МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Методичні рекомендації та контрольні завдання
з навчальної дисципліни

"ЗАХИСТ ІНФОРМАЦІЇ В ІС"

для студентів напряму підготовки "Комп'ютерні науки"
заочної форми навчання

Харків. Вид. ХНЕУ, 2008

Затверджено на засіданні кафедри інформаційних систем.
Протокол №9 від 2.04.2008 р.

М54 Методичні рекомендації та контрольні завдання з навчальної дисципліни "Захист інформації в ІС" для студентів напряму підготовки "Комп'ютерні науки" заочної форми навчання / Укл. В. В. Огурцов, А. О. Поляков. – Харків: Вид. ХНЕУ, 2008. – 44 с. (Укр. мов.)

Включено рекомендації та завдання з основних розділів навчальної дисципліни, які присвячено вивченню методів і засобів захисту інформації в інформаційних системах та призначено для практичного засвоєння й використання криптографічних методів і засобів захисту інформації в ІС.

Рекомендовано для студентів та аспірантів економічних і технічних навчальних закладів, які спеціалізуються в галузі використання й упровадження методів, засобів та механізмів захисту інформації в ІС у різних сферах діяльності.

Вступ

"Захист інформації в інформаційних системах (ІС)" – широкомасштабний курс, повний обсяг знань з якого одержати самостійно досить важко. Він включає велику кількість тематик зі створення комплексної системи захисту інформації в ІС, вивчення видів інформаційних загроз і методів, засобів та механізмів захисту інформації від них.

Дані методичні рекомендації призначені для якісної організації проведення практичних та лабораторних робіт, введених на підставі навчальних планів для студентів напряму підготовки «Комп’ютерні науки» заочної форми навчання з навчальної дисципліни "Захист інформації в ІС".

Методичні рекомендації містять опис 3 основних тем навчальної дисципліни. Кожна тема складається з таких пунктів:

мета роботи;

рекомендації щодо підготовки до виконання роботи;

основні положення;

контрольні завдання (загальні та індивідуальні);

контрольні запитання.

Вивчення тем та виконання завдань містить наступні етапи:

1. Підготовчий етап (до проведення практичного або лабораторного заняття):

а) одержання відповідного даним методичним рекомендаціям завдання, номера варіанта й вимог викладача;

б) вивчення теоретичного матеріалу за відповідною темою;

в) розробка алгоритму виконання завдання.

2. Безпосереднє виконання завдання в аудиторії, в комп'ютерному класі обчислювального центру або самостійно (в іншому місті, наприклад, вдома).

а) проходження допуску до лабораторної роботи (ЛР);

б) установлення (за необхідності), конфігурування додатка;

в) відпрацьовування завдання за варіантом;

г) аналіз отриманих результатів.

3. Складання звіту і захист роботи.

1. Класичні симетричні системи. Дослідження криптостійкості простих симетричних шифрів

1.1. Мета. Ознайомитися з основними принципами шифрування даних на основі найпростіших шифрів. Вивчити елементарні криптографічні операції: перестановки й підстановки. Проаналізувати їх властивості. Вивчити принципи криптоаналізу на основі використання частотного аналізу криптограм. Навчитися здійснювати оцінку криптографічної стійкості простих шифрів.

1.2. Рекомендації щодо підготовки до виконання ЛР

Необхідно вивчити математичні поняття перестановки та підстановки, принципи шифрування й розшифрування текстових повідомлень, а також розуміти модель криптоаналітика.

1.3. Загальні положення ЛР

З поширенням писемності, посиленням централізованої влади, усвідомленням важливості й цінності інформації в суспільстві з'явилася потреба в обміні повідомленнями, що містять конфіденційну інформацію. Під конфіденційною інформацією розуміються будь-які відомості, повідомлення, дані або відомості, в яких утримується інформація, що має як матеріальну, так і особисту цінність для її власника. Розголошення конфіденційної інформації може призвести до втрати репутації індивідуума або організації, що, у свою чергу, тягне матеріальні втрати.

Методи приховування вмісту письмових повідомлень можна розділити на три класи [4]:

I. Методи маскування. За допомогою цих методів здійснюється приховування самого факту передачі інформації.

II. Методи тайнопису або криптографії (від грецьких слів *κρυπτός* – таємний і *γράφω* – пишу). Методи цього класу спрямовані на руйнування значеннєвого значення, тобто зміну повідомлення з метою зробити текст безглуздим для стороннього користувача.

III. Технічні методи приховування інформації, інвертування мови та ін.

Далі будемо розглядати тільки методи другої групи, а саме методи криптографії.

Метод криптографії становить собою множину відображень одного простору (простору відкритих (текстів) повідомлень) в інший простір (простір шифрованих (закритих) криптограм). Кожне конкретне відображення із цієї безлічі відповідає шифруванню з використанням випадкової складової, секретного ключа.

Ознайомимось з основними поняттями.

Повідомлення – текст, малюнок, аудіозапис, зміст або інші електронні дані, що мають значеннєве наповнення й містять конфіденційну інформацію.

Відкритий (вихідний) текст – повідомлення, яке необхідно зробити недоступнимо для сторонніх, тобто порушити його значеннєву логіку. Множина відкритих текстів позначається.

Шифрований (закритий) текст – повідомлення з перекрученим логічним змістом, яке також називається криптограмою, або шифротекстом. Множина криптограм позначається.

Ключ – секретне значення деякого параметра або параметрів, що забезпечує вибір одного перетворення із сукупності можливих для використовуваного методу шифрування. Ключ становить випадкове число або вектор. Множина ключів позначається К.

Шифр – сукупність оборотних перетворень безлічі можливих відкритих текстів у безліч можливих шифртекстів, що здійснюються за певними правилами із застосуванням ключа.

Шифрування – процеси перетворення повідомлень, що складаються із взаємооднозначних процесів зашифровування, у результаті виконання яких відкриті повідомлення відображаються в шифртекст. Математично процес шифрування даних позначається Е.

Розшифрування – вид перетворення повідомлення, що здійснюється з метою відновлення змісту інформації, яка прихована в зашифрованому тексті (шифротексті), в результаті виконання якого зашифроване повідомлення (шифротекст) відображається у відкрите повідомлення (рис. 1.1)

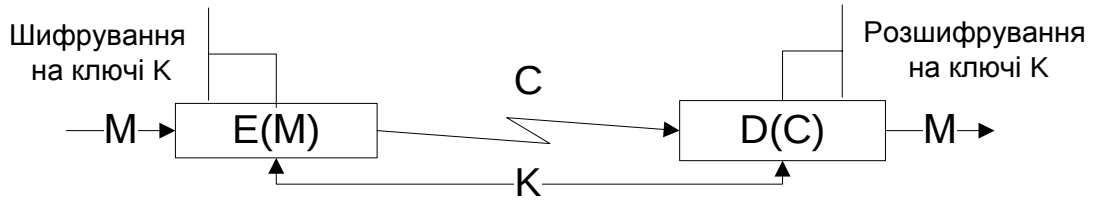

Рис. 1.1. **Модель процесів шифрування-розшифрування**

Криптоаналіз – область криптології, в якій розглядаються питання злому шифрів з метою відновлення інформації у відкритому вигляді або фальсифікації шифрованої інформації, що в результаті повинна бути прийнята як справжня.

Симетричні алгоритми діляться на дві категорії. Одні з них обробляють текст побітово (або побайтово) і називаються потоковими алгоритмами, або потоковими шифрами. Ті ж, які працюють із групами бітів відкритого тексту, називаються блоковими алгоритмами (шифрами). У лабораторній роботі розглядаються найпростіші симетричні шифри, засновані на найпростіших арифметичних операціях підстановки, перестановки й елементах модульної арифметики. Тому всі прості симетричні шифри можна розділити на дві групи шифрів:

1. Перестановочні.
2. Підстановочні:
   а) одноалфавітні;
   б) поліалфавітні.

Алфавітом називаємо довільну скінчену впорядковану множину A, в яку записані повідомлення (відкриті тексти). Приклад українського алфавіту наведено далі:

№	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathrm{A}_{ó}$	А	Б	В	Г	Ґ	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М

№	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
$\mathrm{A}_{ó}$	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_

Повідомлення M є словом в алфавіті A (яке може складатися з багатьох слів у звичайному лінгвістичному розумінні), тобто $M \in \mathrm{A}^*$. Множина A^* називається *простором повідомлень,* або простором *відкритих текстів*.

Шифр називається *блоковим* з періодом l, якщо, шифруючи відображення, задається спочатку на словах довжини l, тобто маємо $E: \mathrm{K} \times \mathrm{A}^l \to \mathrm{C}$, а після цього поширюються на слова довільної довжини наступним чином. Якщо $M = m_1 \| m_2 \| ... \| m_t$, де блоки m_i, $i \le t$, мають довжину l, то $E(K_e, M) = E(K_e, m_1) \| E(K_e, m_2) \| ... \| E(K_e, m_t)$. Якщо ж

останній блок m_t має меншу ніж l довжину, то він доповнюється до повного наперед обумовленим чином. Доповнення блоку може формуватися за одним з правил [1]:

недостатні символи заповнюються однією буквою з алфавіту A;

вибираються з випадкового наперед обумовленого слова;

вибираються з попереднього блоку криптограми;

вибираються з попереднього блоку відкритого повідомлення.

Саме доповнення може бути відкритим і відоме всім, у тому числі і криптоаналітику. Тому для того, щоб доповнення було випадковим, рекомендується, щоб при шифруванні останнього блоку не проходило виродження криптограми, тобто не з'являлася будь-яка апріорна інформація про ключ шифрування.

Перестановкою називаються розташовані в певному порядку k елементи упорядкованої безлічі M або алфавіту.

Підстановка – це взаємооднозначне відображення f деякої кінцевої множини M на множині M' або на себе. При цьому в підстановці беруть участь усі елементи множин M та M'.

Перестановочні шифри

Перестановочні шифри засновані на алгебраїчній операції, що називається перестановкою, внаслідок виконання якої здійснюється шифрування відкритого тексту й дешифрування криптограми.

Перестановочний шифр з ключовим словом

Відкритий текст повідомлення M представлений значеннєвим набором слів в алфавіті A^* довжини t.

Секретний ключ K складається з одного або декількох слів в алфавіті A довжини l.

Алгоритм шифрування E становить наступне відображення, що складається з таких кроків:

1. Із секретного ключа K (секретного слова) формуємо ключову перестановку за наступним правилом.

Ключ K представляється послідовністю букв $k_0k_1k_2...k_i...k_l$ з алфавіту A. Упорядковується букви ключа K за зростанням $k_i...k_2...k_1...k_l...$ тієї ж довжини, але за умови, що кожна буква, яка перебуває праворуч, більша ніж та, що передбуває ліворуч. Номери

позицій букв ключа будуть задавати ключову перестановку $\bar{K} = (i,...,2,...,1,...,l,...)$.

Приклад

Ключове слово: шифр довжиною $l = 4$.

ø	è	ô	ð
0	1	2	3

$\Rightarrow$

è	ð	ô	ø
1	3	2	0

2. Шифрування повідомлення M довжиною t виконується наступним шляхом.

По-перше, повідомлення M доповнюється таким чином, щоб його довжина $t + \Delta$ була кратна довжині ключа K, тобто

$$(t + \Delta) \bmod l = 0, \text{ або } l \mid (t + \Delta),$$

де Δ – довжина доповнення.

Далі шифруємо кожну букву m_i повідомлення M окремо за допомогою ключової перестановки $\bar{K} = (\bar{k}_0, \bar{k}_1, ..., \bar{k}_l)$ за формулою

$$c_i = m_{\bar{k}_{\lfloor i/k \rfloor} + (i \bmod k) \cdot l}, \; i = \overline{0, t + \Delta - 1}, \qquad (1.1)$$

де $k = (t + \Delta) / l$.

У результаті отримуємо криптограму $C = c_0 \| c_1 \| c_2 \| ... \| c_{t+\Delta-1}$.

Дешифрування виконується у зворотному напрямку, використовуючи формулу (1.1). Для відповідної криптограми отримуємо відкритий текст.

Більш зручним та зрозумілим буде наступний опис цього алгоритму, який називається *матричним шифром обходу*.

Повідомлення записується рядками у вигляді прямокутної матриці. Пусті клітинки, що залишилися, заповнюються пробілом або іншою буквою з алфавіту. Криптотекст формується зчитуванням букв із матриці у зміненому порядку, а саме стовпцями. При цьому послідовність, у якій зчитуються стовпці, визначається ключем. Букви ключового слова пишуться над стовпцями і вказують порядок цих стовпців (за збільшенням номерів букв в алфавіті). Приклад наведено на рис. 1.2.

Ключове слово (ключ) задає перестановку букв у повідомлення. Розшифрування виконується з використанням ключа шифрування, а криптограма записується в таблицю відповідно до індексів букв ключового слова, від молодшого до більшого. Після заповнення всієї

таблиці криптограмою відкритий текст одержуємо, зчитуючи таблицю за рядками зліва на право, починаючи з першого рядка й до останнього.

Відкритий текст: `захист_інформації`

Ключ: `шифр`

Ключ	ш	и	ф	р
	3	0	2	1
Відкритий текст	з	а	х	и
	с	т	_	і
	н	ф	о	р
	м	а	ц	і
	ї	_	_	_

Криптограма: `атфа_иірі_х_оц_зснмї`

Рис. 1.2. **Матричний шифр обходу**

Матрична перестановка з подвійним ключем

Матрична перестановка з подвійним ключем становить більш складну перестановку. Для цього відкритий текст записується в матрицю за певним ключем $K_1 = \{1, 2, ..., n\}$, що залежить від довжини тексту. Криптограма утворюється при зчитуванні з цієї матриці за ключем $K_2 = \{1, 2, ..., m\}$. Розмірність матриці дорівнює $n \times m$.

Приклад

Відкритий текст: "*ШИФРУВАННЯ_ПЕРЕСТАВЛЕННЯМ*".

Ключі: $K_1 = \{5, 3, 1, 2, 4, 6, 7\}$;

$K_2 = \{4, 2, 3, 1\}$.

Матриця складається із шести рядків і чотирьох стовпців 7×4 (рис 1.3):

1) запис по рядках відповідно до ключа K_1;
2) читання по стовпцях відповідно до ключа K_2.

1	Н	Н	Я	П
2	Е	Р	Е	С
3	У	В	А	Н
4	Т	А	В	Л
5	Ш	И	Ф	Р
6	Е	Н	Н	Я
7	М	_	_	_
K_1/K_2	1	2	3	4

Криптограма: "ПСНЛРЯ_НРВАИН_ЯЕАВФН_НЕУТШЕМ".

Рис 1.3. **Матрична перестановка з подвійним ключем.**

Шифри перестановки зберігають усі букви відкритого тексту, але розміщують їх у криптотексті в іншому порядку.

Хоча багато сучасних алгоритмів використовують перестановку, із цим пов'язана проблема застосування великого обсягу пам'яті, а також іноді потрібна робота з повідомленнями певного розміру. Тому частіше використовують підстановочні шифри.

Підстановочні шифри

Підстановкою називається взаємооднозначне відображення f деякої кінцевої безлічі M на безліч M' або на себе. При цьому в підстановці беруть участь усі елементи множин M та M'.

Одноалфавітні шифри

Шифр простої заміни

У процесі шифрування здійснюється перетворення відкритого тексту M довжини l таким чином, що кожний символ заміняється на деякий інший. При цьому однаковим символам у відкритому тексті відповідають однакові символи криптотексту, а різним – різні. Ключем є таблиця, в якій установлюється правило заміни символів, тобто кожному символу a алфавіту A ($a \in \mathrm{A}$) ставиться у відповідність символ $b \neq a$ із цього ж алфавіту A.

Позначимо операцію переходу $\rightarrow$ й правило переходу має такий вигляд:

$$a_i, a_j \in \mathrm{A},\ a_i \to a_j, \text{ при } i \neq j,$$

де $i, j \in [0,...,|\mathrm{A}|]$; $|\mathrm{A}|$ – потужність алфавіту, тобто кількість елементів в алфавіті.

Візьмемо алфавіт української мови й позначимо його як алфавіт $\mathrm{A}_{ó}$

№	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathrm{A}_{ó}$	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м
K	й	ц	у	к	е	н	г	ш	з	щ	х	ґ	ф	ї	в	а	п

№	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
$\mathrm{A}_{ó}$	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	_
K	р	л	о	д	ж	є	я	␣	с	м	и	т	ь	б	ю	ч	і

Відкритий текст: `захист_інформації`
Криптограма: `щйсхжєіґр_лдпймґф`

Шифр Цезаря

Використовуємо алфавіт $\mathrm{A}_{ó}$, розглянутий у шифрі простої заміни:

№	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathrm{A}_{ó}$	А	Б	В	Г	Ґ	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М

№	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
$\mathrm{A}_{ó}$	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	_

Виберемо секретний ключ K, що представляється числом з діапазону $1 \le K \le \left|\mathrm{A}_{óêð}\right| - 1$. Як видно, кількість ключів залежить тільки від потужності алфавіту.

Шифрування відкритого повідомлення M у шифрі Цезаря виконується за літерами. Кожна літера заміщається на літеру, що знаходиться на K символів справа літери, що шифрується в алфавіті A. У випадку, якщо при шифруванні деякої літери на ключі K був досягнуть кінець алфавіту, то переходимо в його початок і продовжуємо зсув на кількість, що залишилася, символів із ключа. Приклад: шифрується буква «Х» на ключі $K = 20$, то криптограма дорівнює «И».

Дане перетворення легко описується операцією взяття за модулем потужності алфавіту. Одержуємо:

$$c_i = \left(J\left(m_i\right) + K\right) \bmod n,\ i = \overline{0, t-1},$$

де m_i – i-та літера відкритого тексту;

t – довжина повідомлення в символах;

$J\left(m_i\right)$ – функція, що обчислює порядковий номер букви m_i в алфавіті A;

n – кількість літер в алфавіті.

Розшифровування виконується у зворотному порядку, тобто буква відкритого тексту буде розташовуватися ліворуч на K символів в алфавіті A.

Математично дане перетворення представляється наступною формулою:

$$m_i = \left(J\left(c_i\right) - K\right) \bmod n,\ i = \overline{0, t-1},$$

де c_i – i-та літера криптограми;

t – довжина повідомлення в літерах;

$J\left(c_i\right)$ – функція, що обчислює порядковий номер букви c_i в алфавіті A;

n – кількість літер в алфавіті.

Афінна криптосистема

Узагальненням шифру Цезаря є афінна криптосистема, в якій також розглядаємо алфавіт A потужності n.

В афінній криптосистемі ключ складається із двох компонентів $K = \{a, b\}$, де числа a і b повинні задовольняти наступні умови:

1) $0 \le a, b \le n-1$;

2) числа a і n мають бути *взаємно простими,* тобто $НОД(a, n) = 1$.

Шифрування відкритого тексту виконується за наступною формулою:

$$c_i = \left(a \cdot J\left(m_i\right) + b\right) \bmod n,\ i = \overline{0, t-1};$$

розшифрування здійснюється за таким перетворенням:

$$m_i = \left(\left(J\left(c_i\right) - b\right) a^{-1}\right) \bmod n,\ i = \overline{0, t-1}$$

де a і b – компоненти ключа;

$J(m_i)$ – функція, яка обчислює порядковий номер літери m_i в алфавіті A;

n – кількість літер в алфавіті.

Елемент a^{-1} називається зворотним елементом a за модулем n та задовольняє рівність 1.2:

$$\left(a \cdot a^{-1}\right) \bmod n = 1, \qquad (1.2)$$

де a, a^{-1} – цілі числа, які належать множині цілих чисел $\{0,1,...,n-1\}$.

Обчислення зворотного елемента здійснюється методом перебору, в якому підбирається значення зворотного елемента a^{-1} з множини $\{0,1,...,n-1\}$, що задовольняє формулу (1.2).

Приклад

Обчислимо зворотний елемент до числа $a=3$ за модулем $n=11$. Зворотний елемент дорівнює $a^{-1}=4$.

Взаємна простота a й n необхідна для об'єктивності відображення, в іншому випадку можливі відображення різних символів в один, що призведе до неоднозначності дешифрування.

Шифр Цезаря з ключовим словом

У даному різновиді шифру Цезаря ключ K задається числом k $(0 \le k \le n-1)$ та коротким ключовим словом або пропозицією. Виписується алфавіт, а під ним, починаючи з k-ї позиції, ключове слово. Букви, що залишилися, записуються за абеткою після ключового слова. В результаті одержуємо підстановку для кожної букви. Вимога, щоб всі букви ключового слова були різними, не є обов'язковою - в цьому випадку необхідно записувати ключове слово без повторення однакових букв. Кількість ключів у системі Цезаря із ключовим словом дорівнює $n!$.

Шифр Плейфейера

Даний шифр був придуманий британським ученим сером Чарльзом Вітстоуном (Sir Charles Wheatstone) в 1854 р., однак за шифром закріпилося ім'я його друга – барона Плейфейера, що переконав британське міністерство закордонних справ використовувати цей шифр.

У данному шифрі алфавіт розташовується в матриці в довільному порядку і становить ключ K. Матриця може формуватися й на основі деякого секретного слова, що записується в матрицю зліва направо,

починаючи з першої комірки матриці. Повторювані літери ключового слова упускаються. Інші осередки заповнюються використаними літерами, що залишилися в алфавіті. Розмірність матриці підбирається така, щоб повністю вписати весь алфавіт. Для одержання зазначеної матриці алфавіт доповнюється розділовими символами або іншими унікальними символами.

Ключова матриця, що отримана на основі ключа «`криптоаналіз`», подана на рис 1.4.

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

Рис. 1.4. **Ключова матриця**

Відкритий текст M розбивається на пари символів $m_i m_{i+1}$. Кожна пара символів відкритого тексту заміняється на пари символів з матриці в такий спосіб:

1) якщо символи знаходяться в одному рядку, то кожний із символів пари заміняється на символ праворуч (за останнім символом у рядку йде перший символ цього рядка);

2) якщо символи знаходяться в одному стовпці, то кожний символ пари заміняється на символ, розташований нижче його (за останнім нижнім символом слідує верхній із цього стовпця);

3) якщо символи пари перебувають у різних рядках і стовпцях, то вони вважаються протилежними кутами прямокутника. Символ, що перебуває в лівому куті, заміняється на символ, що стоїть в іншому лівому куті; заміна символу, що знаходиться в правому куті, здійснюється аналогічно. Заміна виконується відповідно до порядку символів відкритої біграми. Приклад: пари символів відкритого тексту «ЗФ» заміняються на пари символів криптограми «ЧН»;

4) якщо у відкритому тексті зустрічаються два однакових символи підряд, то перед шифруванням між ними вставляється спеціальний символ (наприклад, тире або пробіл).

Шифр Плейфейера значно надійніший простих моноалфавітних шифрів. З одного боку, літер усього 26, а біграм – 36 × 36 = 1296, і вже по цьому ідентифікувати біграми складніше, ніж окремі літери.

Відкритий текст: "ШИФР_ПЛЕЙФЕЙЕРА_".

Матрицю алфавіту наведено на рис. 1.5.

ШИ	ОХ
ФР	ЬН
_П	ТЯ
ЛЕ	ҐЗ
ЙФ	ХЇ
ЕЙ	СҐ
ЕР	ТГ
А_	ЩЗ

Шифртекст: "ОХЬНТЯҐЗХЇСҐТГЩЗ"

Рис 1.5. **Шифртекст,отриманий шифром Плейфейера**

Методи розкриття одноалфавітних систем методом повного перебору ключів. Атака "brute force"

Незважаючи на свою простоту в реалізації, одноалфавітні системи шифрування дуже уразливі. Визначимо кількість різних шифрів в афінній системі. Кожний ключ повністю визначається парою цілих чисел a і b, що задають відображення $ax+b$. Для a існує $\phi(n)$ можливих значень, де $\phi(n)$ – функція Ейлера, що повертає кількість взаємно простих чисел з n і n значень для b, які можуть бути використані незалежно від a, за винятком тотожного відображення ($a=1$, $b=0$), що розглядатися не буде. У такий спосіб утворюється $\phi(n)(n-1)$ можливих значень, що не так і багато: при $n=33$ в якості a можуть бути 20 значень (1, 2, 4, 5, 7, 8, 10, 13, 14, 16, 17, 19, 20, 23, 25, 26, 28, 29, 31, 32), тоді загальне число ключів дорівнює 20×(33-1)=659. Перебір такої кількості ключів не буде важким при використанні комп'ютера. Але існують методи, які спрощують цей пошук і можуть бути використані при аналізі більш складних шифрів.

Частотний аналіз

Одним із таких методів є *частотний аналіз*. Його суть методу полягає в порівнянні розподілу літер у криптотексті з розподілом літер в алфавіті вихідного повідомлення. Літери з найбільшою частотою в криптотексті заміняються на літери з найбільшою частотою з алфавіту. Імовірність успішного розкриття підвищується зі збільшенням довжини криптотексту. Існує безліч різних таблиць про розподіл літер у тій або іншій мові (табл. 1.1), але жодна з них не містить остаточної інформації - навіть порядок літер може відрізнятися в різних таблицях. Розподіл літер дуже залежить від типу тесту: проза, розмовна мова, технічна мова та ін.

Таблиця 1.1

Таблиці розподілення літер у різних мовах

В українській мові					
Літера	Частота	Літера	Частота	Літера	Частота
А	0.070	Л	0.028	Ц	0.009
Б	0.010	М	0.033	Ч	0.011
В	0.046	Н	0.070	Ш	0.005
Г	0.013	О	0.082	Щ	0.003
Д	0.028	П	0.025	Ы	0.016
Е	0.043	Р	0.038	ь	0.015
Ж	0.008	С	0.036	Э	0.006
З	0.019	Т	0.051	Ю	0.009
И	0.056	У	0.027	Я	0.021
Й	0.007	Ф	0.005	_	0.134
К	0.036	Х	0.010	І	0,037
Ї	0,006	Ґ	0,000		
В російській мові					
А	0.062	Л	0.035	Ц	0.004
Б	0.014	М	0.026	Ч	0.012
В	0.038	Н	0.053	Ш	0.006
Г	0.013	О	0.090	Щ	0.003
Д	0.025	П	0.023	Ы	0.016
Е	0.072	Р	0.040	Ъ, Ь	0.014
Ж	0.007	С	0.045	Э	0.003
З	0.016	Т	0.053	Ю	0.006
И	0.062	У	0.021	Я	0.018
Й	0.010	Ф	0.002	_	0.174
К	0.028	Х	0.009		
В англійській мові					
A	0.0804	B	0.0154	C	0.0306
D	0.0399	E	0.1251	F	0.0230
G	0.0196	H	0.0549	I	0.0726
J	0.0016	K	0.0067	L	0.0414
M	0.0253	N	0.0709	O	0.0760
P	0.0200	Q	0.0011	R	0.0612
S	0.0654	T	0.0925	U	0.0271
V	0.0099	W	0.0192	X	0.0019
Y	0.0173	Z	0.0009		

Хоча немає таблиці, що може врахувати всі види текстів, але є параметри, загальні для всіх таблиць, наприклад, в англійської мові літера E завжди очолює список частот, а T перебуває на другій позиції. A і O майже завжди треті. Крім того, дев'ять літер англійської мови E, T, A, O, N, I, S, R, H завжди мають частоту вище, ніж у будь-які інші. Ці дев'ять літер заповнюють приблизно 70% англійського тексту. Нижче наведені відповідні таблиці для різних мов (табл. 1.2)

Таблиця 1.2

Таблиці найвагоміших (найбільш поширених) літер у різних мовах

Мова											
Російська		Англійська		Німецька		Французька		Італійська		Фінська	
Літера (Л)	**Частота (Ч)**	**Л**	**Ч**	**Л**	**Ч**	**Л**	**Ч**	**Л**	**Ч**	**Л**	**Ч**
о	0.1090	e	0.1251	e	0.1846	e	0.1587	e	0.1179	a	0.1206
е	0.0872	t	0.0925	n	0.1142	a	0.0942	a	0.1174	i	0.1059
а	0.0751	a	0.0804	i	0.0802	i	0.0841	i	0.1128	t	0.0976
и	0.0751	o	0.0760	r	0.0714	s	0.0790	o	0.0983	n	0.0864
н	0.0642	i	0.0726	s	0.0704	t	0.0726	n	0.0688	e	0.0811
т	0.0642	n	0.0709	a	0.0538	n	0.0715	l	0.0651	s	0.0783
с	0.0545	s	0.0654	t	0.0522	r	0.0646	r	0.0637	l	0.0586
р	0.0484	r	0.0612	u	0.0501	u	0.0624	t	0.0562	o	0.0554
в	0.0460	h	0.0549	d	0.0494	l	0.0534	s	0.0498	k	0.0520
∑	**0.6235**	∑	**0.6990**	∑	**0.7263**	∑	**0.7405**	∑	**0.7500**	∑	**0.7359**

Позначимо, що букви I, N, S, E, A (И, Н, З, Е, А) з'являються у високочастотному класі кожної мови. Також є таблиці частоти появи букв на початку й у кінці слова.

Найпростіший захист проти атак, заснованих на підрахунку частот, забезпечується в системі омофонів (HOMOPHONES) - однозвучних під-становочних шифрів, у яких один символ відкритого тексту відображається на кілька символів шифротексту, їх число пропорційне частоті появи букви. Шифруючи букву вихідного повідомлення, вибираємо випадково одну з її замін. Отже, простий підрахунок частот нічого не дає криптоаналітику. Однак доступна інформація про розподіл пар і трійок букв у різних природних мовах. Криптоаналіз, заснований на такій інформації, буде більш успішним.

Один із способів оцінки ефективності шифрів заснованих на підстановках або перестановках, показаний на рис. 1.6. Лінія, позначена

на рис. 1.6 як *відкритий текст,* відображає розподіл значень відносної частоти входження символів англійського алфавіту в статті *Encyclopedia Britannica,* що присвячена криптології й утримує більше 70 000 символів. Подібний графік характерний для розподілу відносної частоти появи символів і для будь-якого моноалфавітного шифру. Сам графік утворюється в такий спосіб. Число входжень літери в тексті ділиться на число появ у тексті символу «e» (найбільш часто використовуваний символ в англійській мові). У результаті «e» має відносну частоту 1, «t» – близько 0,76 і т. д. Розподілу на горизонтальній осі відповідають букви у порядку зниження значень відносної частоти їхньої появи.

На рис. 1.6 також показаний графік розподілу значень частоти для текстів, шифрованих за допомогою шифру Плейфейера. З метою нормалізації число появ у шифрованому тексті тієї або іншої букви ділилося на число входжень букви «e» у відкритому тексті. Отримані в результаті нормалізації графіки показують, наскільки частота розподілу букв (при використанні якої розкриття, наприклад, підстановочних шифрів виявляється зовсім простою справою) маскується шифруванням. Якщо в процесі шифрування інформація про розподіл повністю ховається, та графік для шифрованого за допомогою такого шифру тексту повинен становити горизонтальну пряму лінію, а криптоаналіз такого тексту з використанням лише шифрованого тексту, очевидно, повинен виявитися практично неможливим. Як видно з рис. 1.6, шифр Плейфейера має більш пологий графік розподілу значень частоти порівняно з відкритим текстом, але все-таки надає криптоаналітику досить широкі можливості для статистичного аналізу збережених структур [1].

У випадку перестановочних шифрів частота символів криптотексту точно збігається із частотою символів відкритого тексту, що приводить до повного збігу графіків. Це дає криптоаналітику інформацію про те, що в шифрі як криптографічне перетворення брала участь перестановка, тобто шифр перестановочний. Відновити відкритий текст не вийде, тому що в частотному аналізі немає інформації про позиції символів як у відкритому тексті, так і в криптограмі. Застосування до криптотексту другого перестановочного перетворення значно підвищить безпеку. Існують і ще більш складні перестановочні шифри, але із використанням комп'ютера можна розкрити майже всі з них.

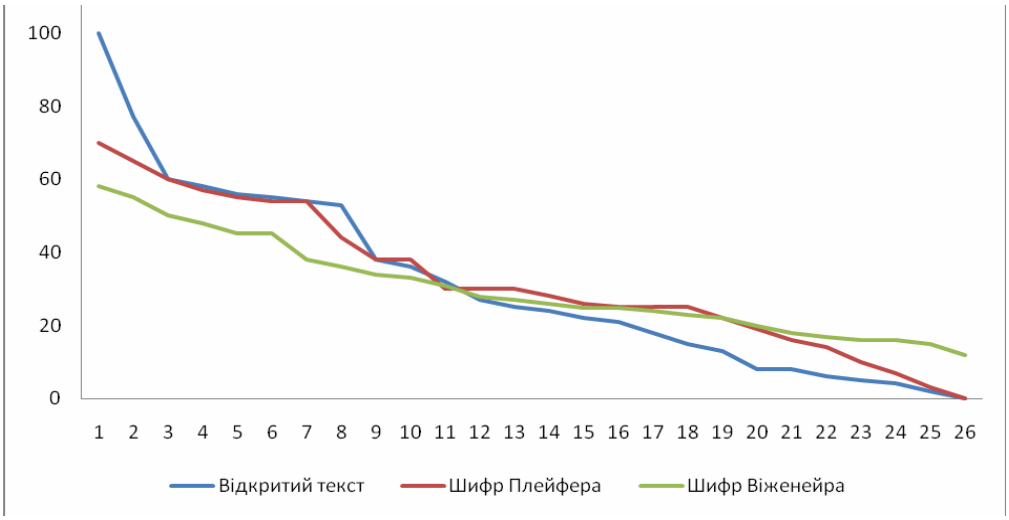

Рис. 1.6. **Відносні частотні графіки відкритого та зашифрованого тексту**

Богатоалфавитні шифри (поліалфавітні)

Поліалфавітні підстановочні шифри були винайдені Ліном Баттістой (Lean Battista) в 1568 році. Основна ідея багатоалфавітних систем полягає в тому, що протягом усього тексту та сама буква може бути зашифрована по-різному. Тобто заміни для букви вибираються з багатьох алфавітів залежно від положення в тексті. Це є гарним захистом від простого підрахунку частот, тому що не існує єдиного маскування для кожної букви в криптотексті. У даних шифрах використовуються множинні однобуквені ключі, кожен з яких застосовується для шифрування одного символу відкритого тексту. Першим ключем шифрується перший символ відкритого тексту, другим - другий і т.д. Після використання всіх ключів вони повторюються циклічно.

Шифр Віженера

Однією з найбільш старших і найбільш відомих багатоалфавітних криптосистем є система Віженера, названа на честь французького криптографа Блейза Віженера (Vigenere). Цей метод був уперше опублікований у 1586 році. У даному шифрі ключ K задається набором з d літер, що приналежать алфавіту А:

$$K = k_0 k_1 ... k_{d-1}, \text{ де } k_i \in \text{A} .$$

Далі набори підписуються з повторенням під повідомленням M:

$$\begin{array}{rcccccccc} M & = & m_0 & m_1 & \dots & m_{d-1} & m_d & \dots & m_t; \\ K & = & k_0 & k_1 & \dots & k_{d-1} & k_0 & \dots & k_{t\,(\mathrm{mod}\,d)}. \end{array}$$

Отриману послідовність складають із відкритим текстом за модулем потужності алфавіту $n=|\mathrm{A}|$. Тобто утворюється наступна формула:

$$C_i\left(M^l,K^d\right)=\left(J\left(m_i\right)+J\left(k_{i\bmod d}\right)\right)(\mathrm{mod}\,n),\ i=\overline{1,t}.$$

Також букву шифротексту можна знаходити з наступної таблиці (табл. 1.3) як перетинання стовпця, обумовленого буквою відкритого тексту, і рядка, обумовленого буквою ключа.

У випадку, якщо ключ K складається з одного символу, $d=1$, то одержуємо класичний шифр Цезаря.

Повторне застосування двох або більше шифрів Віженера буде називатися *складовим шифром Віженера*. Він має рівняння:

$$C_i^*\left(M^l,K_j^{d_j}\right)=\left(J\left(m_i\right)+J\left(k_{0,i\bmod d_0}\right)+J\left(k_{1,i\bmod d_1}\right)+\ldots+J\left(k_{j,i\bmod d_j}\right)\right)\mathrm{mod}\,n,\ i=\overline{1,t},$$

де $K_j^{d_j}=\left\{K_0^{d_0},K_1^{d_1},\ldots,K_j^{d_j}\right\}$ – множина ключів, які мають різні періоди $d_0,d_1,\ldots,d_j$ відповідно.

Шифр із автоключем з використанням відкритого тексту

Подальшою модифікацією системи Віженера є система шифрів з *автоключем (auto-key),* що приписується математикові XVI с. Дж. Кардано, AUTOCLAVE. Шифрування починається з використанням "первинного ключа" (який є справжнім ключем у нашому значенні) й доповнюється з використання повідомлення, зміщеного на довжину первинного ключа, потім виконується додавання за модулем n, який дорівнює потужності алфавіту A.

Перетворення відкритого тексту в криптограму здійснюється за формулою:

$$C_i\left(M^l,K^d\right)=\begin{cases}\left(J\left(m_i\right)+J\left(k_i\right)\right)\mathrm{mod}\,n, & i<d;\\ \left(J\left(m_i\right)+J\left(m_{i-d}\right)\right)\mathrm{mod}\,n, & i\geq d.\end{cases}$$

Розшифрування виконується за формулою:

$$M_i\left(C^l,K^d\right)=\begin{cases}\left(J\left(c_i\right)-j\left(k_i\right)\right)\mathrm{mod}\,n, & i<d;\\ \left(J\left(c_i\right)-J\left(m_{i-d}\right)\right)\mathrm{mod}\,n, & i\geq d.\end{cases}$$

Таблиця 1.3

Приклад таблиці Віженера (для російського алфавіту)

Буквы ключа	Буквы открытого текста																														
	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А
	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б
	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В
	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г
	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д
	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е
	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж
	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З
	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И
	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й
	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К
	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М
	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н
	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы
	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь
	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э
	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю

Наприклад:

Повідомлення M	П Р И В Е Т П Р И М А Т У
Первинний ключ K	В Г П У
Автоключ	П Р И В Е Т П Р И
Шифротекст	С У Ч Х Ф В Ч Т Н Ю П В Ы

Розшифрування не є складним: за первинним ключем K^d розшифровується d перших символів повідомлення, після чого знайдена частина вихідного повідомлення використовується як ключ. Друга частина процесу розшифровки повторюється доти, доки не буде досягнутий кінець криптограми.

Шифр із автоключем з використанням криптограми

Як і в попередньому алгоритмі, шифрування здійснюється із застосуванням "первинного ключа" K, а потім триває за допомогою отриманої криптограми $c_0, c_1, \ldots$ при використанні "первинного ключа". Для цього алгоритму перетворення відкритого тексту в криптограму здійснюється за такою формулою:

$$C_i\left(M^l, K^d\right) = \begin{cases} \left(J\left(m_i\right) + J\left(k_i\right)\right) \bmod n, & i < d; \\ \left(J\left(m_i\right) + J\left(c_{i-d}\right)\right) \bmod n, & i \geq d. \end{cases}$$

Розшифрування відбувається за формулою:

$$M_i\left(C^l, K^d\right) = \begin{cases} \left(J\left(c_i\right) - J\left(k_i\right)\right) \bmod n, & i < d; \\ \left(J\left(c_i\right) - J\left(c_{i-d}\right)\right) \bmod n, & i \geq d. \end{cases}$$

Поліалфавітна заміна

Даний клас шифрів об'єднав у собі два види математичних перетворень: перестановки f і підстановки g. За допомогою операції перестановки формується перша частина ключа шифру, ключова матриця підстановки, що складається з декількох різних функцій f_i. Кожна з функцій становить перестановку алфавіту A. Формування ключової матриці підстановки здійснюється випадковим способом.

Нижче сформовані чотири функції f_0, f_1, f_2, f_2:

№	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	31	32	33
$\mathrm{A}_{б}$	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	_
$f_0(x)$	й	ц	у	к	е	н	г	ш	щ	з	х	ї	ф	і	в	а	п	р	о	л	д	ж	є	я	ч	с	м	и	т	ь	б	ю	_	ґ
$f_1(x)$	м	и	т	ь	б	ю	й	ц	у	к	е	н	ґ	ш	щ	з	х	_	ф	і	в	а	п	р	о	л	д	ж	є	я	ч	с	ї	г
$f_2(x)$	р	о	л	д	ж	є	я	ч	с	м	и	т	ь	б	ю	й	ц	у	к	е	н	г	ш	щ	з	х	ґ	ф	_	в	а	п	і	ї
$f_3(x)$	ш	щ	ґ	х	_	ф	і	в	а	п	р	о	л	д	м	и	т	ь	б	ю	й	ц	у	к	е	н	г	ж	ї	я	ч	с	є	з

Друга частина ключа – це функція підстановки g, що визначає, за допомогою якої функції f будуть шифруватися символи відкритого тексту. Довжина функції g може бути будь-якою. Наприклад: для чотирьох функцій f_i, $i=\overline{1,n}$, функція підстановки може бути рівної $g=\{1,3,0\}$, $g=\{1,0,3,2,0,3\}$. Найбільш оптимально її підбирати кратній довжині повідомлення.

Ключ шифрування K представлений перестановками f_0, f_1, f_2, f_2 і підстановкою $g=\{1,3,0,2,3\}$ довжиною $s=5$.

Шифрування повідомлення здійснюється за правилом:

$$C_i(M,F,g)=f_{g(i \bmod s)}(m_i);$$

розшифровування повідомлення виконується за правилом:

$$M_i(C,F,g)=f_{g(i \bmod s)}(c_i).$$

1.4. Завдання до лабораторної роботи

1. Виконати шифрування свого прізвища, ім'я та по батькові за всіма розглянутими у п.1.3 методами шифрування.
2. Здійснити розшифрування свого прізвища, ім'я та по батькові за всіма розглянутими у п.1.3 методами шифрування.
3. У звіт включити опис усіх дій, як при шифруванні, так і при розшифруванні.
4. Провести оцінку криптографічної стійкості шифрів на основі порівняння множини ключів (кількості) K і множини одержуваних криптограм C. Завдання виконати відповідно до варіанта (табл. 1.4).
5. Порівняти статистичну залежність криптограм і відкритого тексту.
6. Додаткове завдання: створити програму, яка виконує шифрування та розшифрування тексту за методами відповідно варіанта (табл. 1.4)

Таблиця 1.4

Варіанти додаткового завдання

Варіанти	Метод шифрування
1	Шифр Плейфейера. Поліалфавітна заміна
2	Перестановочний шифр із ключовим словом. Шифр із автоключем з використанням криптограми
3	Шифр простої заміни. Шифр із автоключем з використанням відкритого тексту
4	Афінна криптосистема. Поліалфавітна заміна
5	Шифр Цезаря. Шифр Віженера
6	Шифр Цезаря із ключовим словом. Шифр із автоключем з використанням відкритого тексту
7	Матрична перестановка. Поліалфавітна заміна
8	Шифр Плейфейера. Шифр із автоключем з використанням криптограми
9	Перестановочний шифр із ключовим словом. Поліалфавітна заміна
10	Шифр простої заміни. Шифр Віженера
11	Афінна криптосистема. Шифр із автоключем з використанням відкритого тексту
12	Шифр Цезаря. Шифр із автоключем з використанням криптограми

1.5. Контрольні запитання

1. Що таке шифр і шифрування?
2. Що таке конфіденційна інформація?
3. Дайте визначення поняттю «конфіденційність».
4. Розкрийте суть процесу шифрування й розшифрування повідомлень і роль криптоаналітика.
5. Як можна визначити криптографічну стійкість за криптограмою для простих шифрів?
6. Розкрийте сутність частотного криптоаналізу простих шифрів.
7. Що таке перестановка? Які прості шифри її використовують? Яким чином?
8. Що таке підстановка? Які прості шифри її використовують? Яким чином?
9. Яка існує класифікація простих шифрів? Дайте характеристику кожного із класів.

10. Які характеристики повинен мати шифр, щоб протистояти частотному криптоаналізу?

2. 2. Дослідження сучасних асиметричних криптосистем шифрування. Алгоритм RSA.

2.1. Мета. Одержання практичних навичок використання, механізмів асиметричного шифрування, що реалізують послугу безпеки конфіденційності. Дослідження алгоритму RSA.

2.2. Рекомендації щодо підготовки до виконання ЛР

Необхідно вивчити принципи асиметричних криптоперетворень та логіку роботи алгоритму RSA.

2.3. Загальні положення ЛР

Розвиток основних типів криптографічних протоколів (ключовий обмін, електронно-цифровий підпис, автентифікація) був би неможливий без створення відкритих ключів і побудованих на їх основі асиметричних алгоритмів шифрування.

З одного боку, ідея асиметричних алгоритмів тісно пов'язана з розвитком теорії односторонніх функцій, з іншого – з теорією складності. Під односторонньою функцією розуміється легкообчислювальне відображення $f(x): X \to Y$, $x \in X$, при цьому зворотне відображення є складною задачею. Вона називається важкообчислювальною, якщо немає алгоритму для її вирішення з поліноміальним часом роботи. Легкообчислювальною називають задачу, що має алгоритм з часом роботи, представленим у вигляді полінома низького ступеня щодо вхідного розміру задачі, а ще краще алгоритм з лінійним часом роботи.

На сьогоднішній день теоретично не доведено існування односторонніх функцій. Використання їх як основи асиметричних алгоритмів шифрування допустимо тільки до тих пір, поки не знайдені ефективні алгоритми, що виконують звернення односторонніх функцій за поліноміальний час.

Подальшим розвитком односторонніх функцій є побудова односторонніх *функцій із секретом.* Такою функцією називається

$f(x) = y$, значення якої, як і в попередньому випадку, легко обчислити, тоді як зворотне значення без знання деякого секрету важко обчислити. Знання ж секрету дозволяє досить просто реалізовувати операцію звернення односторонніх функцій із секретом. На практиці при застосуванні асиметричного алгоритму шифрування в ролі секретного ключа виступає саме знання секрету, а в ролі відкритого ключа – знання процедури обчислення односторонньої функції з секретом.

Разом з тим необхідно відзначити, що стійкість більшості сучасних асиметричних алгоритмів базується на двох математичних проблемах, які на даному етапі є важкообчислюваними навіть для методу «грубої сили»:

дискретне логарифмування в кінцевих полях;

факторизація великих чисел.

Оскільки на сьогоднішній день не існує ефективних алгоритмів вирішення даних завдань або їх вирішення вимагає залучення великих обчислювальних ресурсів або тимчасових витрат, ці математичні задачі знайшли широке застосування в побудові асиметричних алгоритмів. Їх стійкість розглядається як можливість звести проблему розкриття алгоритмів до вирішення однієї з вищеперелічених математичних задач.

Алгоритми шифрування з відкритим ключем залежать від одного ключа для шифрування й іншого, пов'язаного з першим, ключа для дешифрування. Ці алгоритми мають наступну важливу особливість:

з погляду обчислень нереально визначити ключ дешифрування, знаючи тільки використовуваний криптографічний алгоритм і ключ шифрування.

будь-який із цих двох зв'язаних ключів може служити для шифрування, і тоді інший може застосовуватися для дешифрування.

На рис. 2.1 наведено загальну схему процесу шифрування з відкритим ключем, яка виглядає таким чином:

1. Кожна кінцева система в мережі генерує пару ключів для шифрування і дешифрування отримуваних повідомлень.

2. Кожна з систем публікує свій ключ шифрування, розміщуючи його ключ у відкритому для всіх реєстрі або файлі. Це і є відкритий ключ. Другий ключ, що відповідає відкритому, залишається в особистому володінні.

3. Якщо користувач A збирається послати повідомлення користувача, він шифрує повідомлення, використовуючи відкритий ключ користувача $K_{â}^{B}$ ст.

4. Коли користувач B отримає повідомлення, він дешифрує його за допомогою свого особистого ключа. Інший одержувач не зможе дешифрувати повідомлення, оскільки особистий ключ K_{o}^{B} знає тільки він.

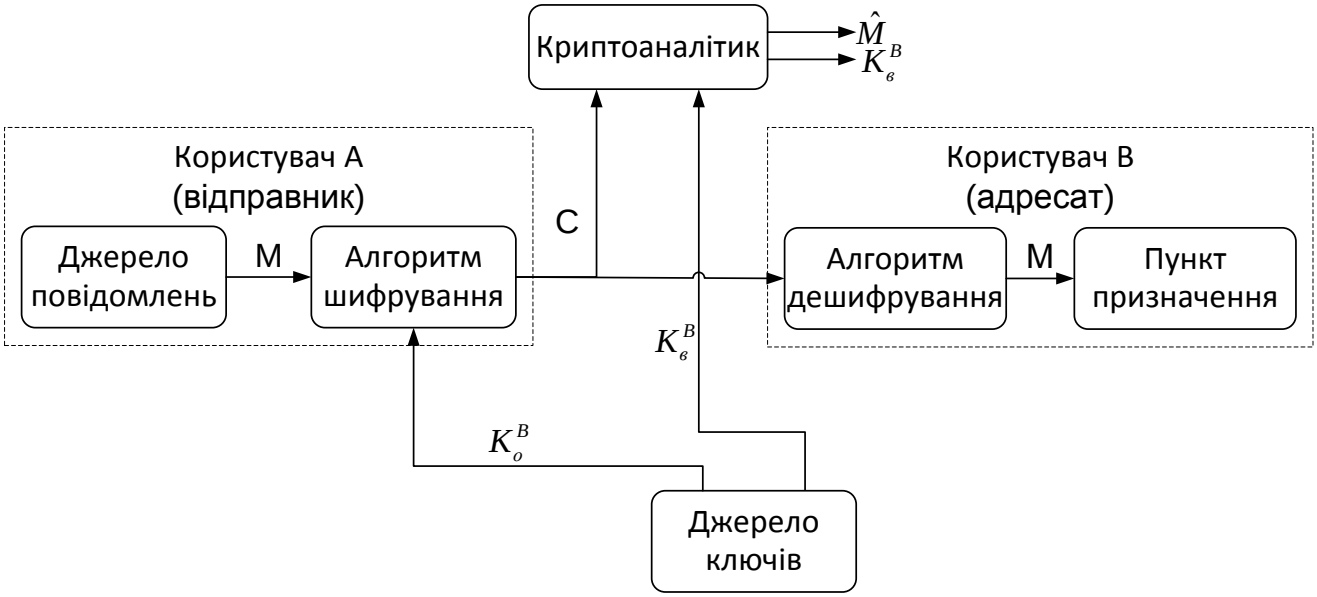

Рис. 2.1. **Загальна схема процесу шифрування з відкритим ключем**

У табл. 2.1 наведене порівняння деяких важливих характеристик симетричного шифрування та шифрування з відкритим ключем.

Для користувача A (відправника) його особистий ключ позначається як $K_{â}^{A}$, а відповідний особистий ключ – $K_{î}^{À}$. Для користувача B (адресата) існує відповідна пара ключів $\left\{K_{â}^{B}, K_{î}^{B}\right\}$. Шифрування відкритого тексту M виконується на відкритому ключі (адресата) й позначається як $E_{K_{î}^{B}}\left(M\right)$. Розшифрування шифротексту C виконується на особистому ключі користувача і позначається $D_{K_{â}^{B}}\left(C\right)$.

Таблиця 2.1

Симетричне шифрування й шифрування з відкритим ключем

Симетричне шифрування	Шифрування з відкритим ключем
Необхідно для роботи	
1. Один алгоритм з одним і тим же ключем служить як для шифрування, так для розшифрування	1. І для шифрування, і для дешифрування використовується один алгоритм, але два ключі: один – для шифрування, а інший – для розшифрування
2. Відправник і одержувач повинні використовувати однаковий алгоритм та ключ	2. Відправник і одержувач повинні мати по одному з пари відповідних ключів
Необхідно для захисту	
1. Ключ має зберігатися в секреті	1. Один з двох ключів має зберігатися в секреті
2. Повинно бути неможливо або принаймні практично неможливо розшифрувати повідомлення за відсутності додаткової інформації	2. Повинно бути неможливо або принаймні практично неможливо розшифрувати повідомлення за відсутності додаткової інформації

Стандарт асиметричного шифрування RSA

Найпоширенішим алгоритмом асиметричного шифрування є алгоритм RSA, названий за першими буквами імен його творців (Rivest, Shamir, Adleman). Розробникам даного алгоритму вдалося ефективно втілити ідею односторонніх функцій із секретом. Стійкість RSA базується на складності факторизації великих цілих чисел.

У 1993 році метод RSA був обнародуваний і прийнятий як стандарт (PKCS # 1: RSA Encryption Standard). RSA можна застосовувати як для шифрування/розшифрування, так і для генерації/перевірки електронно-цифрового підпису (ЕЦП).

Генерація ключів.

Кожен учасник інформаційного обміну генерує пару ключів (відкритий і секретний) відповідно до таких правил:

1. Вибираються два великих простих цілих числа p і q приблизно однакового розміру. Вибір чисел p і q визначається наступними міркуваннями:

збільшення порядку чисел веде до уповільнення операції шифрування/розшифрування;

збільшення порядку чисел p і q веде до збільшення стійкості алгоритму, тому при виборі чисел слід керуватися практичною необхідністю. На практиці зазвичай рекомендується вибирати числа, що містять близько 1500–4096 бітів.

2. Обчислюється модуль системи $n = p \cdot q$ і $\phi(n) = (p-1)(q-1)$ – функція Ейлера.

3. Вибирається достатньо велике число e, що задовольняє умову $1 < e \le \phi(n)$, і взаємно просте з $\phi(n)$, тобто $НОД(e, \phi(n)) = 1$.

4. Використовуючи розширений алгоритм Евкліда, обчислюється велике ціле число d, що відповідає умові:

$$ed \equiv 1 (\mathrm{mod}\, \phi(n)),\ 1 < d < \phi(n).$$

Таким чином, секретним ключем є пара чисел (n, d), а відкритим – пара чисел (n, e). Відкритий ключ поміщається в загальнодоступний довідник.

Шифрування/розшифрування

Після вибору параметрів системи $\{n, e, d\}$, тобто $K_A^B = e$ і $K_I^B = d$, абонент B готовий до прийому зашифрованих повідомлень. Їх передача складається з наступних кроків:

1. Вхідне повідомлення розбивається на блоки $m_i \le 2^{\lfloor \log_2 n \rfloor}$, *де* $\lfloor \cdot \rfloor$ – округлення до найближчого цілого знизу.

2. Обчислюється криптограма $c_i = m_i^e \bmod n$.

3. Значення c_i, яке є зашифрованим блоком повідомлення, посилається по відкритому каналу передачі даних.

4. Розшифрування полягає в обчисленні значення $m_i = c_i^d \bmod n$, використовуючи особистий ключ адресата.

2.4. Завдання до лабораторної роботи

1. Використовуючи програму «Mathematic 6.0» зашифрувати та розшифрувати повідомлення, яке містить П.І.Б. студента.

У пакеті «Mathematic 6.0» кожна команда виконується після виділення її та натискання клавіш «Shift+Enter». Після чого з'являється результат обчислень, як наведено на рис. 2.2.

Рис. 2.2. **Приклад обчислень у пакеті «Mathematic 6.0»**

2. За допомогою пакета «Mathematic 6.0» виконати розрахунок шифрування та розшифрування повідомлення, яке містить П.І.Б. студента. Основні функції, що необхідні для шифрування/дешифрування в пакеті «Mathematic 6.0»:

ToCharacterCode["*string*"]
Повертає список цілих кодів, відповідних символам у рядку «string».
Mod[*m*,*n*]
Повертає залишок ділення m ***на*** n.
NextPrime[n]
Повертає наступне просте число, більше за n.
RandomInteger[{$i_{\max}$}]
Повертає псевдовипадкове число в інтервалі $\{0,\ldots,i_{\max}\}$.
PowerMod[a,b,m]
Повертає $a^b \bmod m$.
PowerMod[a,-1,m]
Знаходить зворотний елемент за модулем m.
GCD[n,b]
Повертає найбільш спільний дільник двох чисел a **і** b.

Формування рядка повідомлення подано на рис. 2.3.

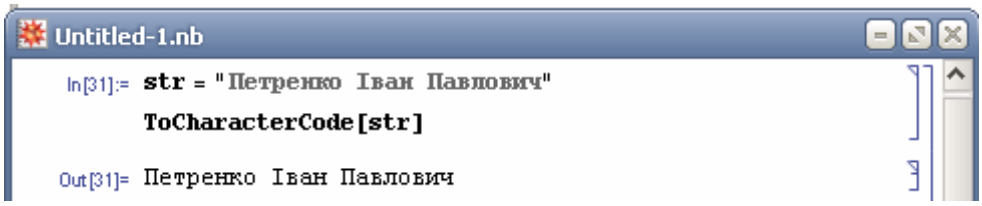

Рис. 2.3. **Рядок відкритого тексту**

Формування параметрів системи шифрування для алгоритму RSA наведено на рис. 2.4.

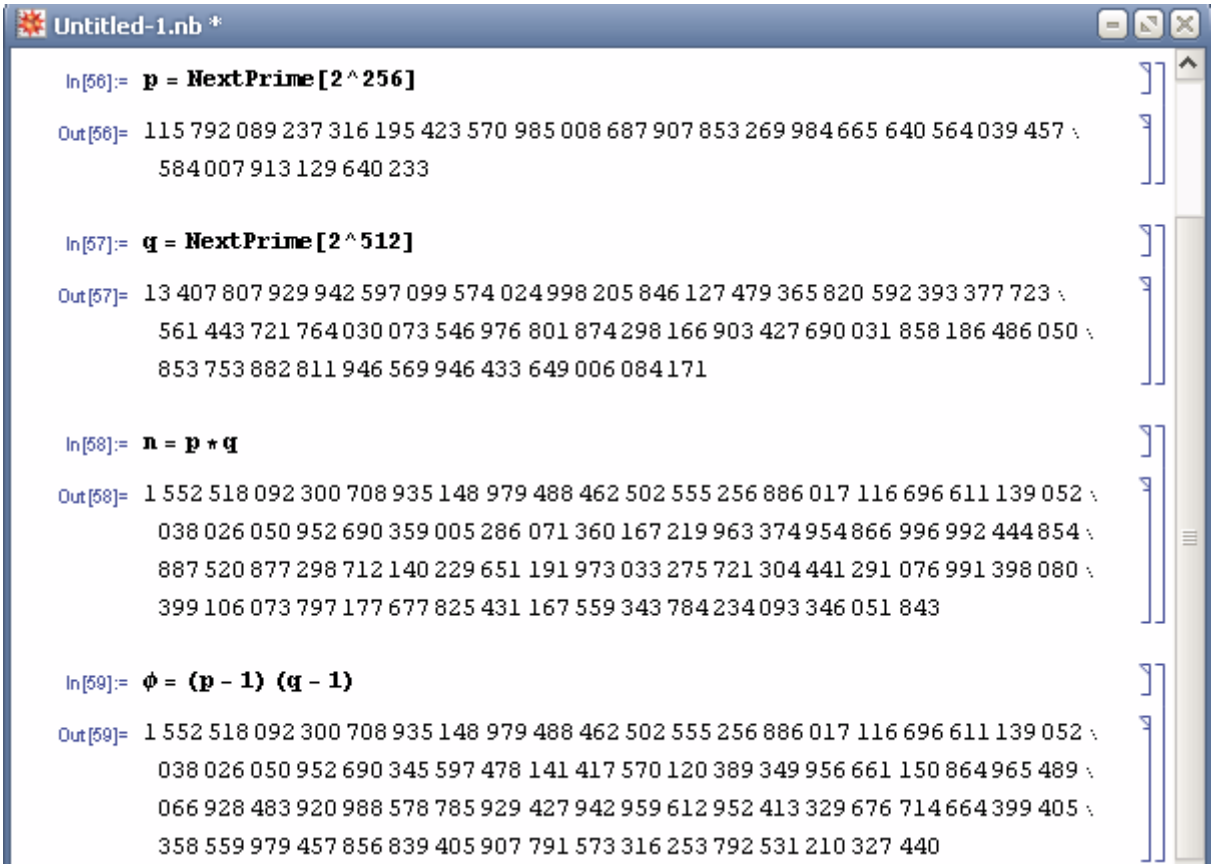

Рис. 2.4. **Формування параметрів RSA: прості числа p, q, модуль перетворення n та функція $\phi(n)$**

Далі генеруємо пару ключів – особистий та відкритий. Особистий ключ d генерується випадково, що задовольняє умову $\text{НСД}(e,\phi(n))=1$. Відкритий ключ e обчислюється як зворотний елемент поля за допомогою функції PowerMod[d,-1,$\phi(n)$]. Порядок генерування проілюстровано на рис. 2.5.

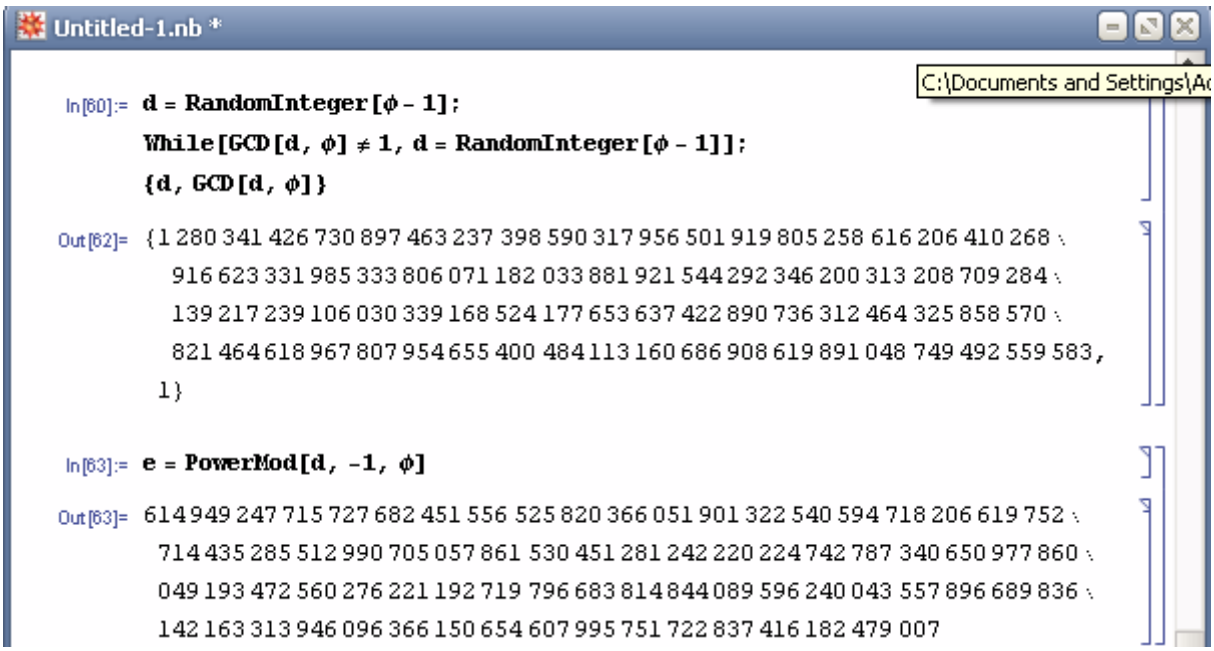

Рис. 2.5. **Генерування пари ключів** $\{e,d\}$

Шифрування повідомлення виконується за допомогою відкритого ключа адресата. Обчислення здійснюється за допомогою функції PowerMod[M_i, d, n] модульного піднесення у степінь (рис. 2.6).

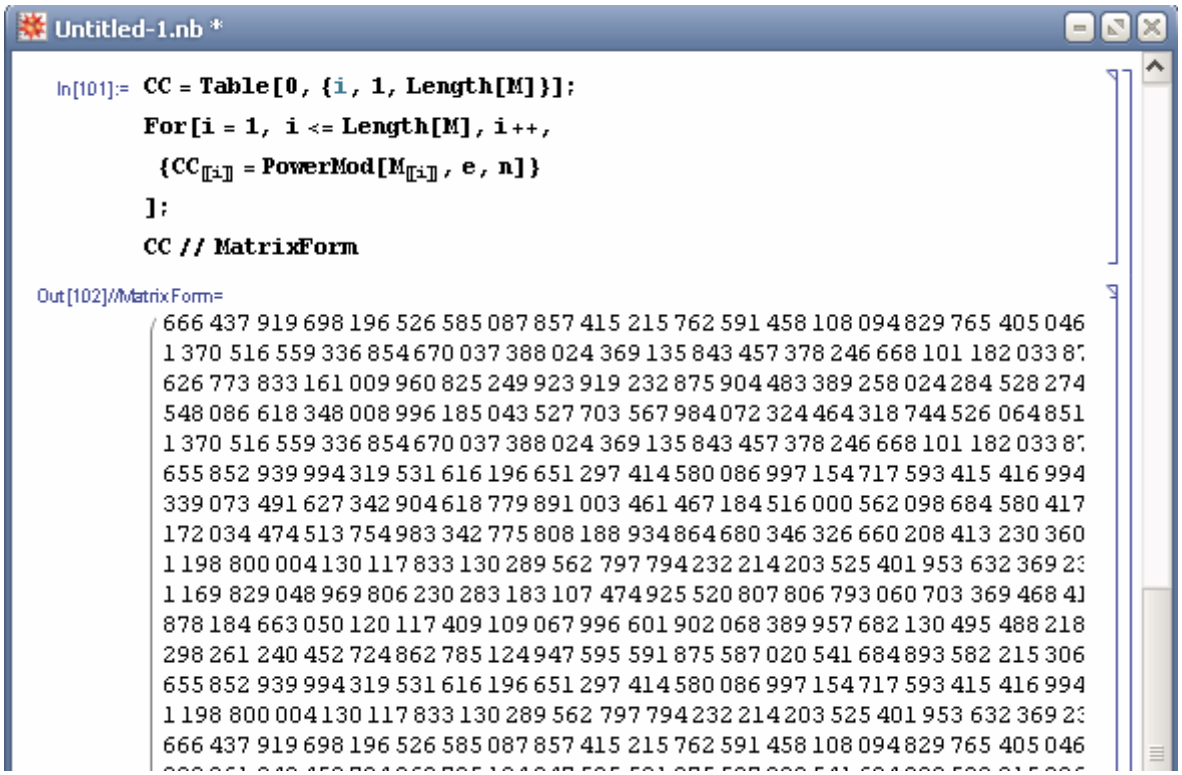

Рис. 2.6. **Формування криптограми**

Розшифровування (рис. 2.7) здійснюється за допомогою особистого ключа адресата d.

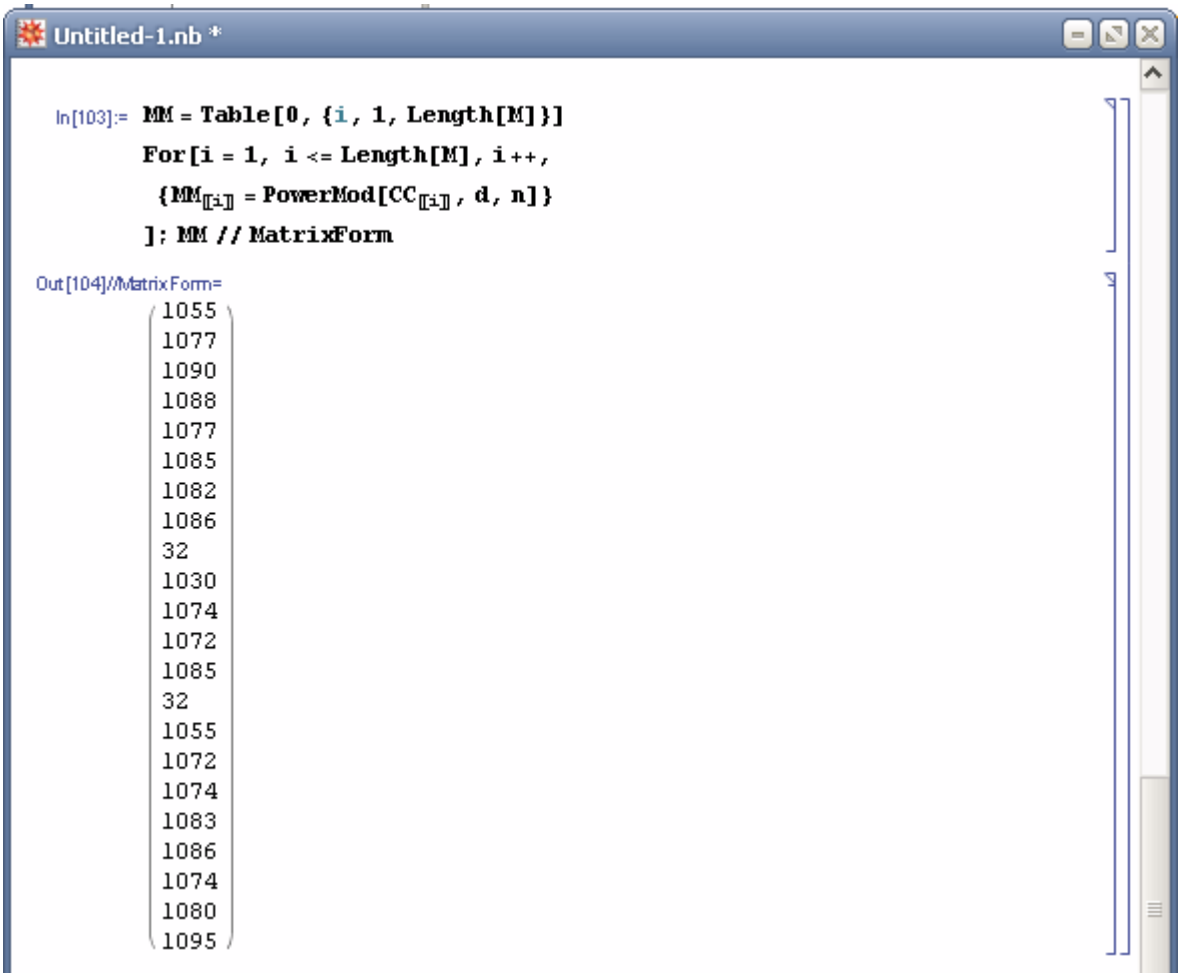

Рис. 2.7. **Розшифрування шифротексту**

Завдання необхідно виконувати відповідно до варіантів, які наведено в табл. 2.2.

Таблиця 2.2

Варіанти індивідуального завдання

№ вар.	Порядок простого числа q (бітів)	Порядок простого числа p (бітів)
1	2	3
1.	896	768
2.	864	832

Закінчення табл. 2.2

1	2	3
3.	832	896
4.	800	960
5.	768	1024
6.	736	1088
7.	704	1152
8.	672	1216
9.	640	1280
10.	608	1344
11.	576	1408
12.	544	1472
13.	512	1536
14.	480	1600
15.	448	1664
16.	416	1728
17.	384	1792
18.	352	1856
19.	320	1920
20.	288	1984

2.5. Контрольні запитання

1. Що таке відкритий ключ?
2. Що таке особистий ключ?
3. Розкрийте сутність асиметричного шифрування.
4. Обґрунтуйте критерії безпеки для формування загально системних параметрів у алгоритмі RSA.
5. Чим відрізняється асиметричне шифрування від симетричного?
6. Опішить послідовність генерації ключів в алгоритмі RSA.
7. Назвіть важкообчислювальні функції та обґрунтуйте їх властивості.
8. Назвіть функції з секретом та їх властивості.

3. Дослідження алгоритму несиметричного цифрового підпису Ель-Гамаля

3.1. Мета. Закріпити теоретичні знання й набути навичок відносно застосування та дослідження систем цифрового підпису з використанням несиметричних криптоперетворень.

3.2. Рекомендації щодо підготовки до виконання ЛР

При підготовці до лабораторної роботи необхідно:

вивчити основні поняття і визначення з питань автентифікації;

вивчити систему автентифікації, що базується на цифровому підписі Ель-Гамаля;

ознайомитися з описом лабораторної роботи та її програмним забезпеченням;

підготувати бланк звіту згідно з розділом "Зміст звіту";

підготувати відповіді на контрольні запитання.

3.3. Загальні положення лабораторної роботи

Рукописні підписи використовуються як доказ авторства паперового документа або принаймні згоди з ним і володіють наступними властивостями:

1. Підпис достовірний. Він переконує одержувача документа в тому, що той, хто підписав, свідомо це зробив.

2. Підпис непідроблений. Він доводить, що саме підписано, і ким саме підписано документ.

3. Підпис не може бути використаний повторно. Він є частиною документа; шахрай не зможе перенести підпис на інший документ.

4. Підписаний документ не можна змінити. Після того, як документ підписаний, його неможливо змінити.

5. Від підпису неможливо відректися. Підпис і документ матеріальні. Той, хто підписав, не зможе згодом стверджувати, що він не підписував документ.

Цифровий підпис (ЦП) повинен володіти тими ж властивостями, що і рукописний. На відмінну від несиметричного шифрування ЦП реалізує послуги безпеки цілісності й автентичності.

Відправник A використовує свою пару ключів $\left\{K_o^A, K_{\hat{a}}^A\right\}$. Накладення підпису виконується на особистому ключі відправника, а перевірка

адресатом – на відкритому ключі. На рис. 3.1 наведено схему використання ключів у цифровому підписі.

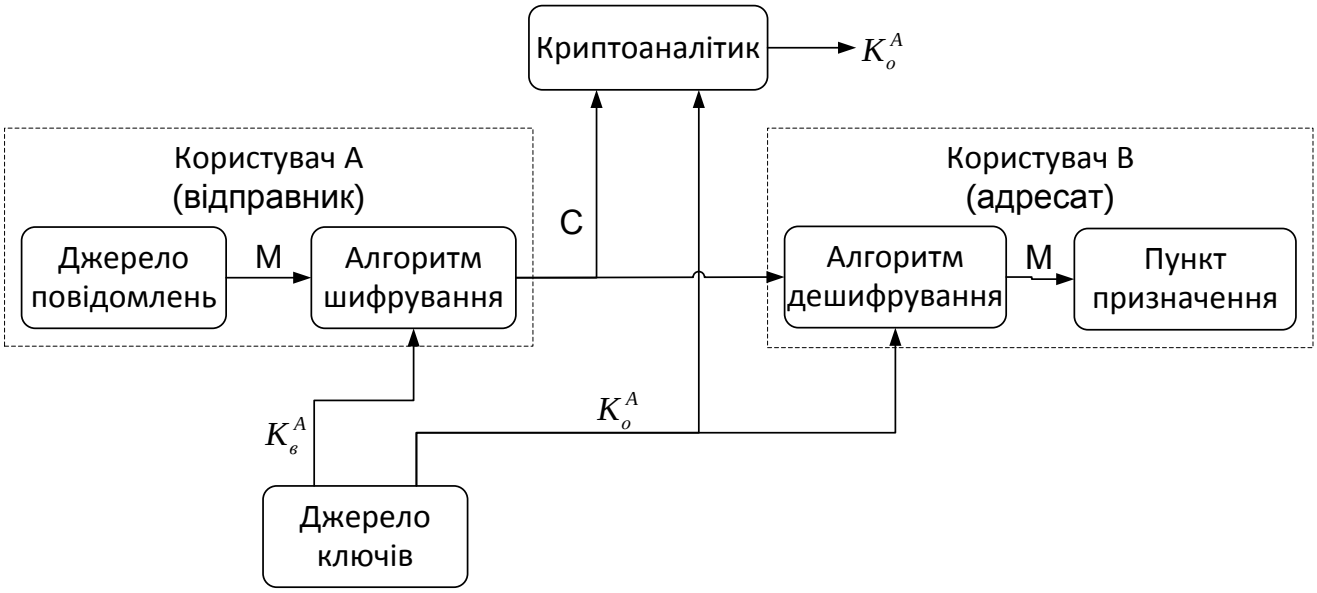

Рис. 3.1. **Криптосистема з відкритим ключем: автентифікація**

Цифровий підпис – цифровий еквівалент підпису, наявність якого в повідомленні дозволяє з високою вірогідністю визначити джерело цього повідомлення і юридично довести, що з деякою вірогідність $Ð_á$ саме це джерело породило дане повідомлення. Але за умови, що ймовірність підробки ЦП криптоаналітиком не перевищує допустимого значення $Ð_â$.

Цифровий підпис є зашифрованою сукупністю даних, що містять:

дані відправника;

дані одержувача;

час створення підпису;

контрольну суму файлу;

підпис відправника.

Цифровий підпис Ель-Гамаля

Система електронного цифрового підпису (ЕЦП), установлена ГОСТ Р 34.10-94, базується на методах криптографічного захисту даних з використанням хеш-функції.

Просте число q повинно мати довжину від 512 до 1024 бітів.

Просте число p – довжину від 1024 до 2048 битів, причому число $(p-1)$ містить множник q.

Число a, $1<a<p-1$,

$$a^q \pmod p = 1.$$

Секретний ключ підпису x – випадкове ціле число, що належить інтервалу $(0,q)$.

Відкритий ключ підпису y обчислюється за формулою:

$$y = a^x \pmod p.$$

Алгоритм формування ЕЦП

1. Обчислити хеш-функцію повідомлення $H(M)$ довжиною 256 бітів. Якщо $H(M)\pmod q = 0$, то $H(M)=1$.

2. Згенерувати випадкове число k, $0<k<q$.

3. Обчислити:

$$r = a^k \pmod p;$$

$$r' = r \pmod q.$$

Якщо $r'=0$, повторити формування числа k.

4. З використанням секретного ключа x обчислити значення

$$s = (xr' + kH(M)) \pmod q.$$

5. Якщо $s=0$ повторити формування числа k.

Підписом для повідомлення M буде вектор (r',s).

Алгоритм перевірки ЕЦП

Перевірка цілісності та достовірності повідомлення і підпису проводиться за наявності відкритого ключа y відправника. Порядок дій формування ЦП:

1. Перевірити умови $0<s<q$ і $0<r'<q$.

Якщо хоч би одна з цих умов не виконується, то підпис вважається недійсним.

2. Обчислити хеш-функцію $H(M_1)$ прийнятого повідомлення M_1.

Якщо $H(M_1)\pmod q = 0$ то $H(M_1)=1$.

3. Обчислити значення:

$$v = H(M_1)^{q-2} (\mathrm{mod}\, q).$$

4. Обчислити значення:

$$z_1 = sv (\mathrm{mod}\, q);$$

$$z_2 = (q - r')v (\mathrm{mod}\, q).$$

5. Обчислити значення

$$u = \left(a^{z_1} y^{z_2} (\mathrm{mod}\, p)\right) (\mathrm{mod}\, q).$$

6. Перевірити умову $r' = u$. Якщо умова виконується, то одержувач ухвалює рішення про те, що отримане повідомлення підписане даним відправником і в процесі передачі не порушена цілісність повідомлення, тобто $M = M_1$. Інакше підпис вважається недійсним.

3.4. Завдання до лабораторної роботи

1. Використовуючи програму «Mathematic 6.0», зашифрувати та розшифрувати повідомлення, яке містить П.І.Б. студента.

2. За допомогою пакета «Mathematic 6.0» виконати формування цифрового повідомлення, яке містить П.І.Б. студента.

У табл. 3.1 наведено перелік хеш-функцій з довжиною їх значення.

Таблиця 3.1

Перелік хеш-функцій з довжиною їх значення

Назва хеш-функції	Довжина значення хеш-функції
Adler32	32-bit циклічний код перевірки на основі надлишковості
CRC32	32-bit циклічний код перевірки на основі надлишковості
MD2	128-bit MD2 код
MD5	128-bit MD5 код
SHA	160-bit SHA-1 код
SHA256	256-bit SHA код
SHA384	384-bit SHA код
SHA512	512-bit SHA код

Основні функції пакета «Mathematic 6.0», що необхідні для реалізації алгоритму:

Hash[expr,"type"]

Для рядка тексту expr отримує цілий хеш-код спеціального типу.

ToCharacterCode["*string*"]

Повертає список цілих кодів, відповідних символам у рядку «string».

Mod[*m*,*n*]

Повертає залишок ділення m **на** n**.**

NextPrime[n]

Повертає наступне просте число, більше за n**.**

RandomInteger[{$i_{\max}$}]

Повертає псевдовипадкове число в інтервалі $\{0,\ldots,i_{\max}\}$**.**

PowerMod[a,b,m]

Повертає $a^b \bmod m$**.**

PowerMod[a,-1,m]

Знаходить зворотний елемент за модулем m**.**

GCD[n,b]

Повертає найбільший спільний дільник двох чисел a **і** b**.**

Формування рядка повідомлення наведено на рис. 3.2.

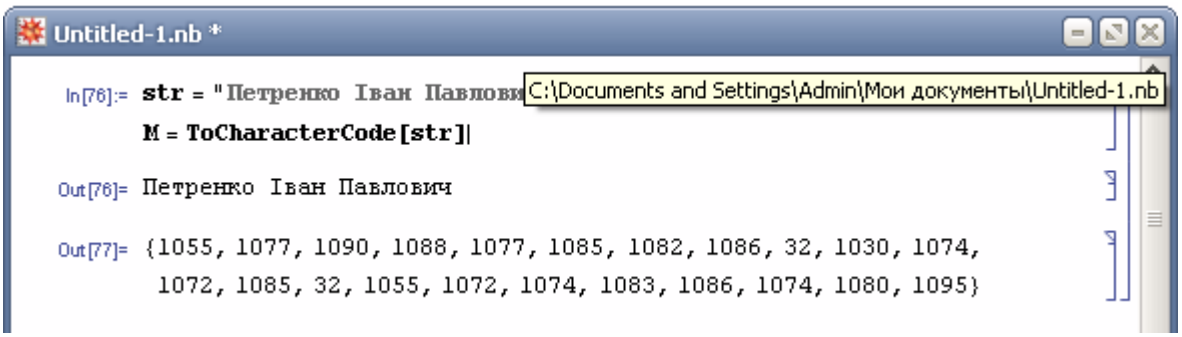

Рис. 3.2. **Рядок відкритого тексту**

Формування параметрів системи ЕЦП Ель-Гамаля подано на рис. 3.3.

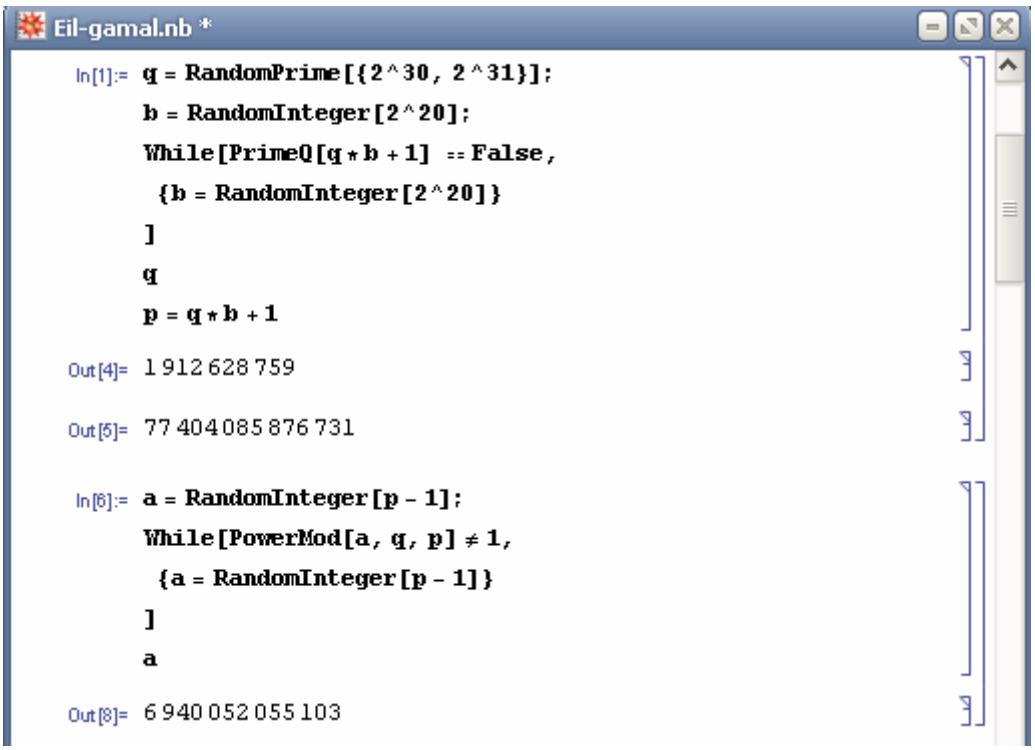

Рис. 3.3. **Формування параметрів ЕЦП Ель-Гамаля: прості числа** p**,** q **і первісний корінь** a

Далі генеруємо пару ключів – особистий та відкритий. Особистий ключ x генерується випадково. Відкритий ключ y обчислюється за допомогою функції PowerMod[a, y , p]. Порядок генерування проілюстровано на рис. 3.4.

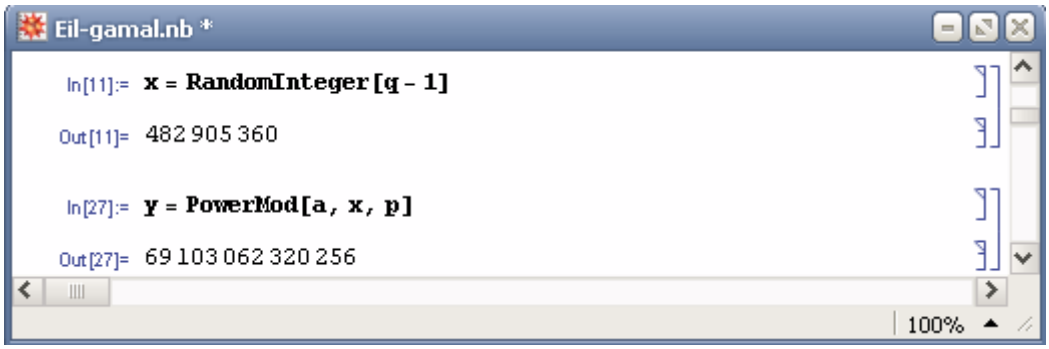

Рис. 3.4. **Генерування пари ключів** $\{x, y\}$

Шифрування повідомлення виконується за допомогою відкритого ключа адресата. Обчислення здійснюються за допомогою функції PowerMod[M_i, d , n] модульного піднесення у степінь.

Формування ЦП. Хеш-значення повідомлення обчислюється функцією `Hash[expr,"type"]`. Отриманий результат подано на рис. 3.5.

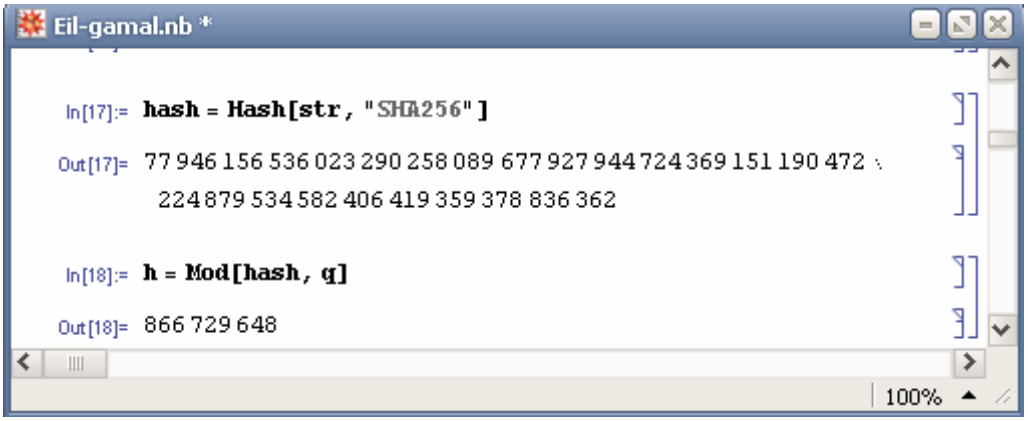

Рис. 3.5. **Обчислення хеш-значення h довжиною 256 бітів для повідомлення str з використанням хеш-функції SHA256**

Далі, згідно з алгоритмом виконується обчислення значень ЦП $\{r', s\}$. Результати обчислень наведені на рис. 3.6.

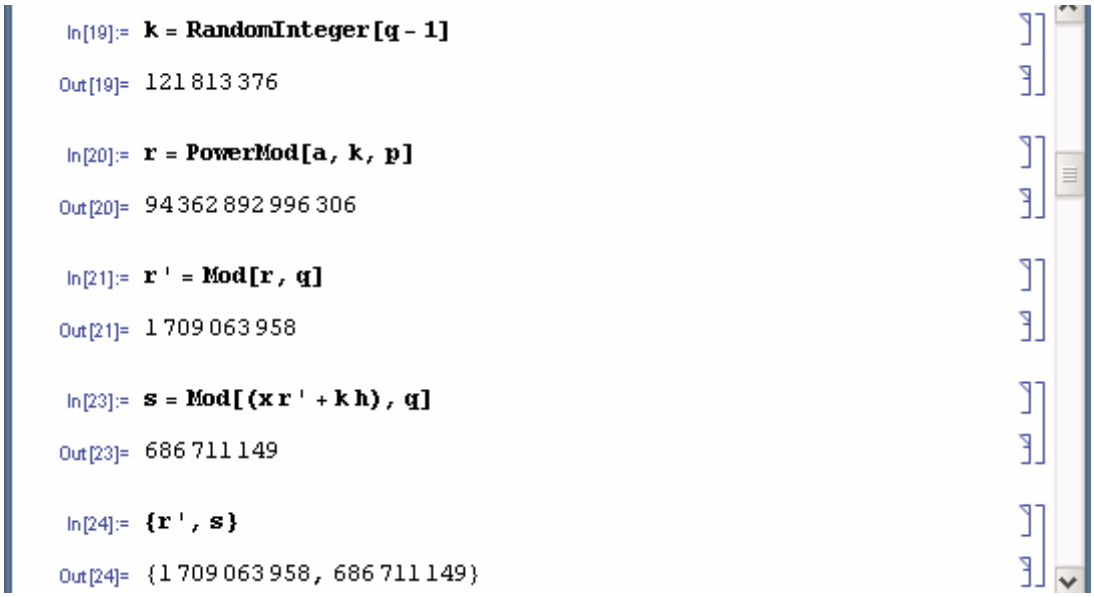

Рис. 3.6. **Результати обчислень при формуванні ЦП**

Процес перевірки цифрового підпису подано на рис. 3.7. У якості результату приймається рішення «правильний» чи «неправильний» цифровий підпис повідомлення.

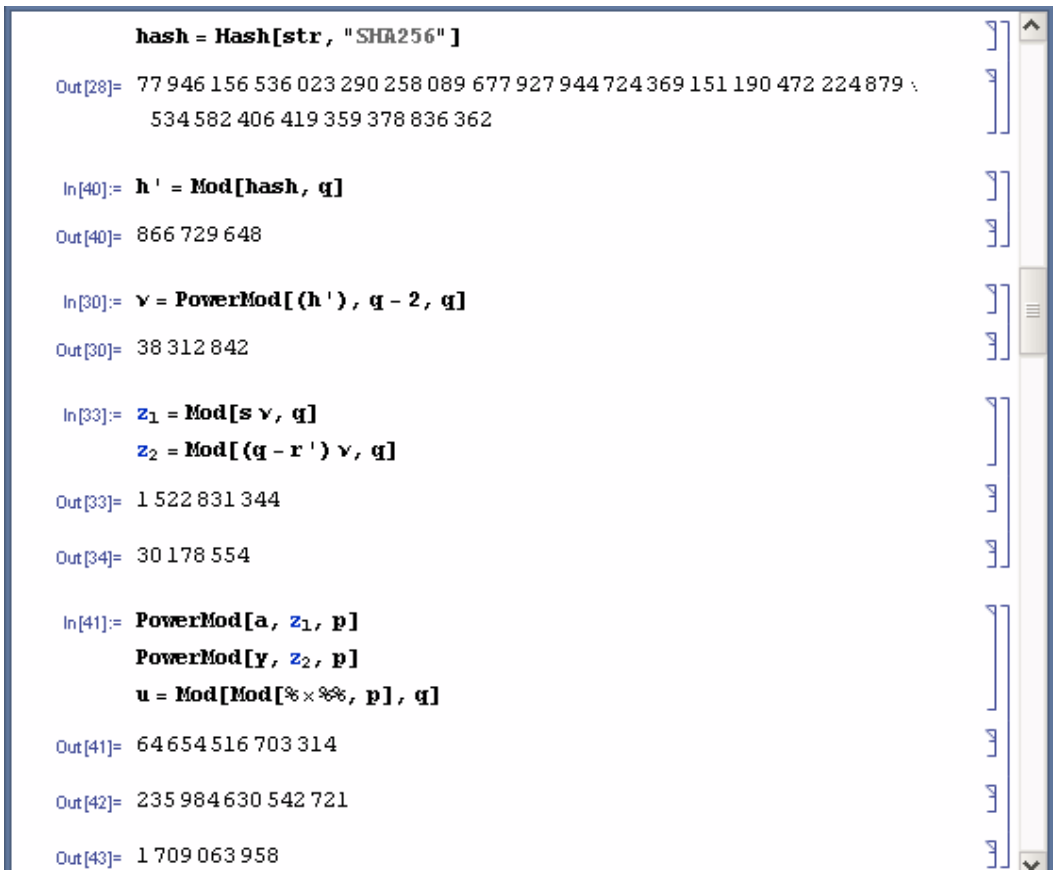

Рис. 3.7. **Перевірка ЦП за алгоритмом Ель-Гамаля**

Рішення про справжність ЦП прийметься на базі порівняння значення u з компонентом ЦП r.

Варіанти індивідуального завдання подані в табл. 3.2.

Таблиця 3.2

Варіанти індивідуального завдання

№ вар.	Порядок простого числа q (бітів)	Порядок простого числа p (бітів)	Алгоритм хешування
1	2	3	4
1.	896	768	Adler32
2.	864	832	CRC32
3.	832	896	MD2
4.	800	960	MD5
5.	768	1024	SHA
6.	736	1088	SHA256
7.	704	1152	SHA384
8.	672	1216	SHA512
9.	640	1280	Adler32
10.	608	1344	CRC32

Закінчення табл. 3.2			
1	2	3	4
11.	576	1408	MD2
12.	544	1472	MD5
13.	512	1536	SHA
14.	480	1600	SHA256
15.	448	1664	SHA384
16.	416	1728	SHA512
17.	384	1792	Adler32
18.	352	1856	CRC32
19.	320	1920	MD2
20.	288	1984	MD5

3.5. Контрольні запитання

1. Розкрійте поняття процедури автентифікації. Сформулюйте основні завдання автентифікації.
2. Викладіть суть алгоритму формування цифрового підпису.
3. Розкрийте суть алгоритму зняття цифрового підпису.
4. Які вимоги пред'являються до ключових даних системи Ель-Гамаля?
5. Складіть 2-рівневу або 3-рівневу схему розповсюдження ключових даних системи Ель-Гамаля.
6. У чому полягає суть і порядок виконання процедури криптоаналізу системи цифрового підпису Ель-гамаля?
7. Сформулюйте можливі загрози, що виникають у системі цифрового підпису. Як забезпечується захист від цих загроз?

Використана література

1. Вербіцький О. В. Вступ до криптології. – Львів: ВНТЛ, 1998. – 248 с.
2. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448 с.
3. Пономаренко В. С. Основи захисту інформації. Навчальний посібник. / В. С Пономаренко, І. В. Журавльова, – Харків: Вид. ХДЕУ, 2003. – 176 с.
4. Столингс В. Криптография и защита сетей: принципы и практика: Пер. с англ., – 2-е. изд. – М.: Изд. дом "Вильямс", 2001. – 672 с.
5. Чмора А. Л. Современная прикладная криптография. – М.: Гелиос АРВ, 2001. – 256 с.

НАВЧАЛЬНЕ ВИДАННЯ

Методичні рекомендації та контрольні завдання з навчальної дисципліни "ЗАХИСТ ІНФОРМАЦІЇ В ІС"

для студентів напряму підготовки "Комп'ютерні науки" заочної форми навчання

Укладачі: **Огурцов Віталій Вячеславович**
Поляков Андрій Олександрович

Відповідальний за випуск: **Пономаренко В. С.**

Редактор **Лященко Т. О.**

Коректор **Чистякова А. В.**

План 2008 р. Поз. №208.

Підп. до друку Формат 60 × 90 1/16. Папір MultiCopy. Друк Riso.

Ум.-друк. арк. 2,75. Обл.-вид. арк. 3,44. Тираж прим. Зам. №

Видавець і виготівник — видавництво ХНЕУ, 61001, м. Харків, пр. Леніна, 9а

Свідоцтво про внесення до Державного реєстру суб'єктів видавничої справи ***Дк №481 від 13.06.2001 р.***

Методичні рекомендації
та контрольні завдання
з навчальної дисципліни
"ЗАХИСТ ІНФОРМАЦІЇ В ІС"

для студентів напряму підготовки "Комп'ютерні науки"
заочної форми навчання