GF(11)$ і базову точку $P = (2,3)$. За допомогою наведеної таблиці скалярного множення точки P, визначте спільний секретний ключ користувачів за умови, що вони обмінялися точками $(8,2)$ і $(5,3)$.

i	2	3	4	5	6	7	8	9	10
iP	$(8,2)$	$(5,3)$	$(4,8)$	$(3,0)$	$(4,3)$	$(5,8)$	$(8,9)$	$(2,8)$	O

а) $(4,8)$; б) $(3,0)$; в) $(4,3)$; г) $(5,8)$; д)$(8,9)$; е) $(2,8)$.

138. При обміні ключами за схемою Діффі – Хеллмана у групі точок еліптичної кривої у рівнянні $P_A = x_A \cdot G$

а) G – відкритий ключ учасника **А**, пара x_A, P_A – його секретний ключ;

б) P_A – відкритий ключ учасника **А**, G – його секретний ключ;

в) x_A – відкритий ключ учасника **А**, P_A – його секретний ключ;

г) P_A – відкритий ключ учасника **А**, x_A – його секретний ключ.

139. Який асиметричний криптоалгоритм, використовуючи 160-бітовий ключ, має стійкість, близьку до стійкості криптоалгоритму RSA-1024?

а) Ель-Гамаля; б) 3-DES;
в) ECC; г)Шаміра.

140. Серед наведених тверджень щодо криптосистем на еліптичних кривих тільки одне *неправильне.* Яке?

а) довжина повідомлення, поданого у вигляді цілого числа, при зашифруванні за допомогою криптосистеми на еліптичній кривій не може перевищити порядок групи точок еліптичної кривої;

б) у криптосистемах на еліптичних кривих ключ довжиною 512 бітів забезпечує при зашифруванні еквівалентний рівень безпеки тому, що дає криптосистема RSA-512;

в) перевірка електронного цифрового підпису за схемою ECDSA триває приблизно вдвічі довше, ніж його створення;

г) перевірка електронного цифрового підпису за схемою ECDSA триває довше, ніж перевірка підпису за схемою RSA.

141. Нехай порядок N еліптичної кривої E над полем F_q розкладається на множники $N = h \cdot l$, де l – просте. За яких умов таку криву можна використати для побудови еліптичної криптосистеми? Вважайте, що q – велике просте число або великий степінь двійки.

а) $2^{50} \le l \le 2^{150}$;

б) $q^k \not\equiv 1 \bmod l$ при $k = 1, 2, ..., 30$;

в) $l > 2^{160}$;

г) $q^h \equiv 1 \bmod l$; д) $l \ne q$; е) $l = q$.

142. Нехай порядок N еліптичної кривої E над полем F_q розкладається на декілька простих множників. За наведеними довжинами цих

множників укажіть криву, яку доцільну вибрати для побудови еліптичної криптосистеми.

а) 33 біти, 70 бітів; б) 70 бітів, 70 бітів, 70 бітів;
в) 30 бітів, 150 бітів, 70 бітів; г) 3 біти, 200 бітів.

143. Визначте чинники, що ускладнюють застосування криптосистем на еліптичних кривих.

а) реальна стійкість таких систем недостатньо вивчена;
б) ускладнена генерація криптографічно стійких еліптичних кривих;
в) відносно повільна генерація електронного цифрового підпису;
г) відносно повільна верифікація електронного цифрового підпису;
д) наявність субекспоненціальних алгоритмів дискретного логарифмування у групі точок еліптичної кривої

144. Укажіть класи еліптичних кривих над полем $GF(p)$, для яких задачу дискретного логарифмування розв'язати простіше, ніж у загальному випадку.

а) суперсингулярні; б) аномальні; в) ізоморфні; г) несингулярні.

145. Вкажіть шифри із змінною довжиною ключа.

а) RC5; б) лінійний афінний шифр; в) DES;
г) 2DES; д) RSA; е) Віженера.

РОЗДІЛ 6. ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС. КРИПТОГРАФІЧНІ ПРОТОКОЛИ

Задача 1. Нехай H_1 і H_2 – дві хеш-функції, що створюють хеш-образи довжиною n бітів і m бітів відповідно, тобто $H_1 : \{0,1\}^* \to \{0,1\}^n$, $H_2 : \{0,1\}^* \to \{0,1\}^m$. Доведіть, що коли принаймні одна з них стійка до утворення колізій, то хеш-функція $H(x) = H_1(x) \,||\, H_2(x)$ також буде стійкою до колізій. Символ $||$ позначає конкатенацію рядків.

Р о з в' я з а н н я. Без шкоди для загальності міркувань припустимо, що хеш-функція H_1 стійка до колізій, а хеш-функція $H(x) = H_1(x) \,||\, H_2(x)$, навпаки, нестійка. Останнє означає, що існують такі значення $x_0 \neq x_1$, для яких $H(x_0) = H(x_1)$. Звідси

$$H_1(x_0) \,||\, H_2(x_0) = H_1(x_1) \,||\, H_2(x_1)$$

і, зокрема $H_1(x_0) = H_1(x_1)$. Тоді пара x_0, x_1 створює колізію для хеш-функції H_1, що суперечить припущенню. Отже, хеш-функція $H(x) = H_1(x) \,||\, H_2(x)$ також має бути стійкою до колізій.

Задача 2. Нехай $H : \{0,1\}^* \to \{0,1\}^n$ – хеш-функція, стійка до колізій. Чи буде стійкою до колізій хеш-функція $H_1 = H(H(x))$?

Р о з в' я з а н н я. Припустимо, що функція $H_1 = H(H(x))$ не стійка до колізій і відома пара різних значень x_0, x_1, для яких $H(H(x_1)) = H(H(x_2))$. Це означає, що

1) або $H(x_1) = H(x_2)$, що можливо, тільки коли хеш-функція H нестійка до колізій;
2) або $H(x_1) \neq H(x_2)$, тобто пара значень $H(x_1), H(x_2)$ створює колізію для функції H.

Обидва випадки суперечать умові задачі. Отже, хеш-функція $H_1 = H(H(x))$ також стійка до колізій.

Задача 3. (E, D) – симетрична схема шифрування повідомлень, MAC – криптографічна хеш-функція з ключем, $K = (K_1, K_2)$ – спільний секретний ключ користувачів, де ключ K_1 для зашифрування/розшифрування, ключ K_2 для хеш-функції. Припустимо, один з користувачів хоче надіслати іншому деяке повідомлення M так,

щоб забезпечити його конфіденційність, цілісність і достовірність. Оцініть рівень конфіденційності і аутентифікації, що дають наступні протоколи передачі:

1). $M, \mathrm{MAC}_{K_2}(E_{K_1}(M))$; 2). $E_{K_1}(M, \mathrm{MAC}_{K_2}(M))$;

3). $\mathrm{MAC}_{K_2}(E_{K_1}(M))$; 4). $E_{K_1}(M), \mathrm{MAC}_{K_2}(M)$;

5). $E_{K_1}(M), E_{K_1}(\mathrm{MAC}_{K_2}(M))$; 6). $C, \mathrm{MAC}_{K_2}(C)$, де $C=E_{K_1}(M)$.

Р о з в’ я з а н н я.

1). Відсутня конфіденційність, бо повідомлення передається у відкритому вигляді.

2). Конфіденційність і аутентифікація забезпечені, оскільки для зашифрування повідомлення і створення його MAC використана безпечна схема шифрування.

3). Повідомлення не передається, тому це не задовольняє вимоги безпечного каналу зв’язку.

4). Якщо через MAC не буде жодного витоку інформації щодо змісту повідомлення, то така схема передачі безпечна.

5). Завдяки шифруванню повідомлення і його MAC передачу можна вважати конфіденційною, аутентифікацію забезпеченою.

6). Щоб створити легітимний MAC, потрібно знати лише ключ K_2, тому немає впевненості, що відправник знав ключ K_1.

Задача 4. Три криптографічні хеш-функції генерують дайджести довжиною 64, 128 і 160 бітів відповідно. Скільки дайджестів потрібно створити, щоб для кожної функції існували два повідомлення з однаковим значення хеш-функції з імовірністю, більшою ніж: а) $\varepsilon = 0,5$; б) $\varepsilon = 0,1$?

Р о з в’ я з а н н я. Проведемо атаку на основі парадоксу «днів народження». Вимагатимемо, щоб усі шукані повідомлення були близькі за змістом. Для цього добавлятимемо надлишковість до повідомлення або модифікуватимемо його, змінюючи зміст слів, вставляючи додаткові слова або зайві пропуски між словами. Якщо позначити перше повідомлення M, а фіктивне повідомлення M', то задача зводиться до створення двох списків з k повідомлень: перший список – $M=\{M_1, M_2, ..., M_k\}$, другий список – $M'=\{M_1', M_2', ..., M_k'\}$.

Наша мета – знайти у цих списках два повідомлення з однаковими значеннями хеш-функції. Оскільки ймовірність успіху такої події

$$P = 1 - e^{-k^2/n},$$

то накладаємо обмеження $1-e^{-k^2/n} \geq \varepsilon$, звідки $k \geq \sqrt{n \ln \frac{1}{1-\varepsilon}}$. Якщо хеш-функція генерує дайджест довжиною N, то загальна кількість їх можливих значень $n = 2^N$ і тоді $k \geq 2^{N/2} \cdot \sqrt{\ln \frac{1}{1-\varepsilon}}$. Це дає змогу обчислити мінімальну кількість повідомлень, для яких імовірність колізії більша за задане значення ε :

Довжина хешу	n	$\varepsilon = 0,5$	$\varepsilon = 0,1$
64 біти	$n = 2^{64}$	$3,6 \cdot 10^9$	$1,4 \cdot 10^9$
128 бітів	$n = 2^{128}$	$1,5 \cdot 10^{19}$	$6,1 \cdot 10^{18}$
160 бітів	$n = 2^{160}$	$1,5 \cdot 10^{24}$	$3,9 \cdot 10^{23}$

Задача 5. Нехай $E(k,M)$ – рівняння зашифрування блокового шифру (наприклад AES з 128-бітовим ключем), де простір відкритих текстів має такий самий розмір, як і простір ключів. Знайдіть колізію для функції стискання

$$f(x,y) = E(x,x) \oplus y.$$

Р о з в’ я з а н н я. Виберемо два будь-які різні повідомлення x_1 і x_2 та покладемо $y_2 = E(x_1,x_1) \oplus E(x_2,x_2) \oplus y_1$. Тоді

$$f(x_2,y_2) = E(x_2,x_2) \oplus y_2 = E(x_2,x_2) \oplus (E(x_1,x_1) \oplus E(x_2,x_2) \oplus y_1) =$$

$$= E(x_1,x_1) \oplus y_1 = f(x_1,y_1).$$

Задача 6. У стандартному алгоритмі хешування SHA-1 джерелом нелінійності перетворення є нелінійні побітові функції, одна з яких

$$f(x_1,x_2,x_3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3.$$

Обчисліть значення цієї функції для усіх можливих 3-бітових рядків та покажіть, що функція має тільки одну лінійну структуру (лінійна структура булевої функції f від трьох змінних визначається за допомогою вектора $w = (w_1,w_2,w_3) \neq (0,0,0)$, для якого $f(x \oplus w) \oplus f(x)$ є константою).

Р о з в’ я з а н н я. Функція $f(x_1,x_2,x_3)$ задається таблицею

$x_1x_2x_3$	$f(x_1,x_2,x_3)$
000	0
001	0
010	0
011	1
100	0
101	1
110	1
111	1

Тепер знайдемо вектор $w=(w_1,w_2,w_3)\neq(0,0,0)$ функції f, для якої $f(x\oplus w)\oplus f(x)=c$ при всіх можливих вхідних значеннях x. Якщо припустити, що $c=0$, то $f(x\oplus w)=f(x)$.

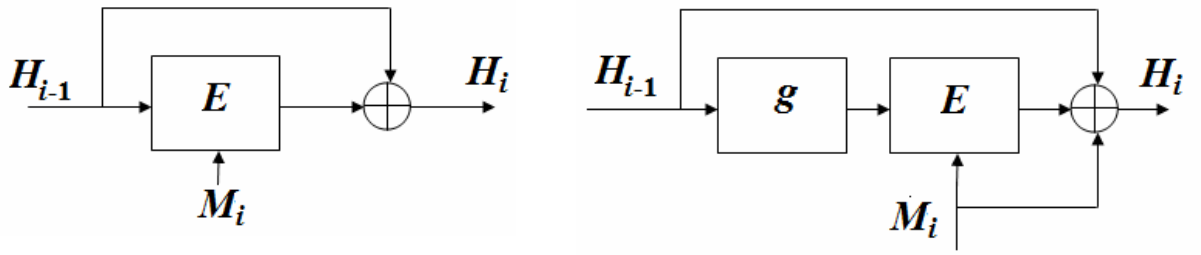
Задача 7. Намалюйте блок-схему для двох хеш-функцій, побудованих на базі блокового шифру E_k з ключем довжини l:

а) $H_i=H_{i-1}\oplus E_{M_i}(H_{i-1})$;

б) $H_i=H_{i-1}\oplus E_{g(H_{i-1})}(M_i)\oplus M_i$,

де M_i – порції відкритого тексту, розмір яких збігається з розміром n блоків, що можна зашифрувати блоковим алгоритмом, H_i – вихід функції хешування після обробки усіх попередніх порцій тексту, g – деяке відображення, що ставить у відповідність вектору довжиною n вектор довжиною n. Чому у першій схемі відсутня функція відображення для формування ключа блокового шифру?

Р о з в’ я з а н н я. Блок-схема хеш-функцій подана на рис.6.1



а) б)

Рис. 6.1

У першій схемі відсутня функція відображення для формування ключа блокового шифру, оскільки там на вхід функції шифрування передаються тільки l бітів відкритого тексту, з яких і формується ключ.

Задача 8. Зашифрування повідомлення M виконується відповідно до рівняння: $C = E_k(M \| H(M))$, де $H(M)$ – хеш-образ повідомлення, E_k – потоковий алгоритм. Покажіть, що така техніка небезпечна, бо якщо криптоаналітик знає увесь відкритий текст M, то у цьому разі він може замінити текст M будь-яким іншим текстом M', підробивши відповідний шифротекст C' так, що отримувач, при верифікації повідомлення визнає його легітимним. Вважайте, що довжини повідомлень M і M' однакові. Чи буде така атака працювати за умови, що контрольна сума обчислюється на основі ключової хеш-функції MAC, тобто $C = E_{k_1}(M \| MAC_{k_2}(M))$?

Р о з в' я з а н н я. Припустимо, що довжина повідомлення M дорівнює n бітів. Спочатку криптоаналітик має обчислити $z_i = m_i \oplus c_i$, де $i = 1,2,..,n$; m_i, c_i – біти відкритого тексту і шифротексту відповідно. Оскільки весь справжній відкритий текст M відомий, то можна отримати хеш-образ $H(M)$ (приймемо, що $h_i(M)$ – i-ий біт хеш-образу, r – його довжина). Відповідно $H(M')$ – хеш-образ іншого повідомлення $M' \neq M$. Далі криптоаналітик визначає:

- $z_{j+n} = h_j(M) \oplus c_{j+n}$, де $j = 1,2,..,r$;
- $c'_i = z_i \oplus m'_i$, де $i = 1,2,..,n$;
- $c'_{j+n} = z_{j+n} \oplus h_j(M')$, де $i = j,2,..,r$.

Тоді біти підробленого шифротексту мають бути генеровані за законом:

$$c'_i = z_i \oplus \{m_1 m_2 ... m_n \| h_1(M) h_2(M) ... h_r(M)\}, \quad i = 1,2,..,n+r.$$

Якщо контрольна сума обчислюється на основі ключової хеш-функції MAC, тобто $C = E_{k_1}(M \| MAC_{k_2}(M))$, то хоча криптоаналітик й може розкрити біти $z_1, z_2, ..., z_n$, він не здатний дізнатися ключовий потік $z_{n+1}, z_{n+2}, ..., z_{n+r}$, що використовується для зашифрування $MAC_{k_2}(M)$. Більш того, навіть дізнавшись про увесь ключовий потік, він не зможе визначити придатний код $MAC_{k_2}(M')$ для іншого повідомлення, поки не отримує ключ k_2.

Задача 9 . Входом хеш-функції є 18-бітовий блок вхідних даних, а виходом – 9-бітовий хеш-образ. Хешування організовано на основі компресійної функції f, що складається з трьох раундів, схожих за структурою на раунди мережі Фейстеля. Вхідний блок розбивається на два півблоки L_0 і R_0. При хешуванні

$$\begin{cases} L_{i+1} = R_i; \\ L_{i+1} = F(R_i) \oplus L_i; \end{cases}$$

$$f(L_0 \| R_0) = R_3 \text{ – хеш-образ;}$$

$$F(b_0,b_1,...,b_8) = S_1(b_0,b_1,b_2) \| S_2(b_3,b_4,b_5) \| S_3(b_6,b_7,b_8).$$

Вихідні біти S-боксів визначаються за таблицями замін:

Вхід	S_1	S_2	S_3
001	001	111	011
001	010	000	001
010	011	001	000
011	100	010	100
100	101	011	010
101	110	100	111
110	111	101	100
111	000	110	010

Знайдіть колізію для значення функції $f(000\,111\,000\,101\,010\,111)$.

Р о з в’ я з а н н я. $\underbrace{000\,111\,000}_{L_0} \| \underbrace{101\,010\,111}_{R_0}.$

$$F(R_0)=F(101\,010\,111)=S_1(101) \| S_2(010) \| S_3(111) = 110 \| 001 \| 010;$$

$$L_1 = F(R_0)= 110001010.$$

Повторивши аналогічні дії у другому і третьому раундах, зобразимо діаграму Фейстеля на рис. 6.2. Остаточно матимемо

$$f(000\,111\,000\,101\,010\,111) = 101000000.$$

З діаграми видно, що біти у позиціях 0, 1 і 2 у хеш-образі залежать тільки від тих бітів відкритого повідомлення, що стоять у позиціях 0, 1, 2, 9, 10 і 11, а біти хеш-образу з позицій 3, 4 і 5 залежать тільки від бітів відкритого повідомлення з позицій 3, 4, 5, 12, 13 і 14, і нарешті на біти з номерами 6, 7 і 8 у хеш-образі впливають лише біти з номерами 6, 7, 8, 15, 16 і 17 (рис. 6.3).

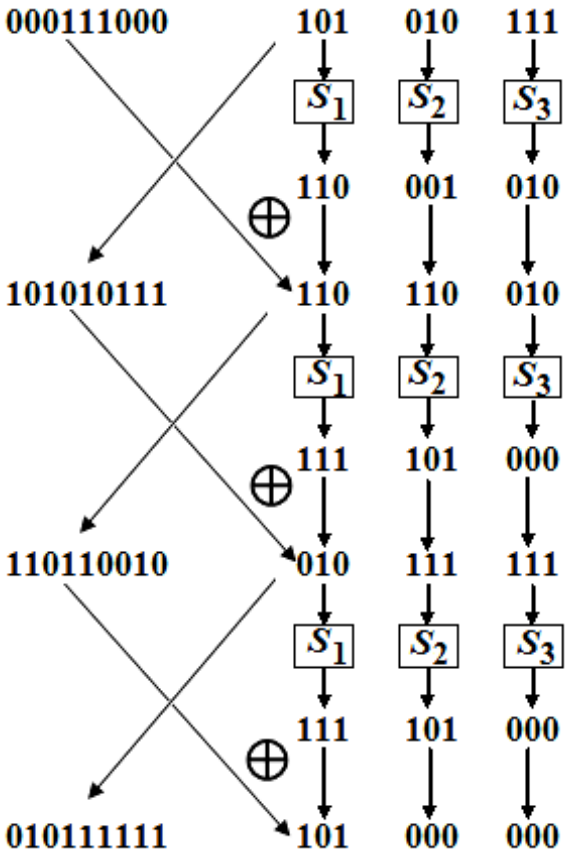


Рис. 6.2

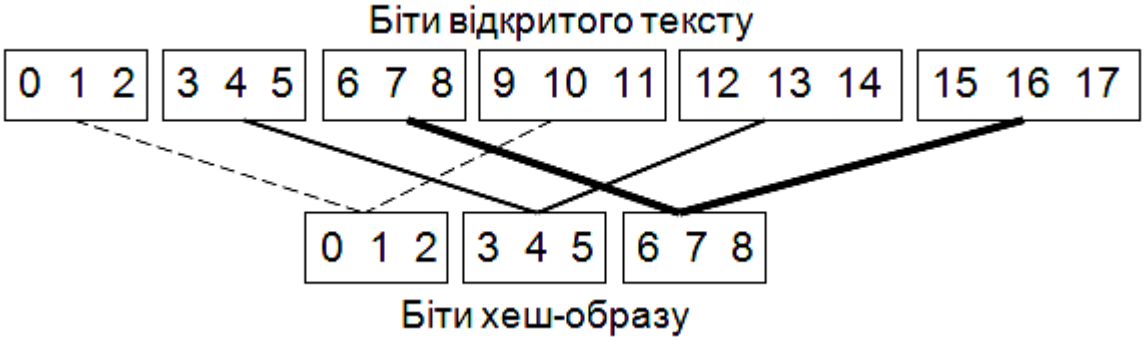


Рис. 6.3

Таким чином, відкритий текст розділяється на три частини, кожна з яких піддається хешуванню окремо. Оскільки за умовою лівий півблок L_3 третього раунду не входить до хеш-образу, а мережа Фейстеля оборотна, то можна застосувати атаку на основі «парадоксу дня народження» тільки до однієї частини тексту. Отже, змінимо перший біт лівого півблоку L_3 на 1 та застосуємо до отриманої бітової послідовності обернене перетворення структури Фейстеля (рис. 6.4).

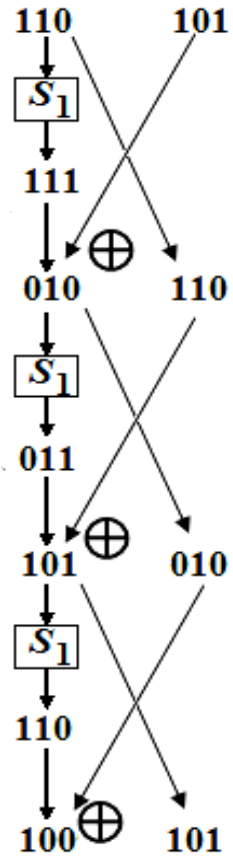


Рис. 6.4

Розрахунки вказують, що входи

$$000\,111\,000\,101\,010\,111$$
$$100\,111\,000\,101\,010\,111$$

створюють колізію заданої хеш-функції.

Задача 10. Фірма з надання послуг цифрового телебачення хоче запобігти крадіжкам у сфері своїх послуг, шифруючи фільми при трансляції за допомогою алгоритму DES. Ключ K_i для шифрування виробляється за допомогою швидкої хеш-функції H на основі ключа K_{AB}, встановленого за схемою Діффі – Хеллмана з простим числом p довжиною 2048 бітів. Ключ K періодично змінюються за законом $K = H(K_{AB} \| i)$, де i – ціле змінне число довжиною 16 бітів. Швидкість передачі даних при телевізійному зв'язку 1 Мбіт/с, тривалість трансляції фільму – 2 години. Припустимо, що зловмисник спроможний знайти ключ DES за 10 хвилин. Як часто має бути змінений ключ K, якщо фірма хоче не допустити офлайн дешифрування фільму не менше ніж протягом місяця?

Р о з в' я з а н н я. Визначимо кількість ключів, які зловмисник може розкрити за один місяць (30 днів):

$$N = \frac{30 \text{ днів}}{10 \text{ хвилин}} = 4320 \text{ кл.}$$

Тоді за дві години трансляції ключ має змінюватися через

$$t = \frac{2 \cdot 3600 \text{ с}}{4320} \approx 1{,}67 \text{ с.}$$

Задача 11. Компанія планує підписати контракт M, використавши систему ЕЦП RSA, причому контракт вступить у силу лише, коли два менеджери компанії незалежно один від одного підпишуть його. Нехай (n, e) – відкриті ключі компанії, d – її секретний ключ, який зберігає секретар компанії. Як має діяти останній, щоб обидва менеджери підписали контракт, не спілкуючись між собою, а підписи були легітимним при верифікації за допомогою відкритого ключа компанії.

Р о з в' я з а н н я. Нехай d_1 – випадкове ціле число з відрізка $[1, n]$ і $d_2 = d - d_1$. Секретар надсилає обом менеджерам контракт M, перший менеджер обчислює значення хеш-функції $H = H(M)$, підносить його до

степеня $H^{d_1} (\mathrm{mod}\, n)$ та надсилає результат секретарю. Другий менеджер аналогічно обчислює значення хеш-функції $H = H(M)$, підносить його до степеня $H^{d_2} (\mathrm{mod}\, n)$ та передає свій результат секретарю. Той перемножує надіслані значення

$$H^{d_1} H^{d_2} (\mathrm{mod}\, n) = H^{d} (\mathrm{mod}\, n) = S$$

та отримує підпис під контрактом. У разі верифікації матимемо $S^e (\mathrm{mod}\, n) = H$.

За такою схемою кожен менеджер не може дізнатися ключа іншого. Якщо відомі значення (n, e) і d_1, перший менеджер не зможе дізнатися d_2 й d із значень $H^{d_2} (\mathrm{mod}\, n)$ або $H^{d} (\mathrm{mod}\, n)$, оскільки вибір числа d_2 випадковий. Отже, він не зможе підписати контракт за другого менеджера у відсутності зговору.

Задача 12. Щоб оцінити час, потрібний для генерації або верифікації електронного цифрового підпису повідомлення, отриманого за допомогою схеми ЕЦП RSA, вважайте, що:

1) комп'ютер працює з 32-бітовими даними, тобто будь-яка змінна зображуються вектором з $m = \lceil l/32 \rceil$ елементів, де l – довжина числа у бітах;

2) одне множення або піднесення до квадрату за модулем двох таких змінних потребує m^2 одиниць часу. За одиницю часу прийміть довжину періоду синхронізації, наприклад $t = 100$ нс;

3) відкрита експонента $e = 2^{16} + 1 = 65537_{10} = 1000000000000001_2$, а довжина закритої експоненти близька до довжини модуля криптосистеми.

Як довго триватиме генерація підпису, якщо довжина модуля дорівнюватиме 512 бітів? На скільки збільшиться цей час, якщо модуль збільшити до 1024 бітів?

Р о з в' я з а н н я. Припустимо, що показник степеня у виразі $x^a \bmod n$ складається з l бітів. Тоді виконання цієї операції в середньому потребує l піднесень до квадрату за модулем і $l/2$ множень, тобто загалом $3l/2$ операцій множення. Ці операції будуть виконані комп'ютером за $3lm^2/2$ одиниць часу або $3 \cdot 100 \cdot lm^2/2$ нс.

Якщо довжина модуля n складає 512 бітів, то $m = \lceil l/32 \rceil = \lceil 512/32 \rceil = 16$. Врахувавши, що під час генерації

електронного підпису за схемою RSA-512 показником степеня слугує закрита експонента, також довжиною 512 бітів, можемо визначити час генерації підпису:

$$T_{\text{генерац.}} = \frac{3 \cdot 100 \cdot l \cdot m^2}{2} = \frac{3 \cdot 100 \cdot 512 \cdot 16^2}{2} \text{нс} \approx 19,7 \text{ мс}.$$

При верифікації підпису користувач підносить хеш повідомлення до степеня e довжиною 16 бітів, виконуючи у цьому разі рівно 17 множень. Отже, у цьому разі час верифікації складає

$$T_{\text{верифік}} = 17 \cdot m^2 \cdot 100 \text{нс} = 17 \cdot 16^2 \cdot 100 \text{нс} \approx 435,2 \text{ мкс}.$$

При збільшенні довжини модуля до 1024 бітів аналогічні розрахунки дають $T_{\text{генерац}} = 157,3$ мс, $T_{\text{верифік}} = 1,741$ мс.

Задача 13. Випадкове повідомлення $M \in Z_n^*$ підписано за схемою електронного цифрового підпису RSA. Відкритий ключ криптосистеми – пара чисел (n,e). Як на основі відомого підпису S цього повідомлення створити легітимний підпис якогось іншого повідомлення $M' \in Z_n^*$?

Р о з в’ я з а н н я. За схемою електронного цифрового підпису RSA підписом повідомлення $M \in Z_n^*$ є $S = M^d \pmod n$. Шукатимемо нове повідомлення у вигляді $M' = 2^e M \bmod n$. Оскільки $ed \equiv 1 (\mod \varphi(n))$, то новий підпис утворюється як

$$S' = (2^e \cdot M)^d \pmod n = 2^{ed} \cdot M^d \pmod n = 2 \cdot M^d \pmod n = 2S \pmod n.$$

Задача 14. Нехай $(n,e) = (1231712773, 1080135473)$ – відкритий ключ криптосистеми RSA деякого банку. Клієнт, вибравши випадкове число $k = 257307676$, хоче, щоб банк підписав відкрите повідомлення $M = 550146327$ у сліпий спосіб (не маючи жодної уяви про зміст повідомлення). Що він має передати банку? Якщо банк відповів йому, надіславши 696569948, то яким є підпис повідомлення?

Р о з в’ я з а н н я. За алгоритмом сліпого підпису у протоколі RSA маскування повідомлення виконується клієнтом і зводиться до обчислення виразу

$$t = M \cdot k^e \bmod n =$$

$$= 550146327 \cdot 257307676^{1080135473} \bmod 1231712773 \equiv 795572137,$$

яке й надсилається до банку.

У разі отримання із банку відповіді $C = 696569948$, підпис повідомлення M визначається як результат зняття маскування:

$$C \cdot k^{-1} \bmod n = 696569948 \cdot 257307676^{-1} \bmod 1231712773 \equiv$$
$$\equiv 696569948 \cdot 1085186384 \bmod 1231712773 \equiv 1000000001.$$

Задача 15. Числа p і g – параметри домену, відкритий ключ абонента у схемі ЕЦП Ель-Гамаля – трійка (p, g, y), його закритий ключ $x \in (1; p-1)$. Припустимо, абонент підписуючи повідомлення M, вибрав рандомізатор r, який збігся з його секретним ключем $x \in (1; p-1)$ (тобто $r = x$) та надіслав іншому абонентові підписане повідомлення $\langle M, a, b \rangle$, $0 < a < p$, $0 < b < p-1$. Як останній зможе розкрити таку схему ЕЦП і визначити закритий ключ та рандомізатор?

Р о з в' я з а н н я. Перевіряючи підпис, можна помітити, що $y \equiv g^x (\bmod p) = g^r (\bmod p) \equiv a$ і зробити висновок $x = r$. Знайдемо r:

$$b = (M - ax) r^{-1} (\bmod p-1) \Rightarrow br = (M - ax) (\bmod p-1) \Rightarrow$$
$$\Rightarrow br + ax = M (\bmod p-1).$$

Оскільки $r = x$, то $r(b+a) = M (\bmod p-1)$. Тоді якщо НСД$(b+a;\ p-1) = 1$, то за узагальненим алгоритмом Евкліда визначимо $(b+a)^{-1} (\bmod p-1)$ і дістанемо $r = M(b+a)^{-1} (\bmod p-1)$.

Задача 16. В алгоритмі ЕЦП за схемою Ель-Гамаля відкритий ключ – трійка $p = 23;\ g = 5;\ y = 17$. Підпис відкритого повідомлення M, хеш-образ якого $H = 3$, складає пара $a = 20,\ b = 21$ (тут $a = g^r (\bmod p)$; $b = (H - ax) r^{-1} (\bmod p-1)$, r – рандомізатор). Припустимо, що отримувач підписаного повідомлення забув про необхідність перевірки умови $a < p$ при верифікації підпису. Як у цьому разі можна підробити електронний підпис для повідомлення M_1 з хеш-образом $H_1 = 7$?

Р о з в' я з а н н я. Знайдемо таке значення u, щоб виконувалось порівняння $H_1 = H \cdot u (\bmod p-1)$:

$$7 = 3u (\bmod 22) \Rightarrow u \equiv 7 \cdot 3^{-1} \equiv 17 (\bmod 22).$$

Позначимо складові підпису повідомлення M_1 як a_1, b_1. Тоді за алгоритмом Ель-Гамаля умова верифікації підпису

$$y^{a_1} a_1^{b_1} \equiv g^{H_1} (\mathrm{mod}\, p).$$

Якщо встановити

$$b_1 = b \cdot u (\mathrm{mod}\, p-1) = 21 \cdot 17 (\mathrm{mod}\, 22) \equiv 5,$$

то значення a_1 визначатиметься з системи порівнянь:

$$\begin{cases} a_1 \equiv a \cdot u (\mathrm{mod}\, p-1), \\ a_1 \equiv a (\mathrm{mod}\, p). \end{cases}$$

Звідси за китайською теоремою про остачі $a_1 = 296 \,\mathrm{mod}\, 506$.

Підпис повідомлення M_1, якому відповідає хеш-значення $H_1 = 7$, утворює пара $a_1 = 296$, $b_1 = 5$, для яких виконується умова верифікації. Таким чином, підпис можна підробити, якщо не контролюються обмеження $a < p$.

Задача 17. ЕЦП за схемою Ель-Гамаля став прикладом для побудови інших схем підписів, схожих за властивостями. У цих схемах p і g – параметри домену, $x \in (1; p-1)$ – секретний ключ особи, що створює підпис, (p, g, y) – відкритий ключ ($y = g^x (\mathrm{mod}\, p)$). Підпис повідомлення M утворює трійка $\langle M, a, b \rangle$, де a обчислюється стандартно $a \equiv g^r (\mathrm{mod}\, p)$, а для визначення b запропоновані інші альтернативні варіанти: а) $b = x^{-1}(M - ra)(\mathrm{mod}\, p-1)$; б) $b = xM + ra (\mathrm{mod}\, p-1)$; в) $b = xa + rM (\mathrm{mod}\, p-1)$. У кожному випадку укажіть умову перевірки правильності підпису.

Р о з в’ я з а н н я. За теоремою Ферма

$$g^{r \,\mathrm{mod}\,(p-1)} (\mathrm{mod}\, p) \equiv g^r (\mathrm{mod}\, p).$$

а) $(g^x)^b a^a (\mathrm{mod}\, p) \equiv (g^x)^{x^{-1}(M-ra)(\mathrm{mod}\, p-1)} (g^r (\mathrm{mod}\, p))^a (\mathrm{mod}\, p) \equiv$

$$\equiv (g^{xx^{-1}(M-ra)(\mathrm{mod}\, p-1)})(\mathrm{mod}\, p) g^{ra} (\mathrm{mod}\, p) \equiv$$

$$\equiv (g^{(M-ra)(\mathrm{mod}\, p-1)})(\mathrm{mod}\, p) g^{ra} (\mathrm{mod}\, p) \equiv g^{(M-ra)} g^{ra} (\mathrm{mod}\, p) \equiv g^M (\mathrm{mod}\, p).$$

Отже, умова верифікації підпису $y^b a^a (\mathrm{mod}\, p) \equiv g^M (\mathrm{mod}\, p)$;

б) $(g^x)^M a^a (\mathrm{mod}\, p) \equiv (g^x)^M (g^r (\mathrm{mod}\, p))^a (\mathrm{mod}\, p) \equiv$

$$\equiv g^{xM+ar} (\mathrm{mod}\, p) \equiv g^b (\mathrm{mod}\, p);$$

умова верифікації підпису $y^M a^a (\mathrm{mod}\, p) \equiv g^b (\mathrm{mod}\, p)$;

в) $(g^x)^a a^M (\mathrm{mod}\, p) \equiv g^{ax} (g^r (\mathrm{mod}\, p))^M (\mathrm{mod}\, p) \equiv$

$$\equiv g^{ax+rM} (\mathrm{mod}\, p) \equiv g^b (\mathrm{mod}\, p).$$

Таким чином, умова верифікації підпису

$$y^a a^M (\mathrm{mod}\, p) \equiv g^b (\mathrm{mod}\, p).$$

Задача 18. Для електронного підпису повідомлень абонент використовує схему Ель-Гамаля з відкритим ключем p, g, y. Він підписав два різних повідомлення M_1 та M_2 і отримав підписи $\langle M_1, a, b_1 \rangle$ і $\langle M_2, a, b_2 \rangle$ (тобто рандомізатор в обох випадках був однаковим). Яким був рандомізатор? Вважайте, що НСД$(r, p-1) = 1$.

Р о з в' я з а н н я. У схемі Ель-Гамаля електронного підпису $a = g^r (\mathrm{mod}\, p)$, $b = r^{-1}(H - ax)(\mathrm{mod}\, p-1)$, де H – дайджест повідомлення, $r \in (1;\ p-1)$ – рандомізатор, $x \in (1;\ p-1)$ – секретний ключ. Якщо повідомленням M_1 і M_2 відповідають дайджести H_1 та H_2, то

$$b_1 = r^{-1}(H_1 - ax)(\mathrm{mod}\, p-1);$$

$$b_2 = r^{-1}(H_2 - ax)(\mathrm{mod}\, p-1);$$

$$b_1 - b_2 = r^{-1}(H_1 - ax) - r^{-1}(H_1 - ax) \bmod (p-1) =$$

$$= r^{-1}(H_1 - H_2) \bmod (p-1).$$

НСД$(r, p-1) = 1 \Rightarrow$ НСД$(b_1 - b_2, p-1) = 1$;

$$\text{НСД}(H_1 - H_2, p-1) = 1.$$

Отже,

$$r = (b_1 - b_2)^{-1}(H_1 - H_2) \bmod (p-1).$$

Задача 19. Одна з операцій в стандарті DSS електронного цифрового підпису – це обчислення виразу $R = (g^k \bmod p) \bmod q$, де

p, q – параметри алгоритму, k – ефемерний ключ. Чи важливий порядок дій при обчисленні цього виразу, тобто чи справджується рівність

$$(g^k \bmod p) \bmod q \equiv (g^k \bmod q) \bmod p ?$$

Р о з в' я з а н н я. $g^k \bmod p \in Z_p^*$, а $g^k \bmod q \in Z_q^*$, тому операції у виразі не комутують. Продемонструємо це числовим прикладом, вибравши параметри $p = 11$ $q = 5$, $g = 3$, $k = 3$.

$$(g^k \bmod p) \bmod q = (3^3 \bmod 11) \bmod 5 \equiv 5 \bmod 5 \equiv 0;$$

$$(g^k \bmod p) \bmod q = (3^3 \bmod 5) \bmod 11 \equiv 2 \bmod 5 \not\equiv 0.$$

Отже, $(g^k \bmod p) \bmod q \not\equiv (g^k \bmod q) \bmod p$.

Задача 20. За стандартом DSS електронним цифровим підписом повідомлення є пара (R, S), де

$$R = (g^k \bmod p) \bmod q,\ S = k^{-1}(H(m) + Ra) \bmod q,$$

p, q, g – доменні параметри, $H(m)$ – дайджест повідомлення m, a – секретний ключ користувача, k – рандомізатор. Покажіть, що: а) значення $S \equiv 0$ дає змогу супротивнику визначити секретний ключ; б) із підпису, в якому $R \equiv 0$, можна визначити використаний рандомізатор та далі створити підпис (з умовою $R \equiv 0$) для будь-якого повідомлення, тобто провести селективну підробку.

Р о з в' я з а н н я. а) З умови $S \equiv 0 \bmod q$ випливає, що $k^{-1}(H(m) + Ra)$ ділиться на q. q – просте, тому на q ділиться або $H(m) + Ra$, або k^{-1}. Друге не можливо, тому приймемо, що $H(m) + Ra \equiv 0 \bmod q$. Оскільки $R \not\equiv 0 \bmod q$, то $a \equiv -H(m) \cdot R^{-1} \bmod q$.

б) Якщо $R = (g^k \bmod p) \bmod q$, то

$$S = k^{-1}(H(m) + 0) \bmod q \equiv k^{-1} H(m) \bmod q.$$

Звідси $k \equiv S^{-1} H(m) \bmod q$. Тепер сфабрикуємо підпис (R', S') іншого повідомлення m' без знання секретного ключа:

$$R' = (g^k \bmod p) \bmod q \equiv 0.$$

$$S = k^{-1}(H(m') + R'a) \bmod q \equiv k^{-1} H(m') \bmod q.$$

Задача 21. Якщо в стандарті DSS електронного цифрового підпису обчислити перший компонент підпису за скороченим виразом $R = g^k \bmod p$ замість $R = (g^k \bmod p) \bmod q$, як передбачено стандартом, то це суттєво збільшить довжину підпису. Як за стандартним коротким підписом обчислити подовжений підпис без знання секретного ключа користувача?

Р о з в' я з а н н я. Нехай за стандартом DSS короткий підпис повідомлення m, дайджест якого $H(m)$, – це

$$R_1 = (g^k \bmod p) \bmod q,\ S_1 = k^{-1}(H(m) + R_1 a) \bmod q,$$

створений з використанням доменних параметрів p, q, g, секретного ключа a і рандомізатора k. Тоді

$$k \equiv S_1^{-1}(H(m) + R_1 a) \bmod q \equiv S_1^{-1} H(m) + S_1^{-1} R_1 a \bmod q = \mu + a \cdot \nu \bmod q,$$

де через μ і ν позначено $S_1^{-1} H(m) \bmod q$ та $S_1^{-1} R_1 a \bmod q$ відповідно. Тепер згенеруємо подовжений підпис повідомлення m – пару (R_2, S_2), врахувавши, що відкритий ключ користувача – це $y = g^a \bmod p$.

$$R_2 = g^{\mu} y^{\nu} \bmod p = g^{\mu} (g^a)^{\nu} \bmod p = g^{\mu + a\nu} \bmod p = g^k \bmod p = R_1;$$

$$S_2 = S_1.$$

Таким чином скорочена формула зменшує довжину підпису, але не надає додаткової стійкості.

Задача 22. Для стандарту DSS електронного цифрового підпису вибрані такі параметри: простий модуль $p = 47$, генератор $g = 2$ порядку 23. Користувач випадково підписав два різних повідомлення на одному й тому самому ефемерному ключі k. Дайджести цих повідомлень $H_1 = 2$ і $H_2 = 3$, а підписи $(4, 21)$ і $(4, 19)$ відповідно. Знайдіть секретний ключ a користувача, не вдаючись до розрахунків дискретного логарифму.

Р о з в' я з а н н я. У стандарті DSS підпис (R, S) складається з обчислень: $R = (g^k \bmod p) \bmod q$; $S = k^{-1}(H + Ra) \bmod q$.

За умовою $(R_1, S_1) = (4, 21)$; $(R_2, S_2) = (4, 19)$. Отже, приходимо до порівнянь: $21 \equiv k^{-1}(2 + 4a)$ і $19 \equiv k^{-1}(3 + 4a)$. Якщо помножимо обидві їх частини на k, то складемо систему порівнянь:

$$\begin{cases} 21k - 4a \equiv 2 \bmod 23, \\ 19k - 4a \equiv 3 \bmod 23. \end{cases}$$

Віднявши порівняння поелементно, дістанемо $2k \equiv -1 \bmod 23$, звідки й визначимо ефемерний $k \equiv 11 \bmod 23$. Тоді $4a \equiv 21 \cdot 11 - 2 \equiv 22 \bmod 23$ і шуканий секретний ключ – це $a \equiv 4^{-1} \cdot 22 \bmod 23 \equiv 6 \cdot 22 \equiv 17 (\bmod 23)$.

Задача 23. Один з варіантів схеми DSS електронного цифрового підпису – це варіант Нюберга – Рюппеля, в якому підпис (R, S) повідомлення M будується так:

$$R = (H \cdot (g^k \bmod p)) \bmod q;$$

$$S = (k - aR) \bmod q,$$

де p – простий модуль, g – генератор порядку q (q – просте число), k – ефемерний ключ, H – хеш повідомлення. Під час генерації абонент повинен перевірити умову $(g^k \bmod p) \bmod q \not\equiv 0$. Покажіть, як із підпису (R, S) на основі доменних параметрів p, q, g і секретного ключа $g^a \bmod p$ можна дізнатися хеш H, $0 < H < q$, повідомлення.

Р о з в’ я з а н н я.

$$H = R \cdot (g^k \bmod p)^{-1} \bmod q \equiv R \cdot (g^{S+aR} \bmod p)^{-1} \bmod q \equiv$$

$$\equiv R \cdot (g^S (g^a)^R \bmod p)^{-1} \bmod q.$$

Задача 24. Для електронного цифрового підпису повідомлень використовується алгоритм ECDSA, крива $E_p(a, b)$ і базова точка G. Секретний ключ – випадкове ціле число d з інтервалу $(0; n)$, відкритий ключ – точка $Q = d \cdot G$. Підпис повідомлення, хеш якого H, складається з пари $(R \equiv x (\bmod n),\ S = k^{-1} (H + d \cdot R) (\bmod n))$, де x – абсциса точки $(x, y) = k \cdot G$, k – випадкове ціле число d з інтервалу $(0; n)$. За алгоритмом ECDSA підпис нелегітимний, якщо $R = 0$ або $S = 0$. Покажіть, що коли таку перевірку було б скасовано і супротивник був би у змозі підібрати число k, при якому абсциса точки $k \cdot G$ була б такою, що дорівнює нулю, то він би зумів підробити підпис для будь-якого повідомлення.

Р о з в’ я з а н н я. Якщо супротивник може визначити число k, при якому абсциса x точки $k \cdot G$ дорівнює нулю, то підпис будь-якого повідомлення, що має хеш H, можна обчислити як

$$(R,\ k^{-1}(H + d \cdot R)(\mathrm{mod}\, n)) = (R,\ k^{-1}H)(\mathrm{mod}\, n)).$$

Такий підпис не залежіть від секретного ключа.

У разі невиконання умови $S \not\equiv 0$, то необхідного для верифікації підпису числа $S^{-1}(\mathrm{mod}\, n)$ не існує.

Задача 25. Нехай у відомій схемі шифрування DHIES з відкритим ключем Z^*_p – підгрупа простого порядку q, p – велике просте число; g – генератор групи (як зазвичай, розміри p і q відповідно 1024 і 160 біт); E – симетричний шифр з ключем довжиною n_1 біт; MAC – функція MAC з ключем довжиною n_2 біт; H – хеш-функція, яка генерує хеш-образи довжиною $n_1 + n_2$ біт. Користувач обирає собі секретний ключ $x < q$ та формує відкритий ключ $X = g^x(\mathrm{mod}\, p)$. Процес шифрування відкритого повідомлення M здійснюються за схемою:

- вибирається випадкове число $y < q$ та визначаються значення
$$Y = g^y \bmod q \text{ і } K = X^y \bmod q;$$
- обчислюється хеш-образ $H(K \| Y)$, який далі подається як
$$k_1 \| k_2;$$
- обчислюються
$$C = E_{k_1}(M) \text{ і } T = MAC_{k_2}(C);$$
- шифротекстом повідомлення вважається $Y \| C \| T$.

Як законний користувач може розшифрувати шифротекст? Яким чином DHIES можна адаптувати до роботи у групі точок еліптичної кривої? Чи матиме це якісь переваги порівняно із наведеною схемою DHIES?

Р о з в’ я з а н н я. Для розшифрування отримувач спочатку має визначити з шифротексту значення Y, C і T. Далі він послідовно знаходить $Y^x = K$, $H(K \| Y) = k_1 \| k_2$ і перевіряє MAC-код:

$T = MAC_{k_2}(C)$. Якщо перевірка засвідчує цілісність шифротексту, то фінальний крок – розшифрування $M = E_{k_1}{}^{-1}(C)$.

Якщо замість підгрупи групи $Z^*{}_p$ вибрати групу точок еліптичної кривої простого порядку q і генератором G, то секретний і ефемерний ключі вибиратимуться так, як і раніше, а модульне піднесення до степеня потрібно замінити на скалярний добуток точок. Значення X, Y, K являтимуть собою точки групи і будуть подані у вигляді координат. Тому це не завадить створити вираз $K \| Y$, який далі й стане аргументом хеш-функції.

Задача 26. У стандарті O'zDST 1092:2005 цифрового підпису Узбекістану (http://pki.uz/downloads/standarts/OzDSt_1092_2009.pdf) уведена спеціальна операція ® множення чисел x і y з параметром R за простим модулем p:

$$x \circledR\ y = x + (1 + xR)y \bmod p.$$

Як можна помножити 100 разів число x само на себе за допомогою операції ® (тобто піднести до 100-го степеня число x), використавши не більше десяти множень і двох додавань за модулем p? Вважайте припустимими попередні обчислення з p і R.

Р о з в' я з а н н я. Усі розрахунки виконуємо за $\bmod p$. За означенням спеціального множення

$$x \circledR\ x = x + (1 + xR)x = 2x + x^2R = [(xR+1)^2 - 1]R^{-1};$$

$$x \circledR\ x \circledR\ x = (2x + x^2R) \circledR x = 2x + x^2R + (1 + 2xR + x^2R^2)x =$$

$$= x^3R^2 + 3x^2R + 3x = [(xR+1)^3 - 1]R^{-1}.$$

Зокрема,

$$\underbrace{x \circledR\ x \circledR \ldots \circledR x}_{\text{100 разів}} = [(xR+1)^{100} - 1]R^{-1}.$$

Очевидно, обчисленню 100-го ступеня числа x передує визначення за розширеним алгоритмом Евкліда оберненого елемента $R^{-1} (\bmod p)$. Усі подальші розрахунки і кількість операцій множення і додавання, які при цьому мають бути виконані, зведені у табл. 6.1.

Таблиця 6.1

Оцінка кількості операцій при обчисленні 100-го ступеня числа

Обчислення	Кількість операцій множення	Кількість операцій додавання
$z = xR + 1$	1	1
$z^2;\quad z^4 = (z^2)^2;\quad z^8 = (z^4)^2;$ $z^{16} = (z^8)^2;\ z^{32} = (z^{16})^2;\quad z^{64} = (z^{32})^2$	0	6
$z^{100} = z^{64} \cdot z^{32} \cdot z^4$	0	2
$[(xR+1)^{100} - 1]R^{-1}$	1	1

Таким чином, потрібно десять множень і два додавання.

Задача 27. Розгляньте наступний протокол відкритого розподілу ключів:

- учасник **A** випадково вибирає два n-бітові рядки k і l, обчислює $m = k \oplus l$ і надсилає m учаснику **B** ;
- учасник **B** також випадково вибирає n-бітовий рядок p, обчислює $t = m \oplus p$ і надсилає t учаснику **A**;
- учасник **A** знаходить значення $r = t \oplus l$ і повертає його учаснику **B**;
- учасник **A** вибирає як ключ рядок k, а учасник **B** – рядок $r \oplus p$.

Чи мають обидва учасники тепер однаковий ключ? Чи є протокол безпечним?

Р о з в’ я з а н н я. Аби упевнитись, що учасники протоколу дійсно розподілили спільний секрет, покажемо, що $r \oplus p = k$:

$$r \oplus p = (t \oplus l) \oplus p = (t \oplus l) \oplus (t \oplus m) = l \oplus m = k.$$

Протокол небезпечний, оскільки нападник може перехопити рядки m, t, r і визначити ключ $k = m \oplus l = m \oplus (r \oplus t)$.

Задача 28. Знайдіть секрет, розділений на частини за $(3,5)$-пороговою схемою Шаміра, якщо частини секрету другого, третього і п’ятого учасників $(2,18)$, $(3,2)$ і $(5,8)$. При розподілі секрету було вибрано поле $GF(23)$.

Р о з в’ я з а н н я. За (t,n)-пороговою схемою розподілу секрету Шаміра частина секрету кожного учасника $\mathbf{A}_i$ протоколу – це пара чисел

(r_i, c_i), $i = 1,2,...,n$, де $c_i = f(r_i)$. Щоб відновити секрет C, використовують інтерполяційну формулу Лагранжа, тобто многочлен $f(x)$ степеня $(t-1)$, який при $x_1, x_2, ..., x_t$ приймає відповідно значення $y_1, y_2, ..., y_t$, визначається за формулою

$$f(x) = \sum_{i=0}^{t-1} y_i \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}.$$

За схемою розподілу секрету многочлен потрібно вибрати так, щоб $f(0) = C$, тому з останнього виразу дістаємо

$$C = \sum_{i=0}^{t-1} c_i S_i, \qquad S_i = \prod_{i \neq j} \frac{r_j}{r_j - r_i}.$$

Отже, відновимо секрет, зібравши частини другого, третього і п'ятого учасників протоколу

$$C = c_2 S_2 + c_3 S_3 + c_5 S_5; \quad c_2 = 18; \quad c_3 = 2; \quad c_5 = 8.$$

$$S_2 = \prod_{i \neq j} \frac{r_j}{r_j - r_2} = \frac{r_3}{r_3 - r_2} \cdot \frac{r_5}{r_5 - r_2} = \frac{3}{3-2} \cdot \frac{5}{5-2} = 3 \cdot 5 \cdot 3^{-1} \equiv 5 \bmod 23;$$

$$S_3 = \frac{r_2}{r_2 - r_3} \cdot \frac{r_5}{r_5 - r_3} = \frac{2}{2-3} \cdot \frac{5}{5-3} = -2 \cdot 5 \cdot 2^{-1} \equiv -5 \bmod 23 \equiv 18 \bmod 23;$$

$$S_5 = \frac{r_2}{r_2 - r_5} \cdot \frac{r_3}{r_3 - r_5} = \frac{2}{2-5} \cdot \frac{3}{3-5} = -2 \cdot 3^{-1} \cdot (-3) \cdot 2^{-1} \bmod 23 \equiv 1 \bmod 23;$$

$$C = c_2 S_2 + c_3 S_3 + c_5 S_5 = 18 \cdot 5 + 2 \cdot 18 + 8 \cdot 1 \equiv 19 \bmod 23.$$

Розподілений секрет – $C = 19$.

Задача 29. Для відновлення секрету, розділеного за схемою Шаміра, чотири людини **А**, **Б**, **В**, **Г** подали свої частини секрету:

$$\textbf{А} \to (1,4); \ \textbf{Б} \to (3,7); \ \textbf{В} \to (5,1); \ \textbf{Г} \to (7,2).$$

Але один з цих людей свою частину секрету вигадав навмання, оскільки використовувалась $(2,3)$-порогова схема Шаміра, коли секрет розподіляють на три частини між трьома учасниками протоколу, а для його відновлення потрібна коаліція будь-яких двох з них. Хто виявився

нечесним і яким був секрет? При розподілі секрету було вибрано поле $GF(11)$.

Р о з в' я з а н н я. За $(2,3)$-пороговою схемою розподілу секрету Шаміра кожен законний учасник отримав пару чисел (r, c), де $c = f(r) = ar + C \bmod p$, де C – розділений секрет, $a = const$. Відновити секрет можна, комбінуючи частини секрету, отримані учасниками **А** і **Б**, або **А** і **В**, або **А** і **Г** , або **Б** і **В**, або **Б** і **Г**, або **В** і **Г**. Отже, складемо відповідні системи порівнянь і розв'яжемо їх.

$$\textbf{А і Б} \rightarrow \begin{cases} a + C = 4 \bmod 11, \\ 3a + C = 7 \bmod 11 \end{cases} \Rightarrow a = 7, C = 8;$$

$$\textbf{Б і В} \rightarrow \begin{cases} 3a + C = 7 \bmod 11, \\ 5a + C = 1 \bmod 11 \end{cases} \Rightarrow a = 8, C = 5;$$

$$\textbf{В і Г} \rightarrow \begin{cases} 5a + C = 1 \bmod 11, \\ 7a + C = 2 \bmod 11 \end{cases} \Rightarrow a = 6, C = 4;$$

$$\textbf{А і Г} \rightarrow \begin{cases} a + C = 4 \bmod 11, \\ 7a + C = 2 \bmod 11 \end{cases} \Rightarrow a = 7, C = 8.$$

Пари **А** і **Б** та **А** і **Г** визначають однаковий секрет $C = 8$, тому учасники **А**, **Б** та **Г** легітимні, секрет вигадав учасник **В**.

Задача 30. Уявіть схему розподілу секрету у вигляді рандомізованого алгоритму, на вхід якого подається секрет у вигляді бітового рядка x довжиною l бітів, а на виході створюється n частин $S_1, S_2, ..., S_n$ секрету. При цьому для відновлення секрету мають бути забрані разом усі n частин, а за допомогою сукупності з $n-1$ або менше частин секрет відновити не можливо. Використавши виключно операцію побітового додавання, розробіть схему, за якою потрібно генерувати частини секрету.

Р о з в' я з а н н я. $x \in \{0,1\}^l$. Виберемо випадково $n-1$ l-бітових рядків $r_1, r_2, ..., r_{n-1} \in \{0,1\}^l$. Тоді частини секрету розподіляться

$$S_1 = r_1; \; S_2 = r_2; \; \ldots \; ; S_{n-1} = r_{n-1};$$

$$S_n = x \oplus r_1 \oplus r_2 \oplus \ldots \oplus r_{n-1}.$$

При такому розподілі $S_1 \oplus S_2 \oplus \ldots \oplus S_n = x$.

ТЕСТИ

1. Криптографічна хеш-функція – це

   а) бієкція; б)ін’єкція; в) сюр’єкція; г) інша відповідь.

2. При збереженні та передачі даних часто застосовують їх стискання. Якщо Ви хочете використати стискання разом з шифруванням, то має сенс

   а) спочатку зашифрувати дані, а потім їх стискати;
   б) порядок шифрування та стискання не має значення;
   в) спочатку стиснути дані, а потім їх зашифрувати;
   г) інша відповідь.

3. Що називають дайджестом повідомлення?

   а) повідомлення, що подається на вхід хеш-функції;
   б) електронно-цифровий підпис повідомлення;
   в) контрольну комбінацію бітів, що дає змогу виявити помилки;
   г) результат обчислення хеш-функції;
   д) шифрований текст.

4. Дайджест вихідного повідомлення використовується для

   а) захисту від несанкціонованої зміни повідомлення;
   б) безпечного обміну ключами;
   в) стискання даних для формування ЕЦП;
   г) таємної передачі повідомлення іншій стороні.

5. У чому полягає суть процесу хешування?

   а) шифрування за допомогою асиметричного алгоритму;
   б) піднесення тексту у вигляді числа у степінь відкритої експоненти;
   в) застосування афінних функцій для шифрування повідомлень;
   г) перетворення вхідного повідомлення довільної довжини у вихідний бітовий рядок фіксованої довжини.

6. Колізія – це…

   а) створення стеганографічною програмою двох зображень, які хоч і мають однаковий вигляд, але в одному прихована таємна інформація;
   б) помилка при хешуванні;
   в) протиріччя у документі;
   г) створення за допомогою хеш-функції для двох різних повідомлень однакового дайджесту;

д) виникнення однакового шифротексту у разі зашифрування одного повідомлення симетричним шифром на двох різних ключах.

7. Яка основна причина виникнення колізій для стійкої хеш-функції?

а) легкість обчислення хеш-образів повідомлень;
б) парадокс «дня народження»;
в) ситуація «людина посередині»;
г) стійкість хеш-функції до першого прообразу.

8. Чому дорівнює ймовірність появи двох однакових знаків у вибірці з t незалежних випадкових знаків n-елементного алфавіту?

а) $1-e^{-a}$, де $0<a\cdot n<C_t^{\,2}$;
б) $1-e^{-nt}$;
в) $1-\sum_{t=1,2} e^{-at}$, де $0<a\cdot n<C_t^{\,2}$
г) $1-e^{-t\sqrt{n}}$.

9. Яка властивість криптографічних хеш-функцій вказана *неправильно*?

а) можливість створювати дайджести повідомлень без ключів;
б) стійкість до виникнення колізій;
в) функціональний зв'язок між аргументами та значеннями функції;
г) взаємно однозначна відповідність між аргументами та значеннями функції;
д) складність визначення аргументу за відомим значенням функції.

10. Які властивості притаманні криптографічним хеш-функціям $H(M)$?

а) для будь-якого значення H_1 хеш-функції неможливо обчислювально ефективно знайти таке повідомлення M, для якого $H_1=H(M)$;
б) для будь-якого повідомлення M неможливо обчислювально ефективно знайти $H(M)$;
в) на вхід хеш-функції можуть подаватися лише блоки даних фіксованої довжини;
г) незалежно від того, яку довжину має вхідне повідомлення M, довжина значення хеш-функції $H(M)$ завжди буде фіксованою;
д) за будь-якої довжини вхідного повідомлення значення хеш-функції обчислюється за поліноміальний час;
е) для будь-якого повідомлення M_1 обчислювально неможливо знайти інше повідомлення M_2, щоб $H(M_1)=H(M_2)$.

11. У чому полягає стійкість функції хешування $H(M)$ до колізій першого роду?

а) для будь-якого хеш-образу H_1 практично неможливо обчислити таке повідомлення M, для якого $H_1 = H(M)$;

б) якщо $H(M_1) = H(M_2)$, то $M_1 = M_2$;

в) довжина хеш-образу має бути фіксованою незалежно від довжини повідомлення;

г) для будь-якого повідомлення M_1 практично неможливо обчислити або підібрати інше повідомлення M_2, для якого $H(M_1) = H(M_2)$.

12. Яку властивість хеш-функції характеризує її стійкість до колізій другого роду?

а) практично неможливо знайти таку пару повідомлень M_1 і M_2, які мали б однакові хеш-образи;

б) якщо хеш-образи одного й того самого повідомлення створені за допомогою різних хеш-функцій, то ці хеш-образи мають збігатися;

в) можливість виправлення помилок при хешуванні;

г) для будь-якого хеш-образу H_1 практично неможливо обчислити таке повідомлення M, для якого $H_1 = H(M)$.

13. Ускладнена стійкість хеш-функцій до колізій означає

а) складність знайти дві хеш-функції, значення яких для певних повідомлень збігаються;

б) складність знайти два різних аргументи, хеш-образи яких однакові;

в) відсутність кореляції між повідомленнями та їх хеш-образами;

г) можливість зміни довжини хеш-образів однієї функції.

14. Нехай криптоаналітик намагається за відомими повідомленням M і його дайджестом $H(M)$ знайти інше повідомлення M', для якого $H(M) = H(M')$. Така постановка задачі характеризує атаку

а) першого прообразу; б) другого прообразу;

в) створення колізії; г) за допомогою грубої сили.

15. Назвіть принцип атаки на електронний цифровий підпис, в основу якої покладено «парадокс днів народження».

а) фабрикується задана кількість повідомлень і їх хеш-образів з метою відшукати однакові хеш-образи;

б) фабрикується задана кількість повідомлень однакової довжини;

в) фабрикується задана кількість хеш-образів для одного повідомлення;
г) фабрикується задана кількість однакових хеш-образів одного повідомлення за допомогою різних хеш-функцій.

16. Хеш-функція створює для повідомлень дайджести фіксованої довжини із m бітів. Як називається атака на хеш-функцію, у ході якої намагаються обчислити $2^{m/2}$ можливих хеш-образів повідомлень з метою знайти однакові?

а) адаптивна атака на основі вибраного відкритого тексту;
б) атака на основі вибраного шифротексту;
в) атака на основі «парадоксу днів народження»;
г) атака «зустріч посередині».

17. Яка ймовірність створити колізію для ідеальної криптографічної хеш-функції, якщо її значення мають довжину 60 бітів?

а) $\frac{30!}{2^{30}}$; б) $\frac{2}{60!}$; в) $\frac{1}{2^{45}}$; г) $\frac{30}{2^{60}}$; д) $\frac{1}{2^{30}}$.

18. За допомогою ідеальної криптографічної хеш-функції $H(x)$ для повідомлень якої завгодно довжини створюється хеш довжини n. Супротивник намагається знайти колізію цієї функції. Як залежить від n кількість спроб, які він має здійснити, щоб досягти мети?

а) $O(2^n)$; б) $O(2^{\sqrt{n}})$; в) $O(2^{n/2})$; г) $O(2^{\log n})$.

19. Функція $H(M)$ – стійка до колізій. Які з нищенаведених функцій також будуть стійкими до колізій? Символ $||$ означає конкатенацію.

а) $H_1(M) = H(0)$; б) $H_2(M) = H(M) \,||\, H(M)$;
в) $H_3(M) = H(H(M))$; г) $H_4(M) = H(M) \oplus H(M)$.

20. Для якої з хеш-функцій H_1, H_2, H_3, H_4 пара повідомлень $M_1 = 000$ і $M_2 = 111$ створюватиме колізію, якщо вихідна хеш-функція $H(M)$ – стійка до колізій? Символ $||$ означає конкатенацію, $|M|$ – довжина повідомлення.

а) $H_1(M) = H(0)$;
б) $H_2(M) = H(|M|)$;
в) $H_3(M) = H(M) \oplus H(M)$;

г) $H_4(M) = H(M[1,2,...,|M|-1])$ (тобто повідомлення без останнього біта).

21. У схемі Меркля – Дамгарда ітеративна функція хешування, основана на

а) побітовому хешуванні;
б) поблоковому хешуванні за допомогою стискання;
в) підстановках;
г) перестановках.

22. При створенні дайджесту повідомлення за схемою Меркля – Дамгарда на i-му кроці ітерації за допомогою однокрокової функції стискання обробляється

а) все повідомлення відразу;
б) результат хешування, отриманий на $(i-1)$-му кроці;
в) результат хешування, отриманий на $(i-1)$-му кроці, та i-ий блок повідомлення;
г) результати хешування, отримані на $(i-1)$-му та $(i-2)$-му кроках;
д) тільки i-ий блок повідомлення.

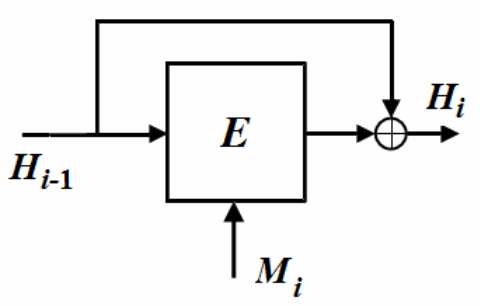


Рис. 6.5

23. Яку з нижченаведених хеш-функцій, побудованих на блоковому шифрі, зображує діаграма на рис. 6.5?

а) $H_i = M_{i-1} \oplus E_{M_i}(H_{i-1})$;
б) $H_i = E_{H_i}(M_{i-1}) \oplus E_{M_i}(H_{i-1})$;
в) $H_i = H_{i-1} \oplus E_{H_i}(M_{i-1})$;
г) $H_i = H_{i-1} \oplus E_{M_i}(H_{i-1})$.

24. Перетворення блока даних за допомогою алгоритму MD5 здійснюється за

а) за 4 раунди; б) за 16 раундів; в) за 64 раунди;
г) кількість раундів залежіть від довжини повідомлення.

25. Навіщо виробники програмного забезпечення при завантаженні його своїм клієнтам через Інтернет публікують хеш-образи програм, отримані за допомогою алгоритму MD5?

а) за допомогою хеш-образів клієнти можуть перевірити справжність сайту, з якого вони завантажили патчі;

б) клієнти можуть у подальшому запитати оновлення програмного забезпечення за допомогою отриманих хеш-образів;
в) хеш-образи потрібні для успішної активації нового програмного забезпечення;
г) клієнти можуть перевірити цілісність програмного забезпечення після завантаження.

26. Що є спільним для алгоритмів хешування MD2, MD4 і MD5?

а) для довільного повідомлення усі алгоритми генерують 160-бітовий хеш-образ;
б) на вхід кожного з них можна подати лише повідомлення довжиною 160 бітів;
в) усі оптимізовані до роботи на комп'ютерах з 32-бітовою архітектурою;
г) усі алгоритми виробляють хеш-образ повідомлення за однакову кількість раундів;
д) у раунді всіх алгоритмів задіяно по чотири логічні функції.

27. Укажіть *правильні* твердження щодо роботи алгоритмів хешування SHA-1 и MD5.

а) якщо алгоритм SHA-1 створює дайджест y повідомлення x, то у разі подачі на вхід алгоритму MD5 повідомлення y на виході отримаємо дайджест x;
б) навіть зміна одного біта у повідомленні, що подається на вхід обох алгоритмів, може спричинити зміну більше 50 % бітів у дайджесті;
в) для обох алгоритмів легко визначити вхідне повідомлення за результуючим дайджестом;
г) існують реальні успішні атаки на криптоалгоритм MD5, за сценарієм яких генеруються пари текстів, що створюють колізію.

28. У скільки разів більше дайджестів повідомлень потрібно створити, щоб знайти колізію хеш-функції SHA-1, ніж у разі підбору колізії хеш-функції MD-4?

а) у 2 рази; б) у 1,5 рази; в) у 1,25 разів;
г) у 4 рази; д) у 5 разів; е) у 10 разів.

29. Які висловлювання щодо хеш-функції SHA-1 є *неправдивими*?

а) якщо після подачі повідомлення x на вхід хеш-функції SHA-1 буде згенеровано дайджест y, то у разі подання на вхід повідомлення y на виході виникає дайджест x;

б) зміна одного біта повідомлення може спричинити зміну більше, ніж одного біта у дайджесті повідомлення, створеного за допомогою SHA-1;
в) довжина дайджесту, створеного за допомогою SHA-1, для будь-якого повідомлення дорівнює 160 бітів;
г) на вхід алгоритму SHA-1 можна подавати тільки повідомлення довжиною 160 бітів;
д) в алгоритмі використовується циклічний код виправлення помилок.

30. Яку кількість бітів міститиме доповнення вихідного повідомлення довжиною 3616 бітів, якщо воно подається для хешування на вхід алгоритму SHA-512?

а) 32; б) 416; в) 480; г) 512; д) інша відповідь.

31. Криптографічна хеш-функція, що реалізується алгоритмом імітозахищеного кодування і призначена для забезпечення неможливості для порушника створювати нові або модифікувати старі повідомлення, називається

а) однобічною хеш-функцією;
б) хеш-функцією з ускладненим виявленням колізій;
в) хеш-функцією, стійкою до виявлення другого прообразу;
г) ключовою хеш-функцією.

32. Навіщо повідомлення передається спільно з його кодоаутентифікацєю (MAC)?

а) для забезпечення конфіденційності повідомлення;
б) для контроля цілісності повідомлення;
в) для забезпечення достовірності повідомлення;
г) для гарантій неможливості у подальшому відмовитися від авторства;
д) для аутентифікації джерела повідомлення.

33. Які активні атаки можна виявити за допомогою MAC повідомлення?

а) зміна повідомлення;
б) видалення повідомлення;
в) вставка додаткового повідомлення;
г) повторення старого повідомлення;
д) зміна порядку передачі двох або більше повідомлень.

34. Алгоритм HMAC – це

а) незалежний від повідомлень алгоритм генерації ключів у синхронних потокових шифрах;
б) алгоритм відкритого розподілу ключів, побудований на складності задачі дискретного логарифмування;
в) алгоритм, який комбінує безключову хеш-функцію та секретний ключ і забезпечує цілісність, істинність та неможливість повторного використання повідомлень;
г) високий рівень доступу до секретного тексту;
д) MAC коди, побудовані із застосуванням блокового шифру.

35. З якою метою було розроблено алгоритм HMAC?

а) щоб зробити швидкість роботи алгоритму близькою до швидкості роботи відповідної хеш-функції;
б) щоб мати можливість стиснути повідомлення без втрати інформації;
в) заради можливості використання секретних ключів та простоти роботи з ними;
г) щоб гарантувати аутентичність повідомлення та джерела двом сторонам, що не довіряють одна одній.

36. Для побудови HMAC повідомлення M використано алгоритм хешування SHA-1:

$$HMAC(K,M) = SHA_1\left[(K \oplus opad) \,||\, (K \oplus ipad) \,||\, M\right],$$

де $ipad$ і $opad$ – блоки виду $0x3636...36$ та $0x5c5c...5c$ відповідно. Які попередні розрахунки можна виконати заради прискорення обчислення HMAC, якщо секретний ключ K фіксований?

а) ітерації блоків $K^+ \oplus ipad$;

б) ітерації блоків $K^+ \oplus opad$;

в) обчислення дайджесту повідомлення;
г) $(K \oplus ipad) \,||\, M$ і $(K \oplus opad) \,||\, M$.

37. За стандартом HMAC на відміну від стандарту MAC повідомлення

а) шифрують;
б) розбивають на блоки та, за необхідністю, доповнюють до потрібної довжини;
в) доповнюють контрольною сумою;
г) розбивають на блоки та кодують.

38. Яке з тверджень щодо HMAC *правильне*?

а) для побудови HMAC використовується RSA хеш-функція;

б) для побудови HMAC повідомлення використовується секретний ключ, відомий лише відправнику;
в) HMAC використовують в протоколах SSL і TLS, щоб забезпечити конфіденційність обміну інформацією;
г) це MAC коди, побудовані на основі безключових швидких хеш-функцій і секретного ключа.

39. На відміну від коду виявлення помилок (MDC) у коді аутентифікації повідомлення (MAC) використовують

а) хеш-функцію; б) секретний ключ;
в) несекретний канал; г) перестановки.

40. З погляду на те, що код MAC та ЕЦП призначені для аутентифікації повідомлень, визначте, яке твердження *правильно* описує їх відмінність.

а) код MAC можна перевірити тільки, знаючи повідомлення, а для верифікації ЕЦП потрібен секретний ключ абонента, що підписав повідомлення;
б) код MAC можна перевірити без секретного ключа, а для верифікації ЕЦП потрібен відкритий ключ абонента, що підписав повідомлення;
в) код MAC можна отримати за допомогою секретного ключа, а для верифікації ЕЦП достатньо отримати сертифікат секретного ключа;
г) код MAC можна отримати за допомогою секретного ключа, використаного для його генерації, а верифікувати ЕЦП можна за відомим відкритим ключем абонента, що підписав повідомлення.

41. Якщо на стороні відправника приєднати до повідомлення його хеш, зашифрований за допомогою симетричного алгоритму з секретним ключем, то це еквівалентно

а) створенню електронного цифрового підпису;
б) забезпеченню таємності передачі повідомлення;
в) генеруванню однобічної функції;
г) створенню кода аутентифікації повідомлення MAC.

42. Які з нижченаведених алгоритмів хешування застосовують при високошвидкісних обчисленнях?

а) MD4; б) MAC; в) SHA-1;
г)RSA; д) RSA-OAEP; е) WHIRLPOOL.

43. Якої властивості не має в електронного цифрового підпису повідомлення?

    а) гарантування достовірності;
    б) непідробленості;
    в) неможливості повторного використання;
    г) підтвердження цілісності документу;
    д) ЕЦП не змінюється при зміні тексту документа;
    е) кожна копія документа повинна підписуватися окремо.

44. У разі придбання покупцем товару на сайті електронної комерції останній повинен надати докази того, що купівля дійсно відбулася між сайтом і покупцем. Якщо для цього задіяти електронний цифровий підпис, то найбільш важливо, що за його допомогою можна гарантувати

    а) справжність цифрового підпису;
    в) цілісність даних з цифровим підписом;
    б) справжність зобов'язень щодо торгової угоди;
    г) конфіденційність відкритих ключів.

45. При генерації ЕЦП повідомлення його дайджест шифрується за допомогою

    а) відкритого ключа відправника;
    б) секретного ключа відправника;
    в) відкритого ключа отримувача;
    г) секретного ключа отримувача.

46. Чому шифротекст повідомлення, отриманий за допомогою симетричного шифру з використанням спільного секретного ключа користувачів, не може замінити електронний підпис повідомлення?

    а) третя сторона (арбітр) не зможе дізнатися, хто з двох користувачів підписав повідомлення, і розв'язувати спори щодо істинності підпису;
    б) третя сторона (арбітр) не зможе бути впевненою, що хтось інший не викрав закритий ключ;
    в) симетрій шифр не гарантує, що протягом достатньо довгого терміну такий електронний цифровий підпис неможливо підробити;
    г) секретний ключ має бути відкритий третій стороні (арбітру) для перевірки підпису.

47. Якщо Ви вважайте, що дехто замінив надіслане Вам захищене повідомлення, то якою буде Ваша дія щодо з'ясування правди?

а) перевірка теми повідомлення;
б) перевірка часу і дати отримання шифротексту;
в) перевірка цифрового підпису повідомлення;
г) звернення до центру сертифікації з метою припинити дію сертифікату Вашого відкритого ключа.

48. Поставте у відповідність поняття та терміни, які найбільш тісно зв'язані з між собою.

1) водяні знаки;	а) гарантування джерела цифрових даних;
2) електронний цифровий підпис;	б) виявлення несанкціонованого доступу до копії електронного документа;
3) комбінація криптоалгоритмів з відкритим і симетричним ключами для розподілу ключів;	в) шифрування;
4) перетворення відкритої інформації у закриту для передачі її відкритою мережею;	г) цифровий електронний конверт.

49. У разі потреби в криптографічному механізмі, що забезпечить цілісність і автентичність Вашого повідомлення, Ви виберете

а) стеганографію; б) хешування;
в) протокол Kerberos; г) цифровий підпис.

50. Яка послідовність підпису повідомлень за допомогою ЕЦП?

а) спочатку обчислюють хеш повідомлення і далі хеш підписують;
б) повідомлення спочатку шифрують, піддають хешуванню і далі підписують;
в) при створенні підпису повідомлення шифрують, а під час верифікації підпису обчислюють хеш повідомлення;
г) обчислюють хеш повідомлення, шифрують його і далі підписують.

51. Наведіть наступні чотири дії в порядку, за яким Ви зможете створити, а дехто потім перевірити Ваш електронний цифровий підпис.

1 – шифрування хеша повідомлення за допомогою секретного ключа;
2 – порівняння надісланого хеша із створеним хешем повідомлення;
3 – створення хеша повідомлення;

4 – розшифрування підпису за допомогою Вашого відкритого ключа.

а) 4,2,1,3; б) 1,4,3,2; в) 3,1,4,2; г) 3,4,2,1.

52. Поставте у відповідність тип підробки електронного цифрового підпису і механізм її здійснення. Вважайте, що супротивник не володіє секретним ключом для підпису, але знає відкритий ключ відправника.

Підробка	Дії супротивника
I – селективна; II – екзистенціальна; III – універсальна	а) супротивник розробляє алгоритм, функціонально еквівалентний алгоритму ЕЦП; б) супротивник для даного повідомлення підробляє підпис; в) супротивник створює пару «повідомлення – підпис», що приймається алгоритмом верифікації.

53. Що з наступного є перевагою схеми ЕЦП на основі криптосистеми RSA над ЕЦП за стандартом DSS?

а) у схемі ЕЦП на основі RSA підписується не саме повідомлення, а його хеш, а в стандарті DSS цього непередбачено;
б) підпис на основі криптосистеми RSA не піддається екзистенціальній підробці;
в) на відміну від криптоалгоритму DSA криптоалгоритм RSA також можна задіяти для шифрування;
г) розмір підпису на основі RSA зазвичай коротший, ніж за стандартом DSS.

54. (n,e) – відкритий ключ користувача криптосистеми RSA, d – секретний ключ. При підписанні довгих повідомлень $M > n$ він створює підпис $(M \bmod n)^d \bmod n$. Які з нижченаведених тверджень будуть *правильними*?

а) при підписанні повідомлень за допомогою ЕЦП RSA існують обмеження на довжину повідомлення;
б) повідомлення M і $M \bmod n$ матимуть різні підписи;
в) при такій організації підпису легко генерувати різні повідомлення, що матимуть однаковий електронний підпис;
г) при підписанні довгих повідомлень $M > n$ потрібно збільшити відкриту експоненту.

55. Якщо абонент, який користується криптосистемою RSA з модулем $n = 55$ та відкритою експонентою $e = 3$, підпише деяке повідомлення, дайджест якого $H(M) = 2$, то для перевірки підпису він має надіслати іншому абоненту

а) $\langle M, 23 \rangle$; б) $\langle H(M), 29 \rangle$; в) $\langle M, 11 \rangle$;
г) $\langle M, 18 \rangle$; д) $\langle H(M), 19 \rangle$; е) інша відповідь.

56. Порівняйте час виконання операцій з відкритим та секретним ключами в криптоалгоритмі RSA та ЕЦП RSA.

а) шифрування тексту триває довше, ніж дешифрування;
б) розшифрування тексту триває довше, ніж шифрування;
в) генерація підпису триває довше, ніж його перевірка;
г) перевірка підпису триває довше, ніж його генерація.

57. S_1 і S_2 – електронні підписи повідомлень m_1 і m_2 відповідно, створені за допомогою алгоритму RSA. Як створити електронний підпис повідомлення $m_1{}^j \cdot m_2{}^k$, де j і k – додатні цілі значення, якщо відомі лише модуль n і відкрита експонента e криптосистеми?

а) $(S_1{}^j \cdot S_2{}^k)^e (\mathrm{mod}\, n)$; б) $S_1{}^j \cdot S_2{}^k (\mathrm{mod}\, n)$;
в) $S_1{}^k \cdot S_2{}^j (\mathrm{mod}\, n)$; г) $(S_1 \cdot S_2)^{(k+j)e} (\mathrm{mod}\, n)$.

58. Порівняйте особливості схеми ЕЦП на основі криптосистеми RSA і криптосистеми Ель-Гамаля. Виберіть *неправильне* твердження.

а) підпис, отриманий за схемою Ель-Гамаля, має дві компоненти, а за схемою RSA – одну;
б) у схемі ЕЦП на основі криптосистеми Ель-Гамаля складність обчислення підпису і його верифікакації однакова;
в) у схемі ЕЦП на основі криптосистеми RSA процес створення підпису повідомлення триває довше, ніж його перевірка;
г) генерація цифрового підпису за схемою Ель-Гамаля – це рандомізований алгоритм, а за схемою RSA – детермінований.

59. Яка умова верифікації електронного цифрового підпису $\langle M, R, S \rangle$ за схемою Ель-Гамаля, якщо доменні параметри p і g, відкритий ключ абонента y, дайджест повідомлення H?

а) $y^R \cdot g^S \equiv R^H \bmod p$; б) $g^{R+H} \equiv y^S \bmod p$;

в) $y^S \cdot S^R \equiv g^H \bmod p$; г) $y^R \cdot R^S \equiv g^H \bmod p$.

60. Укажіть усі умови, за яких порушується стійкість ЕЦП на основі криптосистеми Ель-Гамаля. Вважайте, що (p,g,y)– відкриті параметри криптосистеми, $\langle M,R,S\rangle$ – електронний цифровий підпис.

а) $R > p$; б) $p-1 > S$;
в) параметр g кратний R;
г) $R = g$; д) $S = y$
е) багаторазове використання ефемерного ключа.

61. $p=17$, $g=3$ – доменні параметри криптосистеми Ель-Гамаля, $y=5$ – відкритий ключ абонента, $x=5$ – його секретний ключ. Вибравши рандомізатор $r=7$, він підписав повідомленням M, дайджест якого $H=9$. Яким є цей підпис?

а)$\langle M,8,11\rangle$; б)$\langle M,9,12\rangle$; в)$\langle M,10,13\rangle$;
г) $\langle M,11,14\rangle$; д) $\langle M,12,15\rangle$; е) інш відповідь.

62. Схема Ель-Гамаля електронного цифрового підпису $\langle M,R,S\rangle$ стала взірцем для побудови цілої сім'ї багато в чому схожих за своїми властивостями інших схем підпису. У них підпис верифікується за допомогою перевірки умови $g^A y^B \equiv R^C (\bmod p)$, де трійка (A,B,C) збігається з однією з перестановок чисел $\pm H, \pm R, \pm S$ при певному виборі знаків, H – хеш повідомлення, y– відкритий ключ абонента. Якими є значення (A,B,C) для американського стандарту DSS електронного цифрового підпису?

а) $A=H$, $B=R$, $C=S$; б) $A=-H$, $B=S$, $C=R$;
в) $A=H$, $B=-R$, $C=S$; г) $A=H$, $B=-S$, $C=R$.

63. До основних недоліків схеми ЕЦП на основі криптосистеми Ель-Гамаля відносять

а) повільну швидкість, особливо при підписанні;
б) необхідність змінювати секретний ключ після кожного підписання документу;
в) детермінований тип алгоритму ЕЦП;
г) значну довжину підпису.

64. Який алгоритм лежить в основі алгоритму DSA ЕЦП?

а) RSA; б) Ель-Гамаля; в) DES; г) Діффі – Хеллмана.

65. Який з нижченаведених варіантів описує в алгоритмі DSA основні операції на стадії підписання повідомлення? Вважайте, що довжина повідомлення менша за 2^{64} бітів.

а) повідомлення подається на вхід алгоритму DSA і далі створений 160-бітовий хеш повідомлення передається на вхід алгоритму SHA, який генерує ЕЦП повідомлення;
б) повідомлення подається на вхід алгоритму SHA і далі створений 128-бітовий хеш повідомлення подається на вхід DSA, який генерує ЕЦП повідомлення;
в) повідомлення подається на вхід алгоритму SHA і далі отриманий 160-бітовий хеш повідомлення використовується як ЕЦП повідомлення;
г) повідомлення подається на вхід SHA і далі згенерований 160-бітовий хеш повідомлення передається на вхід алгоритму DSA, який генерує ЕЦП повідомлення.

66. Які з відкритих параметрів (p,q,g,y) алгоритму DSA можуть бути спільними для кількох користувачів одночасно?

а) p; б) q; в) g; г) y.

67. Числа (p,q,g,y) – відкриті параметри алгоритму DSA, число a – секретний ключ, $\langle M,R,S\rangle$ – електронний цифровий підпис, де $S=(H+aR)k^{-1} \bmod q$, H – дайджест повідомлення. Якщо замінити останнє рівняння на $S=(Ha-R)k^{-1} \bmod q$, то якою стане умова верифікації підпису?

а) $R=(y^{SH^{-1}} g^{-SR^{-1}} \bmod p) \bmod q$;
б) $R=(y^{SH} g^{-SR} \bmod p) \bmod q$;
в) $R=(y^{S^{-1}H} g^{-S^{-1}R} \bmod p) \bmod q$;
г) залишиться без змін.

68. Як на практиці можна прискорити реальну генерацію алгоритмом DSA електронного цифрового підпису $\langle M,R,S\rangle$ повідомлення M (без втрати стійкості)?

а) при різних випадкових значеннях ефемерного ключа k виконати попередні обчислення першої компоненти R підпису;

б) при різних випадкових значеннях ефемерного ключа k виконати попередні обчислення другої компоненти S підпису;

в) заздалегідь визначити обернені значення $k^{-1} \bmod q$ для різних випадкових ефемерних ключів;

г) зменшити доменний параметр q до 80 бітів;

д) змінити порядок зведення за модулями чисел p і q при обчисленні першої компоненти R підпису.

69. Порівняйте переваги алгоритмів DSA і Ель-Гамаля електронного цифрового підпису.

а) довжина підпису у 320 бітів, отриманого за алгоритмом DSA, набагато коротша за довжину підпису за схемою Ель-Гамаля;

б) робота алгоритму DSA потребує більшого об'єму пам'яті, ніж робота алгоритму Ель-Гамаля;

в) час обчислення підпису за алгоритмом DSA менший, ніж за алгоритмом Ель-Гамаля;

г) на відміну від алгоритму Ель-Гамаля в алгоритмі DSA параметр p стає спільним для групи користувачів, що послабляє стійкість алгоритму.

70. За американським стандартом DSS електронний цифровий підпис може бути сформовано усіма наведеними нижче алгоритмами за винятком

а) ECDSA; б) AES; в) RSA; г) DSA.

71. Стійкість алгоритму ECDSA основана на складності проблеми

а) факторизації великих чисел за допомогою еліптичної кривої;
б) дискретного логарифмування у скінченному полі;
в) дискретного логарифмування у групі точок еліптичної кривої;
г) перевірних матриць лінійних кодів.

72. Не існує[1] субекспоненційного алгоритму для розв'язання задачі

а) факторизації великих чисел;
б) факторизації великих чисел за допомогою еліптичної кривої;
в) дискретного логарифмування у скінченному полі;
г) дискретного логарифмування у групі точок еліптичної кривої.

73. Що є спільного в алгоритмах ECDSA і DSA?

[1] На момент видання посібника

а) в обох алгоритмах легко згенерувати системні параметри;
б) обидва підписи коротші, ніж підпис за схемою RSA;
в) друга компонента S підпису $\langle R,S\rangle$ в обох алгоритмах обчислюється за рівняннями, що мають однакову структуру;
г) генерування підписів за допомогою кожного алгоритму триває довше, ніж його верифікація.

74. Які відмінності між алгоритмами ECDSA і DSA Ви можете назвати?

а) алгоритм DSA базується на схемі електронного підпису Ель-Гамаля, а алгоритм ECDSA – на схемі підпису RSA;
б) алгоритм DSA використовує для хешування алгоритм SHA-1, а алгоритм ECDSA – алгоритм SHA-2;
в) алгоритм DSA використовує підгрупу порядку q групи $GF^*(p)$, а алгоритм ECDSA – групу точок еліптичної кривої над полем $GF(p)$;
г) різна кількість зведень за модулем при обчисленні першої компоненти R підпису $\langle R,S\rangle$.

75. Назвіть довжину ключа алгоритму ECDSA, при якому забезпечується рівень захисту, еквівалентний рівню, що дає алгоритм DSA з ключем довжиною 1024 бітів.

а) 2048 бітів; б) 512 бітів; в) 320 бітів; г) 160 бітів; д) 80 бітів.

76. Користувач підписав повідомлення M з хешем $H=4$ за стандартом ECDSS електронного цифрового підпису з алгоритмом ECDSA, вибравши еліптичну криву $y^2=x^3+2x+9$ над полем $GF(13)$ і базову точку $G=(1,8)$ порядку 17. За умови, що закритий ключ користувача $d=5$, рандомізатор $k=2$, цей підпис

а) $\langle M,10,7\rangle$; б) $\langle M,9,6\rangle$; в) $\langle M,8,5\rangle$; г) $\langle M,7,4\rangle$; д) $\langle M,6,3\rangle$.

77. Українським стандартом електронного цифрового підпису є

а) DSS;
б) ГОСТ Р 34.10-2001;
в) СТБ 1176.2-99;
г) ДСТУ 4145-2002.

78. Що може надати можливість абонентам мережі упевнитися, що особи або організації, від яких вони отримують шифровані повідомлення, дійсно є тими, за кого вони себе видають?

а) хеш-образи повідомлень;
б) біометричні підписи;

в) симетричне шифрування; г) сертифікати ключів.

79. Яку з організацій чи установ можна визначити як нейтральну, що засвідчує цифрові сертифікати ключів?

а)центр сертифікації (СА); б) центр затвердження ключів;
в) зона авторизації; г) парольна установа.

80. Який з наведених принципів ***не*** покладено в основу створення інфраструктури відкритих ключів (РКІ)?

а) секретний ключ відомий лише користувачу;
б) центр сертифікації створює сертифікат відкритого ключа;
в) усі користувачі довіряють один одному і центру сертифікації;
г) центр сертифікації підтверджує або спростовує належність відкритого ключа користувачу, який має відповідний секретний ключ.

81. Задачі, що вирішує інфраструктура РКІ, – це

а) забезпечення конфіденційності та цілісності інформації;
б) забезпечення аутентифікації користувачів;
в) забезпечення захисту від DDoS атак;
г) забезпечення можливості підтвердження дій, скоєних користувачами з інформацією;
д) авторизація суб’єктів.

82. В умовах децентралізації керування ключами, користувач відповідає за створення

а) цифрового сертифікату відкритого ключа;
б) списку анульованих сертифікатів відкритих ключів;
в) відкритого і секретного ключів для асиметричного шифрування;
г) анулювання цифрового сертифікату відкритого ключа.

83. Назвіть серед нижченаведеного дві компоненти інфраструктури відкритих ключів.

а) паспорти користувачів; б) цифрові сертифікати;
в) зашифровані дані; г) центр сертифікації.

84. Центр сертифікації ключів є

а) основною структурою, що формує цифрові сертифікати центрів сертифікації нижчого рівня та/або кінцевих користувачів;
б) допоміжною структурою, що формує цифрові сертифікати центрів нижчого рівня та кінцевих користувачів;

в) основною структурою, що формує пари секретних та відкритих ключів центрів нижчого рівня та кінцевих користувачів;
г) основною структурою, що формує цифрові сертифікати тільки центрів сертифікації нижчого рівня, але не кінцевих користувачів.

85. Відкриті ключі та інша інформація про користувача зберігається центром сертифікації у вигляді

а) зламозахищених пристроїв;
б) цифрових сертифікатів;
в) електронних відбитків пари «відкритий ключ – секретний ключ» користувача;
г) білетів з часовими мітками звернень до центру по інформацію.

86. Зберігання секретних ключів третьою стороною називається

а) ключовою банківською операцією;
б) хешуванням ключів;
в) депонуванням ключів;
г) резервним копіюванням ключів.

87. Що з вищенаведеного ***не*** входить до складу цифрового сертифікату відкритого ключа?

а) серійний номер; б) ім’я власника сертифіката;
в) закритий ключ; г) ім’я центру сертифікації.

88. Припустимо, що менеджер Вашої компанії хоче створити інфраструктуру для керування відкритими ключами і переконатися, що система повністю стандартизована. Якому стандарту мають відповідати сертифікати відкритих ключів?

а) X.501; б) X.509; в) IEEE 802.3; г) IEEE 802.11.

89. Якщо центр сертифікації видає Вам, як користувачеві, сертифікат формату X.509 Вашого відкритого ключа, то цей сертифікат підписаний за допомогою

а) Вашого відкритого ключа;
б) Вашого закритого ключа;
в) відкритого ключа центру сертифікації;
г) закритого ключа центру сертифікації.

90. Як Ви, звернувшись до центру сертифікації з питання отримання сертифікату для свого відкритого ключа, можете довести останньому, що Ви знає закритий ключ, відповідний Вашому відкритому?

а) поставити на запиті свій електронний цифровий підпис, який центр сертифікації перевірить за допомогою відкритого ключа користувача;
б) за допомогою залученого посередника;
в) письмово повідомити центр про значення закритого ключа;
г) за допомогою протоколу з нульовим розголошенням;
д) за допомогою протоколу «людина посередині».

91. Мінімальна інформація, що має бути записана у сертифікаті відкритого ключа, – це

а) прізвище, дата закінчення дії сертифіката, цифровий підпис центру та його поштова адреса;
б) прізвище, дата видачі сертифіката, дата закінчення дії сертифікату, відкритий ключ;
в) прізвище, роль користувача в інформаційній системі; серійний номер сертифіката, відкритий ключ;
г) прізвище, відкритий ключ, серійний номер сертифіката, цифровий підпис центру.

92. Центр сертифікації анулює сертифікати формату X.509 відкритих ключів за допомогою

а) знищення з комп'ютерної пам'яті;
б) публікації у репозиторії списку анульованих сертифікатів;
в) циркулярних листів центру сертифікації;
г) об'яви в пресі.

93. Уявіть, що 20.03.2012 р. дехто поставив свій електронний цифровий підпис під документом, а 22.03.2012 р. центр сертифікації ключів анулював сертифікат його відкритого ключа. При яких датах перевірки цей підпис вважатиметься легітимним, якщо сертифікат ключа було видано 01.03.2012 р.? Звичайно, алгоритм верифікації підпису не виявив протиріч.

а) 19 квітня 2012 р.; б) 21 березня 2012 р.; в) 23 березня 2012 р.

94. У якій із ситуацій сертифікат відкритого ключа треба анулювати?

а) клієнт банку на вимогу співробітника банку повідомив йому код доступу і пароль, що захищають його ЕЦП на ключовому носії;
б) банк повідомив свого клієнта, що виникли технічні несправності, які перешкоджали використанню електронних документів, підписаних клієнтом;
в) звільнився відповідальний співробітник компанії, який мав доступ до секретних ключів;

г) власник секретного ключа згенерував іншу ключову пару і отримав ще один сертифікат нового відкритого ключа;
д) смарт-картка, на якій зберігався секретний ключ, була дуже пошкоджена вогнем і перестала працювати;
е) протягом останнього часу власник ключа довго не використовував відкритий ключ.

95. Якими єнаслідки втрати Вашим співробітником зв'язки криптографічних ключів?

а) це порушення безпеки, потрібно анулювати його сертифікат відкритого ключа;
б) співробітник може відновити ключі;
в) він не зможе розшифрувати збережені файли;
г) інша відповідь.

96. Як можна отримати інформацію про анульовані сертифікати відкритих ключів?

а) перевірити статус сертифіката у режимі реального часу, надіславши запит до центру сертифікації;
б) перевірити статус сертифіката, зробивши запит власнику відкритого ключа за допомогою онлайнового протоколу;
в) звернутися до списку анульованих сертифікатів (CRL), що надсилається центром сертифікації прикладанням, де використовуються сертифікати;
г) запитати у відвідувачів веб-форуму, де обговорювалися останні зміни у списках анульованих сертифікатів з моменту його випуску.

97. Яке твердження *правильне*?

а) у будь-якому протоколі аутентифікації ключ сесії завжди створюється третьою довіреною стороною;
б) у будь-якому протоколі аутентифікації ключ сесії завжди створюється тільки одним учасником;
в) в одних протоколах аутентифікації ключ сесії створює центр розподілу ключів (KDC), а в інших – один з учасників мережі;
г) у будь-якому протоколі аутентифікації ключ сесії залежіть від вже існуючих «старих» ключів, що є в учасників мережі.

98. У якій спосіб учасники криптографічних протоколів розподілу ***не*** можуть підтвердити наявність ключа у себе?

а) обчислення хеш-коду ключа;
б) використання ключа в хеш-функції з ключем;
в) шифрування відомої величини з використанням ключа;

г) створення колізії для хеш-коду ключа;
д) доказ з нульовим розголошенням знання.

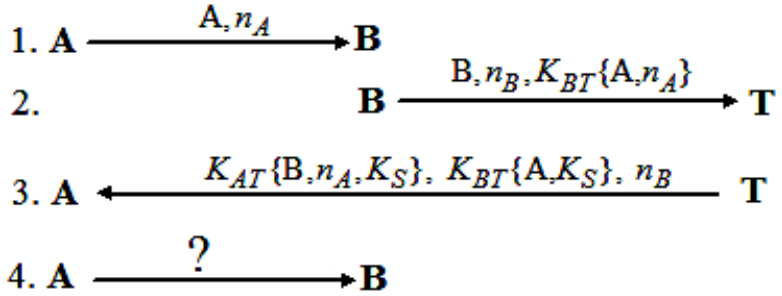
99. *Правильними* твердженнями щодо протоколу простого оновлення сеансового ключа на основі випадкових чисел є

а) в основі протоколу лежить симетричний алгоритм шифрування;
б) на першому кроці учасник **A** надсилає учаснику **B** відкритим каналом зв'язку випадкове число r_A;
в) на другому кроці учасник **B** надсилає зашифроване повідомлення, що містить число r_A і свою часову мітку t_B;
г) усього протокол потребує надсилання двох повідомлень.

100. Яку з наведених систем аутентифікації використовує центр розподілу ключів (KDC)?

а) сертифікати;
б) алгоритм CHAP;
в) компактний пристрій у вигляді USB-брелока – Security token;
г) протокол Kerberos.

101. Розглянемо протокол, в якому учасники **A** і **B** використовують довірену третю сторону **T** , щоб провести взаємну аутентифікацію і встановити сеансовий ключ K_S. Перед початком протоколу учасники **A** і **T** мають спільний секретний ключ K_{AT}, а учасники **B** і **T** – спільний ключ K_{BT}; n_A і n_B – випадкові числа, згенеровані учасниками **A** і **B** відповідно. Протокол містить чотири повідомлення, перші три з яких такі:



Яке повідомлення має отримати учасник **B** від учасника **A**, щоб завершити протокол?

а) $K_{AT}\{A, K_S\},\ K_S\{n_B\}$;
б) $K_{BT}\{A, K_S\},\ K_S\{n_B\}$;
в) $K_{BT}\{A, K_S\},\ n_B$;
г) $K_S\{A, K_{AT}, n_B\}$.

102. Визначте, скільки повідомлень з перших трьох кроків протоколу із задачі 101, має бачити зловмисник, щоб згенерувати повідомлення, наведені у таблиці. Для відповіді поставте зірочку у відповідній клітині, врахувавши таку символіку:
0 – якщо можна генерувати повідомлення відразу, не отримуючи жодної інформації з протоколу;
∞ – коли згенерувати повідомлення неможливо за будь-яких умов;
1,2,3 – якщо для генерування повідомлення необхідно бачити відповідно 1, 2 чи 3 повідомлення.

Повідомлення	0	1	2	3	∞
n_B					
$K_{AT}\{n_A\}$					
$K_X\{A\}$, де X – «свіжий» сеансовий ключ					
$n_A, n_B, K_{BT}\{A, K_S\}$					
$K_S\{A\}$					

103. У протоколі Нідхейма – Шредера центр розподілу ключів (KDC)

а) аутентифікує учасників обміну інформацією;
б) розподіляє ключі сесії;
в) розподіляє відкриті ключі учасників протоколу;
г) перевіряє сертифікати відкритих ключів учасників протоколу.

104. Яка головна мета передачі двох останніх повідомлень у протоколі Нідхейма – Шредера?

а) учасник **B** хоче упевнитися, що учасник **A** реально володіє сеансовим ключем, виробленим центром довіри і вказаним у квитку у третьому повідомленні;
б) центр розподілу ключів має записати у квиток створений і зашифрований ним сеансовий ключ та передати квиток учаснику **A**;
в) центр розподілу ключів хоче підтвердити «свіжість» сеансового ключа і вказує час його передачі у вигляді часової мітки у квитку, надісланому учаснику **B**;
г) учасник **A** надає учаснику **B** зашифроване випадкове число, яке той повинен розшифрувати і модифікувати так, щоб довести свою спроможність використовувати сеансовий ключ.

105. Яке твердження щодо протоколу Kerberos є *правильним*?

а) це двосторонній протокол розподілу ключів;

б) це протокол, який реалізує схему Діффі – Хеллмана відкритого розподілу ключів;
в) це протокол розподілу ключів, оснований на симетричних криптосистемах;
г) це протокол аутентифікації користувачів за допомогою SMS-повідомлень.

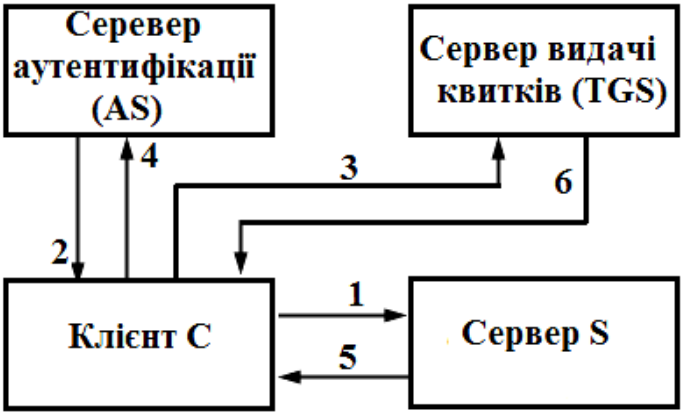


Рис. 6.6

106. Укажіть, за якою чергою взаємодіють учасники протоколу Kerberos (рис.6.6)

а) 4,2,3,6,1,5;
б) 5,3,6,4,2,1;
в) 6,4,2,1,5,3;
г) 3,6,4,2,5,1.

107. Які основні відмінності протоколу Kerberos від протоколу Нідхема – Шредера?

а) у протоколі Kerberos збільшена кількість повідомлень, що пересилаються між клієнтом і сервером аутентифікації;
б) на відміну від протоколу Нідхема – Шредера у протоколі Kerberos користувачеві видається первинне посвідчення (квиток – Ticket Granting Ticket) для доступу до мережевих ресурсів;
в) у протоколі Нідхема – Шредера передбачена синхронізація системних годинників учасників протоколу, а у протоколі Kerberos – ні;
г) у протоколі Нідхема – Шредера передбачені технічні заходи проти атаки методом повторення сеансу, а протокол Kerberos цій атаці легко піддається.

108. З якої причини у протоколі Kerberos застосовані системні годинники учасників протоколу?

а) для забезпечення надійного зв’язку;
б) для коректного визначення терміну дії квітків для доступу до мережевих ресурсів;
в) для генерації вектора ініціалізації, потрібного для шифрування ключів;
г) для визначення оптимального режиму шифрування.

109. За допомогою асиметричних ключів окрім виконання криптографічних операцій

а) керують симетричними ключами;
б) зберігають ключі;
в) генерують нові симетричні ключі;
г) відновлюють старі ключі.

110. У яких криптографічних протоколах його учасники виробляють спільний секрет як функцію від інформації, що вноситься кожним з них, при цьому ніхто наперед визначити спільний секрет не може?

а) протоколах транспортування ключів;
б) протоколах оновлення ключів;
в) протоколах обміну ключів;
г) протоколах розробки похідного ключа.

111. Який ризик виникає в мережі при організації шифрованого листування між користувачами, якщо в задіяній криптосистемі принципово неможливо використати усі можливі ключі з ключового простору?

а) небезпека повторення ключів; б) скорочення довжини ключа;
в) колізія ключів; г) поява слабких ключів.

112. Нехай зашифрування/розшифрування здійснюється за допомогою симетричного семантично стійкого шифру з ключем довжиною l бітів. Банк хоче розділити ключ на 3 частини p_1, p_2 і p_3 так, щоб розшифрувати повідомлення можна було тільки при наявності будь-яких двох з цих частин. Для цього банк генерує пари бітових рядків (k_1, k_1') і (k_2, k_2') з умовою $k_1 \oplus k_1' = k$ і $k_2 \oplus k_2' = k$ (довжина кожного з рядків k_1, k_1', k_2, k_2' дорівнює l бітів). Як банку розподілити ці частини, щоб ключ розшифрування відновлювався тільки з двох будь-яких частин, а одна частина ключ не відновлювала?

а) $p_1 = (k_1, k_2)$, $p_2 = (k_1, k_2)$, $p_3 = k_2'$;

б) $p_1 = (k_1, k_2)$, $p_2 = (k_1', k_2)$, $p_3 = k_2'$;

в) $p_1 = (k_1, k_2)$, $p_2 = k_1'$, $p_3 = k_2'$;

г) $p_1 = (k_1, k_2)$, $p_2 = (k_1', k_2')$, $p_3 = k_2'$;

д) $p_1 = (k_1, k_2)$, $p_2 = (k_2, k_2')$, $p_3 = k_2'$.

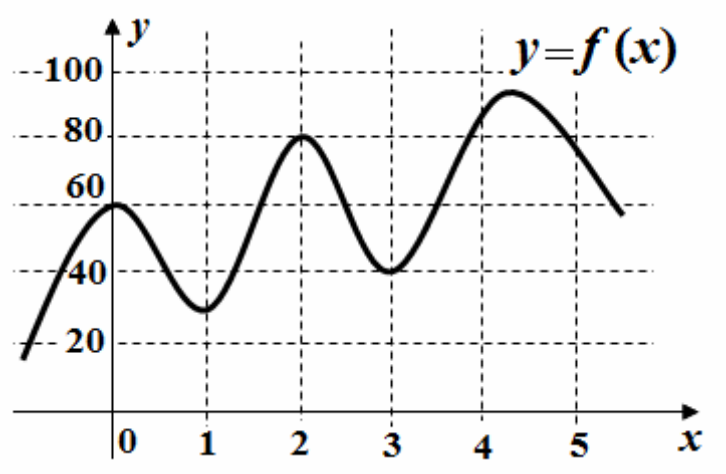


Рис. 6.7

113. Щоб розділити секрет за $(3,5)$-пороговою схемою Шаміра, вибрано деякий многочлен $y = f(x)$ над полем $GF(139)$, графік якого подано на рис. 6.7. Чому дорівнює цей секрет?

а) 30; б) 40; в) 50;
г) 60; д) 80; е)90.

114. Протокол Шаміра розподілу секрету

а) оснований на можливості відновити многочлен n-го степеня з коефіцієнтами із поля $GF(p)$ за його значеннями у n точках;

б) оснований на можливості відновити многочлен n-го степеня за його значеннями у $n+1$ точці;

в) дозволяє побудувати (t,n)-порогову схему;

г) розбиває секрет на n частин так, що його відновлення можливо лише за умови, що відомі значення всіх частин секрету.

115. Яка з нищенаведених схем ***не*** відноситься до схем розподілу секрету?

а) схема Діффі – Хеллмана;

б) (t,n)-порогова схема Шаміра;

в) векторна схема, основана на використанні точок багатовимірного простору (схема Блеклі);

г) схема, основана на китайській теоремі про остачі.

116. Фармацевтична компанія вирішила зашифрувати рецептуру нових ліків за допомогою симетричного шифру, а секретний ключ розділити між головним фармацевтом, двома його заступниками та п'ятьма офісними клерками так, щоб відновити секретний ключ зміг або сам головний фармацевт, або, якщо свої секретні частини об'єднають, один заступник та два клерки, або тільки два заступники, або тільки п'ять клерків. Якщо таку схему розподілу секрету розглядати як схему $(5,16)$ Шаміра, то як має бути розділений секрет між співробітниками компанії?

а) 6 частин – головному фармацевту, по 3 частини – заступникам; по 1 частині – клеркам;

б) 3 частини – головному фармацевту, по 2 частини – заступникам; по 1 частині – клеркам;

в) 16 частин – головному фармацевту, по 5 частини – заступникам; по 1 частині – клеркам;
г) 5 частин – головному фармацевту, по 3 частини – заступникам; по 1 частині – клеркам.

117. За $(k,10)$-пороговою схемою Шаміра розподілу секрету значення k може змінюватися

а) від 10 до $10+k$; б) від 2 до 9; в) від 2 до 10; г) від 10 до $10k$.

118. Доведення з нульовим розголошенням можна використати як

а) схему розподілу ключів;
б) схему доведення цілісності інформації;
в) схему ідентифікації для інтерактивної системи доведення;
г) спосіб довести неможливість перехоплення переданої інформації.

119. У процесі доведення з нульовим розголошенням один учасник переконує іншого у

а) неможливості перехопити передану інформації;
б) надійності механізму закриття переданої інформації;
в) коректності свого твердження, відкриваючи виключно йому, як партнеру, всі кроки доведення коректності твердження;
г) коректності свого твердження, не надаючи тому жодної інформації про те, чому це твердження коректне.

120. У протоколі доведення з нульовим розголошенням, основаному на задачі про ізоморфізм графів

а) обидва учасники протоколу знають ейлерів цикл у графах;
б) обидва учасники протоколу знають гамільтонів цикл у графах;
б) обидва учасники протоколу можуть обчислювально ефективно розв'язати задачу розпізнавання ізоморфізму графів;
в) лише один з учасників протоколу може обчислювально ефективно розв'язати задачу розпізнавання ізоморфізму графів;
г) один учасник переконує іншого, що графи ізоморфні.

121. Укажіть кроки із схеми доведення з нульовим розголошенням, основаної на складності задачі на пошук гамільтонового циклу у графі.

а) учасник **A** генерує випадкову перестановку вершин у графі;
б) учасник **A** генерує випадковий граф;
в) учасник **B** надсилає учаснику **A** випадкову перестановку;
г) учасник **A** надсилає учаснику **B** гамільтонів цикл у деякому графі.

122. Нагадаємо, що потреба у третій довіреній стороні (центрі довіри) є не тільки у тристоронніх протоколах розподілу ключів, основаних на симетричних криптосистемах. Центр сертифікації відкритих ключів для асиметричної криптографії також потребує довіреного серверу. Відзначте подібності та відмінності між цими двома схемами з погляду використання довірених серверів. Для відповіді поставте потрібні букви а) – ж) у клітини таблиці.

	Довірена третя сторона у протоколах з симетричними криптосистемами	Інфраструктура відкритих ключів
Конфіденційність		
Цілісність		
Корисність		
Рівень довіри		

а) зберігає довгострокові секретні ключі для кожного користувача системи;
б) зберігає лише відкриті ключі користувачів, які не потребують захисту;
в) сервер надсилає користувачам зашифрований сеансовий ключ;
г) не потрібен обмін ключами абонентів з сервером;
д) доступ до серверу лише для отримання ключів для перевірки електронного підпису.
е) довіра до серверу;
є) доступ до серверу на початку та протягом сеансу зв'язку.

123. Якщо людина підписала електронний цифровий документ за умови, що вона не ознайомлена з його змістом, то така модифікація ЕЦП називається

а) доказом з нульовим розголошенням; б) сліпим ЕЦП;
в) зашифрованим підписом; г) маскою.

124. Абонент **B** використовує для електронного підпису документів схему RSA з відкритим ключем (n,e) і секретним ключем d. Припустимо, що абонент **A** хоче, щоб **B** підписав повідомлення M, не ознайомившись з його змістом. Згідно з протоколом сліпого цифрового підпису абонент **A** вибирає випадкову величину r з умовою $\text{НСД}(n,r)=1$ і надсилає абоненту **B** значення $X = r^e \cdot M \bmod n$. Той підписує $t = X^d \bmod n$ отримане повідомлення і повертає його абоненту **A**. Як далі абоненту A знайти електронний підпис S повідомлення M?

а) $S = (rt)^{-1} \bmod n$;
б) $S = rt^{-1} \bmod n$;
в) $S = r^{-1}t \bmod n$;
г) $S = r^2 t \bmod n$;
д) $S = r^{-1}t^2 \bmod n$;
д) $S = r^{-2}t \bmod n$.

125. Протоколи електронних платежів базуються на

а) груповому ЕЦП;
б) часових мітках платежу;
в) доведенні з нульовим розголошенням;
г) цифровому конверті;
д) сліпому ЕЦП;
е) хеші електронних грошей.

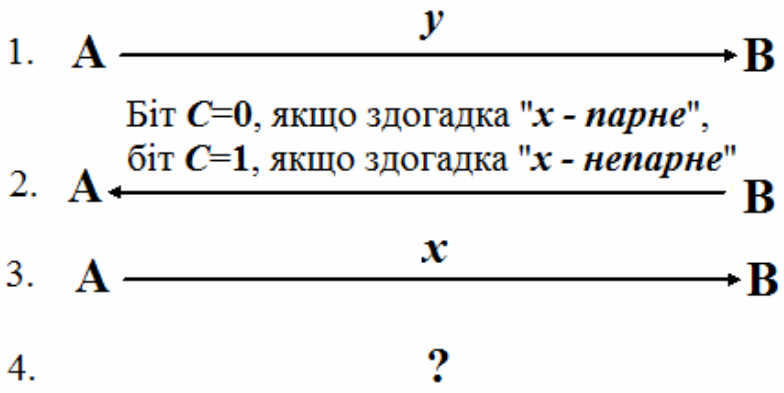
126. Мета криптографічного захисту електронних грошей

а) їх ототожнення з безготівковими грошима;
б) забезпечення анонімності покупця;
в) забезпечення неможливості повторного використання грошей;
г) уведення персоналізованих механізмів поповнення електронного гаманця;
д) уведення обмеження розміру електронного гаманця для запобігання інфляції.

127. Криптографічний протокол, що дає змогу двом його учасникам, які не довіряють один одному, згенерувати спільний випадковий рівноймовірнісний біт, називається

а) протоколом з нульовим розголошенням;
б) протоколом чесного обміну;
в) схемою розподілу секрету;
г) протоколом підкидання монети по телефону.

128. Параметри протоколу підкидання монети на основі дискретного логарифма: p – велике просте число; g – твірний елемент групи $GF^*(p)$. Учасник **А** навмання вибирає число $x \in GF(p)$ і обчислює $y = g^x \bmod p$. Визначте останній четвертий крок наведеного протоколу:



а) учасник **В** визначає $x = g^y \bmod p$ і перевіряє умову $x = y$;

б) учасник **В** визначає $y' = g^x \bmod p$ і перевіряє умову $y' \neq y$;

в) учасник **В** визначає $y' = g^x \bmod p$ і перевіряє умову $y' = y$;

г) учасник **В** визначає $g' = (y')^{-x} \bmod p$ і перевіряє умову $g' = y'g$.

129. Нехай у протоколі прив'язки до біту P_1 – імовірність того, що учасник, який підкидає монету, зможе змінити вибраний біт після отримання догадки від іншого учасника; P_2 – імовірність того, що учасник, який вгадує, зможе дізнатися значення біта, вибраного іншим учасником, ще до об'яви своєї догадки; P_3 – імовірність вибору учасником, що підкидає монету, біта «1» щоразу при підкиданні монети. Укажіть *правильні* твердження щодо цих імовірностей.

а) $P_1 \to 0$, $P_2 \to 0$, $P_3 = 1/2$;

б) $P_1 \to 1/2$, $P_2 \to 1/2$, $P_3 = 1/2$;

в) $P_1 \to 1$, $P_2 \to 1$, $P_3 = 0$;

г) $P_1 \to 0$, $P_2 \to 1$, $P_3 = 1$.

130. Установіть відповідність між криптографічними примітивами і метрикою їхніх параметрів безпеки.

I – блоковий шифр;	а) довжина ключа;
II – хеш-функція;	б) довжина дайджесту;
III – HMAC;	в) довжина шифротексту.

131. Упорядкуйте наведені шифри у відповідності з потужністю їхнього ключового простору, починаючи з шифру з найменшою кількістю ключів. За необхідністю вважайте, що використовується український алфавіт.

1. 3DES з трьома ключами k_1, k_2, k_3;
2. AES із стандартним найбільшим за розміром ключем;
3. Шифр Віженера з періодом гами 16 букв;
4. RSA-1024;
5. DESX.

а) 3,5,2,1,4; б) 5,3,1,4,2; в) 1,3,5,4,2; г) 1,5,3,2,4.

132. З’єднайте лніями подані у лівому стовпці типи криптоатак з відповідними алгоритмами або режимами шифрування, що піддаються цим атакам.

Атака на основі відкритого тексту	Схема Діффі – Хеллмана
Атака на основі вибраного відкритого тексту	RSA
Атака на основі вибраного шифротексту	3DES
Атака «чоловік посередині»	Одноразовий блокнот
Атака із спільним модулем	CBC

133. Розділіть операції а) – ж), що виконуються при обміні зашифрованими і підписаними повідомленнями за допомогою PGP, на ті, що

I – здійснюються тільки на стороні відправника;
II – здійснюються тільки на стороні отримувача;
I – здійснюються обома сторонами;
IV – не виконуються жодною зі сторін.

а) генерування випадкового ключа;
б) доступ до закритого ключа;
в) декомпресія за допомогою алгоритму ZIP;
г) визначення хеш-образу повідомлення;
д) доступ до відкритого ключа;
е) визначення відкритого ключа перетворення на основі відкритого ключа отримувача;
ж) визначення відкритого ключа перетворення на основі відкритого ключа відправника;
з) верифікація сертифікату відкритого ключа відправника.

РОЗДІЛ 7. ПРАВДА ЧИ НЕПРАВДА?

Виберіть правильну відповідь.

		Твердження
Правда	Ні	Якщо E_k – блоковий шифр, то наступна схема шифрування безпечна проти атаки з вибраним відкритим текстом: для шифрування повідомлення M, відправник шифрує випадкове число r за допомогою блокового шифру E_k на ключі k та обчислює криптограму $E_k(r) \oplus M$
Правда	Ні	Дехто генерує відкритий та секретний ключі для криптосистеми RSA і публікує відкритий ключ. Цього достатньо, щоб він міг надіслати будь-кому надійно зашифрованого листа
Правда	Ні	Генерація великого обсягу якісних ключів є основною проблемою шифрування за допомогою одноразового шифрувального блокноту
Правда	Ні	Використання у схемах електронного цифрового підпису криптографічних алгоритмів з відкритим ключем дозволяє забезпечити цілісність документа та ідентифікувати особу, що його підписала
Правда	Ні	Шифр Цезаря вразливий до атаки на основі відомого відкритого тексту
Правда	Ні	Ключовий простір афінного шифру складається з 33^2 різних ключів (алфавіт – український)
Правда	Ні	Якщо відкритому тексту НЕДІЛЯ відповідає шифротекст ТАРААН, то для зашифрування не міг використовуватися афінний шифр
Правда	Ні	У якості ключа шифру Хілла можна вибрати будь-яку квадратну матрицю з ненульовим детермінантом

Правда	Ні	Сучасні криптографічні примітиви мають протистояти відомим атакам на основі відомого відкритого тексту, а не атакам на основі вибраного відкритого тексту
Правда	Ні	Для проведення атак на основі побічних каналів потрібно знати відкритий та секретний ключі
Правда	Ні	Існують досконало стійкі шифри
Правда	Ні	Основний недолік асиметричних криптосистем – низька швидкість виконання шифрувальних операцій
Правда	Ні	При обчисленні MAC повідомлення надзвичайно важливо застосовувати рандомізований вектор ініціалізації, непередбачуваний зловмисником
Правда	Ні	Потрійне послідовне шифрування за допомогою одного й того ж самого шифру з різними ключами завжди має більшу стійкість, ніж одноразове шифрування цим шифром
Правда	Ні	Подвійне послідовне застосування одного й того ж самого шифру з різними ключами недоцільне внаслідок загрози проведення атаки «зустріч посередині»
Правда	Ні	Генератор псевдовипадкових бітових послідовностей може пройти певний набір статистичних тестів, але виявитися неякісним з точки зору криптографічного захисту інформації
Правда	Ні	Щоб провести атаку «зустріч посередині» необхідно мати пару «відкритий текст – відповідний шифрований текст»
Правда	Ні	Атака «зустріч посередині» відноситься до атак з на основі відомого відкритого тексту

Правда	Ні	AES – блоковий шифр, оснований на мережі Фейстеля
Правда	Ні	Кількість раундів стандарту AES-128 дорівнює 14
Правда	Ні	Шифрування за допомогою алгоритму 2-DES суттєво більш стійке, ніж за допомогою звичайного DES
Правда	Ні	Криптосистема 3-DES з двома різними ключами суттєво стійкіша, ніж криптосистема 2-DES
Правда	Ні	Складність повного перебору ключів AES-128, у 2^{72} разів більше ніж у випадку повного перебору ключів криптоалгоритму DES
Правда	Ні	Криптосистема DES має 32-раундову структуру Фейстеля
Правда	Ні	Зашифрування відкритого тексту 000…00 за допомогою алгоритму DES з будь-яким ключем перетворює його у шифрований текст 000…00
Правда	Ні	Мета шифрування та кодування інформації завжди різні
Правда	Ні	Якщо повідомлення підписане за допомогою схеми ЕЦП RSA, то для перевірки підпису потрібно піднести підпис до степеня e (за модулем n), де e – відкрита експонента абонента, який підписав документ
Правда	Ні	Збільшення довжини модуля криптоалгоритму RSA з 1024 біт до 2048 біт подвоює кількість операцій, потрібних для його факторизації
Правда	Ні	Вразливою до атак за побічними каналами є лише криптосистема RSA
Правда	Ні	Якщо електронний цифровий підпис реалізовано на основі алгоритму RSA та хеш-функції SHA-1, то

		усі протоколи, де задіяний такий підпис, можна зламати
Правда	Ні	Безпека шифрування за допомогою криптоалгоритму RSA базується на задачі дискретного логарифмування
Правда	Ні	Якщо $n = 77$ – модуль RSA, то 5 – припустиме значення відкритої експоненти
Правда	Ні	Криптоалгоритм DES у режимі OFB можна застосовувати для генерації гами для потокового шифру
Правда	Ні	Система ЕЦП гарантує неможливість відмови від авторства
Правда	Ні	Шифрування за допомогою криптосистем на основі еліптичних кривих менш ефективно, ніж за допомогою криптосистеми Ель-Гамаля
Правда	Ні	Колізія – це слабкість шифру, яка полягає у тому, що шифрування різних відкритих текстів з використанням різних ключів може привести до однакового шифротексту
Правда	Ні	Замість криптоалгоритму DES у якості сучасного стандарту шифрування США обрано криптоалгоритм RIJNDAEL
Правда	Ні	Кількість слабких ключів AES-128, AES-192 і AES-256 дорівнює 16, 24 і 32 відповідно
Правда	Ні	X-509 – стандарт, що визначає формати даних та розподілу відкритих ключів за допомогою сертифікатів з електронними цифровими підписами
Правда	Ні	Алгоритми AES і RSA можуть використовуватися для шифрування електронної пошти підвищеної конфіденційності (PEM)

Правда	Ні	Криптоалгоритм RSA – досконало стійкий шифр
Правда	Ні	Можна побудувати поліалфавітний шифр на основі кількох моноалфавітних
Правда	Ні	Шифр одноразового блокноту є стійким проти атак на основі відкритого тексту, якщо у секреті зберігають його ключі, що мають випадковий характер та рівномірний розподіл
Правда	Ні	Якщо ключ шифру DES або шифру AES дійсно випадковий, ніколи не використовуються повторно, і тримається в секреті, то обидва шифри є стійким проти атак на основі відкритого тексту
Правда	Ні	У випадку блокового шифру із структурою Фейстеля процедури зашифрування та розшифрування (програмне забезпечення або апаратний засіб) нічим не відрізняються
Правда	Ні	Протокол Діффі – Хеллмана реалізує електронний цифровий підпис, але не так ефективно, як RSA
Правда	Ні	Для обчислення хеш-образу повідомлення за допомогою криптографічної хеш-функції SHA-1 потрібен секретний ключ
Правда	Ні	Алгоритм хешування, рекомендований у стандарті електронного цифрового підпису DSS, створює дайджести, довжина яких дорівнює 128 біт
Правда	Ні	Для забезпечення однакової стійкості довжина ключів криптосистем з відкритим ключем має бути набагато більшою, ніж у ключів симетричних шифрів
Правда	Ні	Стійка до відновлення другого прообразу криптографічна хеш-функція обов’язково є стійкою до колізій
Правда	Ні	Протокол Нідхема – Шредера автентифікації та обміну ключами виконується за п’ять кроків

Правда	Ні	Протокол KERBEROS вразливий до атаки «людина посередині»
Правда	Ні	У протоколі KERBEROS часи всіх клієнтів та серверів синхронізовані
Правда	Ні	Протокол KERBEROS відноситься до протоколів з арбітражем
Правда	Ні	Якщо особа хоче отримати сертифікат відкритого ключа у центрі сертифікації ключів, то центр крім сертифікату передає їй копію свого секретного ключа
Правда	Ні	Можливо так розділити секретну інформацію між абонентами A, B і C, що пари учасників A і B або A і C зможуть його відновити, а пара учасників B і C або поодинці учасники A, B і C не зможуть отримати жодної інформації про секрет

СПИСОК ЛІТЕРАТУРИ

1. Бабаш, А. В. Криптография [Текст]: учеб. пособие / А. В. Бабаш, Г. П. Шанкин. – М.: СОЛОН-Р, 2002. – 511 с.

2. Бабенко, Л. К. Современные алгоритмы блокового шифрования и методы их анализа [Текст] / Л. К. Бабенко, Е. А. Ищукова. – М.: Гелиос, 2006. – 376 с.

3. Бернет, С. Криптография. Официальное руководство RSA Security [Текст]: пер. с англ. / С. Бернет, С. Пейн. – М.: Бином-Пресс, 2002. – 292 с.

4. Болотов, А.А. Элементарное введение в эллиптическую криптографию: протоколы криптографии на эллиптических кривых. / А.А. Болотов, С.Б. Гашков, А.Б. Фролов. – М.: КомКнига, 2004. – 280 с.

5. Болотов, А.А. Алгоритмические основы эллиптической криптографии. / А.А. Болотов, С.Б. Гашков, А.Б. Фролов, Часовских А.А.. – М.:РГСУ, 2004. –499 с.

6. Василенко, О. Н. Теоретико-числовые алгоритмы в криптографии [Текст] / О. Н. Василенко. – М.: МЦНМО, 2003. – 328 с.

7. Введение в криптографию / Под общ. ред. В.В.Ященко. 3-е изд., доп. [Текст] / Ященко В.В.- М.:МЦНМО: «ЧеРо», 2000. – 236с.

8. Горбенко, І. Д. Прикладна криптологія. Теорія. Практика. Застосування [Текст] / І. Д. Горбенко, Ю. І. Горбенко. – Х. : Форт, 2012. – 870 с.

9. Иванов, М. А. Криптографические методы защиты информации в компьютерных системах и сетях [Текст]: учеб.-справ. пособие / М. А. Иванов. – М.: КУДИЦ-ОБРАЗ, 2001. – 368 с.

10. Иванов, М. А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей [Текст] / М. А. Иванов, И. В. Чугунков. – М.: КУДИЦ-ОБРАЗ, 2003. – 238 с.

11. Конхейм, А. Г. Основы криптографии [Текст]: пер. с англ. / А. Г. Конхейм. – М.: Радио и связь, 1987. – 412 с.

12. Лидл, Р. Конечные поля [Текст]: пер. с англ. / Р. Лидл, Г. Нидеррайтер. – М.: Мир, 1988. – 820 с.

13. Мао, В. Современная криптография: теория и практика [Текст]: пер. с англ. / В. Мао. – М.: ИД Вильямс, 2005. – 768 с.

14. Математичні основи криптографії [Текст]: навч. посібник / Г. В. Кузнецов, В. В. Фомичов, С. О. Сушко, Л. Я. Фомичова. – Д.: НГУ, 2004. – 391 с.

15. Математичні основи криптоаналізу [Текст]: навч. посібник / С. О. Сушко, Г. В. Кузнецов, Л. Я. Фомичова, А. В. Корабльов. – Д.: НГУ, 2004. – 391 с.

16. Нечаев, В. И. Элементы криптографии. Основы защиты теории информации [Текст]: учеб. пособие / В. И. Нечаев. – М.: Высш. шк., 1999. – 109 с.

17. Основи криптографічного захисту інформації [Текст]: підручник / Г.М.Гулак, В.А. Мухачов, В.О. Хорошко, Ю.Є. Яремчук. – В.: ВНТУ, 2011. – 198 с.

18. Основы криптографии [Текст]: учеб. пособие / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – М.: Гелиос, 2002. – 480 с.

19. Панасенко, С. П. Алгоритмы шифрования. Специальный справочник [Текст] / С. П. Панасенко. – С.Пб.: БХВ-Петербург, 2009. – 576 с.

20. Поточные шифры. Результат зарубежной открытой криптологии [Електронный ресурс] / Москва. – www/ URL: http://www.ssl.stu.neva.ru/psw/crypto/potok/str_ciph.htm/. – 01.12.1997 – Загл. с экрана.

21. Ростовцев, А. Г. Теоретическая криптография [Текст] / А. Г. Ростовцев, Е. Б. Маховенко. – С.Пб.: АНО НПО Профессионал, 2005. – 480 с.

22. Смарт, Н. Криптография [Текст]: пер. с англ. / Н. Смарт. – М.: Техносфера, 2005. – 528 с.

23. Столингс, В. Криптография и защита сетей: принципа и практика [Текст]: пер. с англ. / В. Столлингс. – М.: ИД Вильямс, 2001. – 672 с.

24. Тилборг Х.К.А. Основы криптологии [Текст]: пер. с англ. / Тилборг ван Х.К.А.. – М.: Мин, 2006. – 471 с.

25. Фомичов, В. М. Методы дискретной математики в криптологии. [Текст]: учеб. пособие / В. М. Фомичов. – М.: Диалог-МИФИ, 2010. – 423 с.

26. Фороузан, Б.А. Криптография и безопасность сетей [Текст]: пер. с англ. / Б. А. Фороузан. – М.:ИУИТ Бином. Лаборатория знаний, 2010. – 784 с.

27. Харин, Е. С. Математические основы криптологии [Текст]: учеб. пособие / Е. С. Харин, В. И. Берник, Г. В. Матвеев. – Минск: БГУ, 1999. – 319 с.

28. Хорошко, В. А. Методы и средства защиты информации [Текст] / В. А. Хорошко, А. А.Чекатков; под общ. ред. Ю. С. Ковтанюка. – К.: Юниор, 2003. – 504 с.

29. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си [Текст]: пер. с англ. / Б. Шнайер. – М.: Триумф, 2002. – 916 с.

30. Яглом, А. М. Вероятность и информация [Текст] / А. М. Яглом, И. М. Яглом. – М.: Наука, 1973. – 511 с.

31. Baigneres, T. A Classical Introduction to cryptography Exercise Book [Text] / T. Baigneres, P. Junod, Y. Lu, J. Monneart, S. Vaudenay. – Springer, 2006. – 254 p.

32. Hoffstein, J. An Introduction to Mathematical Cryptography [Text] / J. Hoffstein, J. Pipher, J.H. Silverman. – Springer, 2008. – 523 p.

33. Menezes, A. J. The Handbook of Applied Cryptography [Text] / A. J. Menezes, P. K. Oorschot, S. A. Vanstone. – New York: CRC Press, 1997. – 816 p.

34. A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications [Text]: NIST Special Publication 800-22 Rev1. – Gaithersburg, Maryland: NIST, 2008. – 153 p.

Навчальне видання

Бабенко Тетяна Василівна
Гулак Геннадій Миколайович
Сушко Світлана Олександрівна
Фомичова Людмила Яківна

Криптологія у прикладах, тестах і задачах

Навчальний посібник

Видано в авторській редакції

Підп. до друку 10.10.13. Формат 30×42/4.
Папір офсетний. Ризографія. Ум. друк. арк. 17,7.
Обл.-вид. арк. 17,7. Тираж 300 пр. Зам. №

Підготовлено до друку та видрукувано
у Державному вищому навчальному закладі
«Національний гірничий університет»
Свідоцтво про внесення до Державного реєстру ДК №1842
від 11.06.2004р.

49005, м. Дніпропетровськ, просп. К. Маркса, 19.