МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ І. І. МЕЧНИКОВА
Кафедра комп’ютерної алгебри та дискретної математики

О.В. Савастру

«Криптографія»

Методичні вказівки до самостійної роботи для здобувачів другого (магістерського) рівня вищої освіти з галузі знань 11 «**Математика та статистика**»

Одеса -2023

Криптографія. Методичні вказівки до самостійної роботи для здобувачів другого (магістерського) рівня вищої освіти з галузі знань 11 «Математика та статистика» – Одеса.-2023

Укладач:
Савастру Ольга Володимирівна, кандидат фізико-математичних наук, доцент, доцент кафедри комп'ютерної алгебри та дискретної математики

Рецензенти:

Рекомендовано до друку Вченою Радою ФМФІТ Одеського національного університету імені І.І. Мечникова

Протокол № від_____ 2023 р.

ЗМІСТ

Вступ ……4

Криптосистеми з відкритим ключем……. 6

Система RSA……6

Система Рабина……..11

Криптосистема Ель-Гамала……..16

Цифровий підпис…….21

Список рекомендованої літератури…….25

ВСТУП

Проблема забезпечення захисту інформації існує з того часу, як людина навчилася використовувати її для своїх власних цілей. Техніки та методи захисту були надзвичайно різноманітними. Їх розробка сприяла потребам дипломатії, військової діяльності, фінансової та комерційної діяльності. У сучасному інформатизованому світі, коли людина змушена довіряти багато речей комп'ютерам (робити електронні платежі, вирішувати ділові питання або отримувати доступ до певної інформації, наприклад, через Інтернет), навіть не маючи стосунку до військових або інших державних чи комерційних таємниць, може скластися ситуація, в якій можливі порушення прав і свобод особистості, якщо не забезпечений належний захист її інформаційних інтересів. Криптографія - це один із можливих способів захисту інформації. Її методи використовуються вже давно, а зараз вона переживає період активного розвитку, зокрема завдяки своїм застосуванням у суспільному та економічному житті.

Мета дисципліни: оволодіння студентами базових знань в галузі теоретичної криптографії та криптоаналізу, в методах побудови важкооборотних функцій та їх застосувань для побудови асиметричних криптосистем, отримати базові поняття про різноманітні криптографічні протоколи.

Завдання дисципліни: надати студентам знання в галузі криптографії, вміння розраховувати та застосовувати важкооборотні функції, володіти методами побудови різноманітних криптографічних протоколів, зокрема, протоколів аутентифікації, цифрового підпису, криптографічних протоколів у електронній комерції, ***в тому числі у блокчейн-технологіях***, вміння розробляти криптосистеми на еліптичних кривих.

У процесі навчання студенти отримують необхідні знання під час проведення аудиторних занять (лекційних, практичних) та самостійної роботи. Велике значення в процесі вивчення та закріплення знань має самостійна робота студентів, на яку відводиться значна частина кількості годин, які приділяються

на вивчення дисципліни. Наведені методичні вказівки містять стислий виклад лекційного матеріалу з двох тем курсу:

Тема 4. Криптосистеми з відкритим ключем.

Тема 6. Цифровий підпис.

Теоретичний матеріал супроводжується прикладами розв’язання задач та вправами для самостійної роботи.

КРИПТОСИСТЕМИ З ВІДКРИТИМ КЛЮЧЕМ

У 1976 році W. Diffie і M. Hellmann запропонували нову концепцію криптосистем з відкритим ключем, яка полягає в тому, що процес шифрування доступний для загального використання, а розшифрування може бути успішно виконане лише тим, хто має секретний ключ. Згідно з цією концепцією, система вимагає наявності двох ключів - відкритого, який є загальнодоступним, і закритого, секретного, яким володіє лише адресат. Це включає в загальну схему обміну закритою інформацією спеціальний генератор ключів, який створює відповідні пари.

КРИПТОСИСТЕМА RSA

Криптосистема RSA була запропонована у 1977 році R. Rivest, A. Shamir, L. Adleman. Вона стала першою системою з відкритим ключем і завоювала міцні позиції в асиметричній криптографії. Стійкість системи полягає в складності звуженої завдання факторизації.

Генерування ключів. Вибирають два різних великих простих числа p і q, знаходиться добуток $n = p \cdot q$ та значення функції Ойлера $\varphi(n) = (p-1)\cdot(q-1)$. Потім вибирається число $e \in Z^*_{\varphi(n)}$ та обчислюється величина d, $ed \equiv 1(\mathrm{mod}\,\varphi(n))$. Вважають відкритим ключем числа n, e, а секретним ключем – d .

Шифрування. Криптосистема RSA є блоковою. Відкритий текст M розбивають на блоки $M = m_1 \ldots m_l$, де $m_j \in Z^*_n$, і $j = 1, \ldots, l$. Тобто кожен з блоків розглядається як елемент кільця Z^*_n. Якщо m_j є блоком відкритого тексту, то результат його шифрування виглядає так: $c_j = m_j^e\,(\mathrm{mod}\,n)$, $j = 1, \ldots, l$.

У результаті виходить закритий текст як $C = c_1 \ldots c_l$.

Розшифрування. Блоки закритого тексту піддають процедурі, яка використовує секретний ключ.

Саме: $m_j = c_j^d \pmod n$, $j = 1, \ldots, l$.

Після чого формується відкритий текст $M = m_1 \ldots m_l$.

Для кожної з описаних дій існують ефективні алгоритми. А саме: алгоритми для побудови великих простих чисел, вибору числа *e* та розв'язання конгруенції за великим модулем (розширений алгоритм Евкліда), для процедур шифрування та розшифрування (бінарний метод). Це свідчить на користь ефективності системи в цілому.

Приклад. Зашифрувати повідомлення «ПРОДАЙ», використовуючи алфавіт
«|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|_|»
і шифр RSA.

Рішення. Оберемо прості p і q. Нехай $p = 53$, $q = 67$.

Тоді $n = 3551$, а $\varphi(n) = (p - 1)(q - 1) = 3432$.

Покладемо $e = 1021$, розв'язуючи конґруенцію $ed = 1 \pmod{\varphi(n)}$, отримаємо, що $d = 1021^{-1} \equiv 1237 (\mathrm{mod}\, 3432)$. Нами сформовано ключи криптосистеми. Оцифруємо відкритий текст

«ПРОДАЙ».

Використовуючи 34 літерний алфавіт, отримаємо

«192018050013».

Розіб'ємо його на блоки довжини 4:

«1920 1805 0013».

Підносячи кожний блок до степеня e = 1021 за модулем 3551, отримуємо:

$$1920^{1021} \equiv 2393 (\mathrm{mod}\, 3551)$$

$$1805^{1021} \equiv 1788 (\mathrm{mod}\, 3551)$$

$$13^{1021} \equiv 2188 (\mathrm{mod}\, 3551)$$

І відповідно цифровий шифртекст «2393 1788 2188».

Якщо тепер кожний блок цього текста підвести до степеня 1237 по mod 3551, то

вихідний цифровой текст.

Приклад. Повідомлення англійською мовою зашифровано шифром RSA: «1974636312012674112926721119001226296 3».

Використано наступний алфавіт:

«|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z|_».

Розшифруйте повідомлення, визначивши секретний ключ *d*, якщо відомий відкритий ключ $n = 95$, $e = 23$

Рішення.

$$n = 95 = 5 \cdot 19 \quad \Rightarrow \quad p = 5, \quad q = 19$$

$$\phi(n) = (5-1)(19-1) = 72.$$

Розв'язуємо конґруенцію $ed \equiv 1(\mathrm{mod}\,\varphi(n))$.

$$23d \equiv 1(72),$$

$$d \equiv 47(72).$$

Розіб'ємо зашифрований текст на блоки довжини 2:

«19 74 63 63 12 01 26 74 11 29 26 72 11 19 00 12 26 29 63».

Підносячи кожний блок до степеню e = 47 за модулем 95, отримуємо:

$$19^{47} \equiv 19(\mathrm{mod}\,95), \quad 74^{47} \equiv 4(\mathrm{mod}\,95), \quad 63^{47} \equiv 17(\mathrm{mod}\,95),$$

$$63^{47} \equiv 17(\mathrm{mod}\,95), \quad 12^{47} \equiv 8(\mathrm{mod}\,95), \quad 1^{47} \equiv 1(\mathrm{mod}\,95),$$

$$26^{47} \equiv 11(\mathrm{mod}\,95), \quad 74^{47} \equiv 4(\mathrm{mod}\,95), \quad 11^{47} \equiv 26(\mathrm{mod}\,95),$$

$$29^{47} \equiv 14(\mathrm{mod}\,95), \quad 26^{47} \equiv 11(\mathrm{mod}\,95), \quad 72^{47} \equiv 3(\mathrm{mod}\,95),$$

$$11^{47} \equiv 26(\mathrm{mod}\,95), \quad 19^{47} \equiv 19(\mathrm{mod}\,95), \quad 0^{47} \equiv 0(\mathrm{mod}\,95),$$

$$12^{47} \equiv 8(\mathrm{mod}\,95), \quad 26^{47} \equiv 11(\mathrm{mod}\,95), \quad 29^{47} \equiv 14(\mathrm{mod}\,95),$$

$$63^{47} \equiv 17(\mathrm{mod}\,95).$$

І відповідно цифровий шифртекст:

«190417170801110426141103261900081114 17».

Вихідний текст: «TERRIBLE_OLD_TAILOR».

ЗАДАЧА 1.

Повідомлення англійською мовою зашифровано шифром RSA:

«3157396848520100625160».

Використано наступний алфавіт:

«|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z|».

Розшифруйте повідомлення, визначивши секретний ключ *d*, якщо відомий відкритий ключ

$n = 77$, $e = 37$.

ЗАДАЧА 2.

Повідомлення англійською мовою зашифровано шифром RSA:

"0416065767003304170067".

Використано наступний алфавіт:

" |A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V| Y|Z|".

Розшифруйте повідомлення, визначивши секретний ключ *d*, якщо відомий відкритий ключ $n = 91$, $e = 31$.

ЗАДАЧА 3.

Повідомлення англійською мовою зашифровано шифром RSA:

«0123007680083176725233147613415241087572 44».

Використано наступний алфавіт:

" |A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V| Y|Z| _ |".

Розшифруйте повідомлення, визначивши секретний ключ *d*, якщо відомий відкритий ключ $n = 91$, $e = 17$.

ЗАДАЧА 4.

Повідомлення англійською мовою зашифровано шифром RSA:

«1974636312012674112926721119001226296 3».

Використано наступний алфавіт:

"|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V| Y|Z| _ |".

Розшифруйте повідомлення, визначивши секретний ключ d, якщо відомий відкритий ключ $n = 95$, $e = 23$.

ЗАДАЧА 5.

Повідомлення англійською мовою зашифровано шифром RSA:

"7339256468017968640072".

Використано наступний алфавіт:

"|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V| Y|Z|".

Розшифруйте повідомлення, визначивши секретний ключ d, якщо відомий відкритий ключ $n = 85$, $e = 47$.

ЗАДАЧА 6.

Повідомлення англійською мовою зашифровано шифром RSA:

"39733701364020900514318631 62".

Використано наступний алфавіт:

"|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V| Y|Z| _ |".

Розшифруйте повідомлення, переконавшись, що секретний ключ $d = 7$, відкритий ключ $n = 8777$, $e = 4903$, і довжина шифрувального блоку дорівнює 4.

ЗАДАЧА 7.

Повідомлення англійською мовою зашифровано шифром RSA:

«299275931953763113824793229741782461714 4».

Використано наступний алфавіт:

"A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V| Y|Z| _ |"

Розшифруйте повідомлення, якщо відкритий ключ $n = 63695461$, $e = 568741$.

ЗАДАЧА 8.

Повідомлення англійською мовою зашифровано шифром RSA:

"0946575935609070188828863977 0197".

Використано наступний алфавіт:

"A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V| Y|Z| _ |".

Розшифруйте повідомлення, якщо відкритий ключ $n = 40216009$, $e = 54217$.

КРИПТОСИСТЕМА РАБІНА

Криптосистема Рабіна (1979 р., Rabin) теж ґрунтується на складності завдання цілісної факторизації. Але виглядає дещо простіше у процедурі шифрування порівняно з RSA.

Генерування ключів. Вибираються два великі різні прості числа p і q (як правило, $p \equiv q \equiv 3 \pmod 4$). Обчислюється їх добуток $n = p \cdot q$ і вважають відкритим ключем число n, а секретним – p і q.

Шифрування. Відкритий текст M разбивають на блоки $M = m_1 \ldots m_l$, де $m_j \in Z_n^*$, $j = 1, \ldots, l$ і піддають поблочному шифруванню за правилом $c_j = m_j^2 \pmod n$, $j = 1, \ldots, l$. У результаті виходить закритий текст у вигляді $C = c_1 \ldots c_l$.

Розшифрування. Блоки закритого тексту піддають процедурі, яка використовує секретний ключ. Саме: $m_j = \sqrt{c_j} \pmod n$, $j = 1, \ldots, l$. Після чого формується відкритий текст $M = m_1 \ldots m_l$. Зважаючи на те, що отримаємо формально чотири відповіді для кожного блоку, вихідний текст має смислове навантаження і тому слід вибирати саме ту відповідь, яка таке має.

Приклад. Зашифрувати повідомлення «ПРОДАЙ», використовуючи алфавіт

«|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|_|»

і шифр Рабіна.

Рішення. Оберемо прості p і q. Нехай $p = 53$, $q = 67$.

Тоді $n = 3551$, а $\varphi(n) = (p - 1)(q - 1) = 3432$.

Оцифруємо відкритий текст

«ПРОДАЙ».

Використовуючи 34 літерний алфавіт, отримаємо

«192018050013».

Розіб'ємо його на блоки довжини 4:

«1920 1805 0013».

Підносячи кожний блок до степеня 2 за модулем 3551, отримуємо:

$$1920^2 \equiv 462 (\mathrm{mod}\, 3551)$$

$$1805^2 \equiv 1758 (\mathrm{mod}\, 3551)$$

$$13^{1021} \equiv 169 (\mathrm{mod}\, 3551)$$

І відповідно цифровий шифртекст «0462 1758 0169».

Приклад. Повідомлення англійською мовою зашифровано шифром Рабіна:

«1811364538121208».

Використано наступний алфавіт:

«|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z|».

Розшифруйте повідомлення, якщо секретний ключ p=59, q=79.

Рішення. $n = 59 \cdot 79 = 4661$, тому розіб'ємо зашифрований текст на блоки довжини 4:

«1811 3645 3812 1208».

Для розшифровки першого блока будемо поступати наступним чином.

Числа p і q мають вигляд 4m + 3, $p = 4 \cdot 14 + 3$, $q = 4 \cdot 19 + 3$.

Відомо, якщо x є квадратичним лишком $\mathrm{mod}\, k$ ($y = \sqrt{x}\,(\mathrm{mod}\, k)$)і $k = 4m + 3$, то за критерієм Ойлера

$$x^{2m+1} \equiv 1 (\mathrm{mod}\, k).$$

Отже, множимо обидві частини отриманої конгруенції на x, отримаємо:

$$y \equiv \pm x^{m+1} (\mathrm{mod}\, p);$$

Тому

$$x_1 = 1811 (\mathrm{mod}\, 59) = 41 (\mathrm{mod}\, 59), \quad y_{1,2} = \pm 41^{15} = 49,10 (\mathrm{mod}\, 59)$$

$$x_2 = 1811 (\mathrm{mod}\, 79) = 73 (\mathrm{mod}\, 79), \quad y_{3,4} = \pm 73^{15} = 51,28 (\mathrm{mod}\, 79)$$

Розв'язуємо чотири системи конгруенцій

$$\begin{cases} z \equiv 49 (\mathrm{mod}\, 59) \\ z \equiv 51 (\mathrm{mod}\, 79) \end{cases}, \quad \begin{cases} z \equiv 49 (\mathrm{mod}\, 59) \\ z \equiv 28 (\mathrm{mod}\, 79) \end{cases},$$

$$\begin{cases} z \equiv 10 (\mathrm{mod}\, 59) \\ z \equiv 51 (\mathrm{mod}\, 79) \end{cases}, \quad \begin{cases} z \equiv 10 (\mathrm{mod}\, 59) \\ z \equiv 28 (\mathrm{mod}\, 79) \end{cases}$$

Отримаємо чотири відповіді, ці набори цифр слід доповнити цифрою- «0» так, щоб довжина отриманого блока дорівнювала 4. Можна побачити, що тільки одна відповідь, яка відповідає четвертій системі, буде мати сенс: $0423 (\mathrm{mod}\, 4661)$. Вона відповідає парі літер «EX».

Виконуючи такі ж дії із наступними блоками, ми отримаємо:

$$3645: \quad \begin{cases} z \equiv -20 (\mathrm{mod}\, 59) \\ z \equiv 13 (\mathrm{mod}\, 79) \end{cases} \rightarrow \quad 1514 \rightarrow \quad PO$$

$$3812: \quad \begin{cases} z \equiv -53 (\mathrm{mod}\, 59) \\ z \equiv 40 (\mathrm{mod}\, 79) \end{cases} \rightarrow \quad 1304 \rightarrow \quad NE$$

$$1208: \quad \begin{cases} z \equiv 21 (\mathrm{mod}\, 59) \\ z \equiv 55 (\mathrm{mod}\, 79) \end{cases} \rightarrow \quad 1319 \rightarrow \quad NT.$$

Вихідне повідомлення «EXPONENT».

ЗАДАЧА 1.

Повідомлення англійською мовою зашифровано шифром Рабіна:

«2530057605275831».

Використано наступний алфавіт:

«|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z|».

Розшифруйте повідомлення, якщо секретний ключ $p = 71$ і $q = 83$.

ЗАДАЧА 2.

Повідомлення англійською мовою зашифровано шифром Рабіна:

«3857375802231661».

Використано наступний алфавіт:

«|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z|».

Розшифруйте повідомлення, якщо секретний ключ $p = 59$ і $q = 79$.

ЗАДАЧА 3.

Повідомлення англійською мовою зашифровано шифром Рабіна:

«1811364538121208».

Використано наступний алфавіт:

«|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z|».

Розшифруйте повідомлення, якщо секретний ключ $p = 59$ і $q = 79$.

ЗАДАЧА 4.

Повідомлення англійською мовою зашифровано шифром Рабіна:

«13514074040015211189».

Використано наступний алфавіт:

«|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z|».

Розшифруйте повідомлення, визначивши секретний ключ *p* та *q*, якщо відомий відкритий ключ $n = 5251$.

ЗАДАЧА 5.

Повідомлення англійською мовою зашифровано шифром Рабіна:

«1491198312920416».

Використано наступний алфавіт:

«|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z|».

Розшифруйте повідомлення, визначивши секретний ключ *p* та *q*, якщо відомий відкритий ключ $n = 3953$.

ЗАДАЧА 6.

Повідомлення англійською мовою зашифровано шифром Рабіна:

«2663298506961316».

Використано наступний алфавіт:

«|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z|».

Розшифруйте повідомлення, визначивши секретний ключ *p* та *q*, якщо відомий відкритий ключ $n = 3763$.

ЗАДАЧА 7.

Повідомлення англійською мовою зашифровано шифром Рабіна:

«37804306511718723710508462173150004587840672507 4».

Використано наступний алфавіт:

«|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z| _ |».

Розшифруйте повідомлення, якщо відкритий ключ $n = 65624921$.

КРИПТОСИСТЕМА ЕЛЬ-ГАМАЛА

Криптосистема Ель-Гамала є прикладом ймовірнісного алгоритму шифрування. Імовірнісні системи у певному сенсі вважаються стійкішими, ніж детерміновані. У такому разі стійкість об'єкта ґрунтується на складності завдання дискретного логарифмування групи F_p^*, де p – непарне просте. Розглянемо один із варіантів системи.

Генерування ключів. Вибирається велике просте число p і первісний корінь за модулем p – число g; потім вибирається деяке ціле a, $1 < a < p-1$ і обчислюється величина $h = g^a \pmod p$, після чого вважають відкритим ключем числа p, g и h, а секретним ключем – число a .

Шифрування. Відкритий текст оцифровується і розбивається на блоки $M = m_1 \ldots m_l$ де $m_j \in Z_p^*$, $j = 1, \ldots, l$. Для кожного блоку m_j вибирається випадкове число r_j, $j = 1, \ldots, l$ і далі проводяться обчислення $c_{1j} = g^{r_j} \pmod p$ і $c_{2j} = m_j \cdot h^{r_j} \pmod p$. У результаті вважають $E(m_j) = c_j = (c_{1j}, c_{2j}) \in Z_p^* \times Z_p^*$, $j = 1, \ldots, l$. Після чого формується закритий текст виду $C = c_1 \ldots c_l$.

Розшифрування. З закритого тексту $C = c_1 \ldots c_l$ виділяють блок c_j, $j = 1, \ldots, l$ і обчислюють блок відкритого тексту $m_j = c_{2j} \cdot c_{1j}^{-a} \pmod p$. Далі формують відкритий текст $M = m_1 \ldots m_l$.

Приклад. Приклад шифрування за криптосистемою Ель-Гамала.
Нехай заданий відкритий текст: «TIMEO DANAOS ET DONA FERENTES».
Його цифровий еквівалент, розбитий на блоки довжиною шість, виглядає так (тут додається в кінці тексту літера «J»):
«190812 041426 030013 001418 260419 260314 130026 050417 041319 041809».

Нехай обрано просте число p = 994991. В якості числа g обрано первісний корінь за модулем p: g = 7.

Обираємо число a = 475 і обчислюємо h = 659454 (mod 994991).

Візьмемо r = 211 загальним для всіх блоків відкритого тексту. Тоді c_1= 073747. Цифра «0» на початку додана для того, щоб c_1 мала вигляд блока довжиною шість. Обчислюючи за описаним вище правилом елементи виду c_2 і збираючи їх разом, отримуємо шифртекст, де на початку записано c_1, що служить своєрідним підказкою при розшифруванні:
«073747 127613 201338 222776 758335 502424 595730 925985 939171 182708 742271».

Приклад. Повідомлення англійською мовою зашифровано шифром Ель-Гамала:

«07*4351573771537531».

Використано наступний алфавіт:

«|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z|».

Розшифруйте повідомлення, якщо відкритий ключ є $p = 79$, $g = 3$, $h = 48$. Величина c_1 – загальна для всіх блоків і дорівнює 07.

Рішення. Обчислимо a:

$$h \equiv g^a \pmod p,$$
$$48 \equiv 3^a \pmod{79},$$
$$a = 17.$$

Знайдемо блоки відкритого повідомлення:

$$m_j \equiv c_{2j} c_{1j}{}^a \pmod p,$$
$$m_1 \equiv 43 \cdot 7^{-17} \pmod{79} = 18 \quad \to \quad S,$$
$$m_2 \equiv 51 \cdot 7^{-17} \pmod{79} = 14 \quad \to \quad O,$$
$$m_3 \equiv 57 \cdot 7^{-17} \pmod{79} = 11 \quad \to \quad L,$$
$$m_4 \equiv 37 \cdot 7^{-17} \pmod{79} = 21 \quad \to \quad V,$$
$$m_5 \equiv 71 \cdot 7^{-17} \pmod{79} = 4 \quad \to \quad E,$$
$$m_6 \equiv 53 \cdot 7^{-17} \pmod{79} = 13 \quad \to \quad N,$$

$$m_7 \equiv 75 \cdot 7^{-17} (\bmod 79) = 2 \quad \rightarrow \quad C,$$

$$m_8 \equiv 31 \cdot 7^{-17} (\bmod 79) = 24 \quad \rightarrow \quad Y.$$

Вихідний текст «SOLVENCY»

ЗАДАЧА 1.

Повідомлення англійською мовою зашифровано шифром Ель-Гамала:

«55*0512140058744228».

Використано наступний алфавіт:

«|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z|».

Розшифруйте повідомлення, перевіривши, що секретний ключ $a = 10$, якщо відкритий ключ $p = 83$, $g = 2$, $h = 28$.

Розмір c_1 – загальна для всіх блоків і дорівнює 55.

ЗАДАЧА 2.

Повідомлення англійською мовою зашифровано шифром Ель-Гамала:

«53*27721172273664».

Використано наступний алфавіт:

«|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z|».

Розшифруйте повідомлення, перевіривши, що секретний ключ $a = 35$, якщо відкритий ключ $p = 89$, $g = 3$, $h = 19$.

Розмір c_1 – загальна для всіх блоків і дорівнює 53.

ЗАДАЧА 3.

Повідомлення англійською мовою зашифровано шифром Ель-Гамала:

«43*0907471051040748».

Використано наступний алфавіт:

«|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z|».

Розшифруйте повідомлення, якщо відкритий ключ є $p = 83$, $g = 2$, $h = 66$.

Величина c_1 – загальна для всіх блоків і дорівнює 43.

ЗАДАЧА 4.

Повідомлення англійською мовою зашифровано шифром Ель-Гамала:

«22*7992085239888300224888».

Використано наступний алфавіт:

«|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z|».

Розшифруйте повідомлення, якщо відкритий ключ є $p = 97$, $g = 5$, $h = 85$.

Величина c_1 – загальна для всіх блоків і дорівнює 22.

ЗАДАЧА 5.

Повідомлення англійською мовою зашифровано шифром Ель-Гамала:

«52*43732181294388».

Використано наступний алфавіт:

«|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z|».

Розшифруйте повідомлення, якщо відкритий ключ є $p = 89$, $g = 3$, $h = 66$.

Величина c_1 – загальна для всіх блоків і дорівнює 52.

ЗАДАЧА 6.

Повідомлення англійською мовою зашифровано шифром Ель-Гамала:

«47*460334435043273507».

Використано наступний алфавіт:

«|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z|».

Розшифруйте повідомлення, якщо відкритий ключ є $p = 59$, $g = 2$, $h = 14$.

Величина c_1 – загальна для всіх блоків і дорівнює 47.

ЗАДАЧА 7.

Повідомлення англійською мовою зашифровано шифром Ель-Гамала:

«34*3969335319360029660616».

Використано наступний алфавіт:

«|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z|».

Розшифруйте повідомлення, якщо відкритий ключ є $p = 73$, $g = 5$, $h = 10$.

Величина c_1 – загальна для всіх блоків і дорівнює 34.

ЗАДАЧА 8.

Повідомлення англійською мовою зашифровано шифром Ель-Гамала:

«79*1626042824302208380852380846 38».

Використано наступний алфавіт:

«|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z| _ |».

Розшифруйте повідомлення, якщо відкритий ключ є $p = 83$, $g = 2$, $h = 74$.

Величина c_1 – загальна для всіх блоків і дорівнює 79.

ЦИФРОВИЙ ПІДПИС

Будемо розглядати завдання двох систем цифрового підпису: **з урахуванням RSA і Ель-Гамала.**

У першому випадку Аліса, підписуючи повідомлення M, будує підпис S наступним чином:

вона вважає $S(M, d_A, e_B) = E(D(M, d_A), e_B)$, де E і D – алгоритми шифрування та розшифрування, а d_A і e_B – секретний ключ Аліси та відкритий ключ Боба відповідно. Боб, отримавши повідомлення M, перевіряє підпис під ним, виконуючи процедуру: $X = E(D(S, d_B), e_A)$, де d_B і e_A – секретний ключ Боба і відкритий ключ Аліси відповідно. Якщо $X = M$, то підпис приймається.

У другому випадку створюються ключі, як у системі Ель-Гамала.

Відкритий ключ: $p,\ g,\ h$;

Секретний ключ: a.

Підписування. Аліса виробляє свій підпис S під повідомленням *M* таким чином:

1) вибирає випадкове число $r \in Z_{p-1}^*$;

2) обчислює $s_1 = g^r (\mathrm{mod}\, p)$;

3) обчислює $r' = r^{-1} (\mathrm{mod}(p-1))$;

4) обчислює $s_2 = (M - as_1) r' (\mathrm{mod}(p-1))$;

5) вважає $S = (s_1, s_2)$.

Підтвердження підпису. Боб перевіряє справедливість порівняння

$$g^M \equiv h^{s_1} s_1^{s_2} (\mathrm{mod}\, p).$$

Приклад. Нехай Аліса відправляє Бобу повідомлення «NO» і при цьому використовує підпис на основі криптосистеми RSA.

Ключі Аліси: $n_A = 71 \cdot 89 = 6319$, $\varphi(n_A) = 6160$, $e_A = 201$, $d_A = 521$.

Ключі Боба: $n_Б = 61 \cdot 73 = 4453$, $\varphi(n_Б) = 4320$, $e_Б = 191$, $d_Б = 3551$.

Аліса відправляє Бобу повідомлення, перед тим закодувавши відкритий текст «NO» $\to 1314 = M$

$C = E_B(D_A(M)) = E_Б(1314^{521} (\mathrm{mod}\, 6319)) = E_Б(2146) = 2146^{191} (\mathrm{mod}\, 4453) = 2734$.

Боб, отримавши повідомлення C, обчислює

$M = E_A(D_B(C)) = E_A(2734^{3551} (\mathrm{mod}\, 4453)) = E_A(2146) = 2146^{201} (\mathrm{mod}\, 6319) = 1314$.

Отже, Боб, якщо він вірить у стійкість системи RSA, повинен прийняти це повідомлення як повідомлення від Аліси (тут невеликі модулі взяті з міркувань простоти демонстрації схеми).

Приклад. Нехай Аліса знову надсилає Бобу повідомлення «NO», використовуючи протокол Ель-Гамала. Вона обирає $p = 541$, $g = 2$, і $a = 101$, отже, $h = 2^{101} = 68 (\mathrm{mod}\, 541)$. Цифровий вигляд повідомлення: «1314». Аліса виконує наступні дії:

1) обирає випадкове $r = 67 \in Z^*_{540}$;

2) обчислює $s_1 = 2^{67} (\mathrm{mod}\, 541) = 297$;

3) обчислює $r' = 403$;

4) обчислює $s_2 = (1314 - 101 \cdot 297) \cdot 403 (\mathrm{mod}\, 540) = 531$;

5) формує підпис $(297, 531)$.

Боб, отримавши повідомлення «NO» ← «1314», перевіряє виконання конгруенції:

$$2^{1314} = 68^{297} \cdot 297^{531} (541),$$
$$343 = 44 \cdot 266 (\mathrm{mod}\, 541).$$

Приклад. Сфальшувати підпис Аліси на основі RSA під повідомленням «DANCE» в алфавіті «|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z|», якщо $n = 95$, $e_A = 41$, $e_B = 23$.

Рішення. «DANCE» : «03 04 13 02 04».

$n = 5 \cdot 19, \quad \varphi(n) = 4 \cdot 18 = 72 \quad \to \quad d_A = 65 (\mathrm{mod}\, 72).$

$$c_1 = \left(3^{65}\right)^{23} = 22(\mathrm{mod}\,95),$$

$$c_2 = \left(0^{65}\right)^{23} = 00(\mathrm{mod}\,95),$$

$$c_3 = \left(13^{65}\right)^{23} = 32(\mathrm{mod}\,95),$$

$$c_4 = \left(2^{65}\right)^{23} = 78(\mathrm{mod}\,95),$$

$$c_5 = \left(4^{65}\right)^{23} = 4(\mathrm{mod}\,95).$$

$$C: \quad 2200327804,$$

$$S = C^{d_A}(\mathrm{mod}\,n),$$

$$S = 2200327804^{65}(95) = 14,$$

$$(C,S) = (2200327804,14).$$

ЗАДАЧА 1

Сфальшувати підпис Аліси на основі RSA під повідомленням «WORLD» в алфавіті «|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z|», якщо $n = 95$, $e_A = 43$, $e_B = 17$.

ЗАДАЧА 2

Сфальшувати підпис Аліси на основі RSA під повідомленням «STOP» в алфавіті «|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z|», якщо $n = 8051$, $e_A = 25$, $e_B = 37$.

ЗАДАЧА 3

Сфальшувати підпис Аліси на основі RSA під повідомленням «BONUS» в алфавіті «|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z|», якщо $n = 86519$, $e_A = 49$, $e_B = 73$.

ЗАДАЧА 4

Виробити підпис Аліси на основі схеми Ель-Гамала під повідомленням Бобу «HOME»

в алфавіті «|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z|», і | перевірити її правильність, якщо $p = 359$, $g = 7$, $a = 75$.

ЗАДАЧА 5

Виробити підпис Аліси на основі схеми Ель-Гамала під повідомленням Бобу «FOREST» в алфавіті «|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z|», і |перевірити її правильність, якщо $p = 2897$, $g = 3$, $a = 441$.

ЗАДАЧА 6

Виробити підпис Аліси на основі схеми Ель-Гамала під повідомленням Бобу «VICTORY» в алфавіті «|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z|», і |перевірити її правильність, якщо $p = 541$, $g = 2$, $h = 188$.

ЗАДАЧА 7

Показати, що підпис Аліси під повідомленням «YES» англійською мовою в алфавіті

«|A|B|C|D|E|F|G|H|I|J|K|L|M|N|O|P|Q|R|S|T|U|V|W|X|Y|Z|» сфальсифікована, якщо

$S = (365,396)(388,316)(73,43)$ и $p = 541$, $g = 2$, $h = 188$.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Вербіцький О.В. Вступ до криптології. Львів: Науково-технічна література, 1998. 248с.
2. Гринченко О.М., Мамчур Є.В. Концептуальні засади захисту інформації в умовах економіки. К.: НУХТ, 2016. 282с.
3. Гуржій О.В., Красножон Д. В. Криптографія і захист інформації в електронній комерції. К.: Вид-во НПУ ім. М.П. Драгоманова, 2015. 180с.
4. Задірака В.К., Олексюк О.С., Недашковський М.О. Методи захисту фінансової інформації: навчальний посібник. К.: Вища школа, 2000. 460с.
5. Клесов О.І. Елементарна теорія чисел та елементи криптографії, Київ: ТВіМС, 2017. 394с.
6. Мазур О.І. Криптографічні алгоритми та протоколи захисту електронних коштів. К.: НАУ, 2015. 188с.
7. Химич В.І. Криптографічні аспекти безпеки інформаційно-комунікаційних систем. К.: ВПЦ "Київський університет", 2012. 448 с.
8. Шеремета Ю.І. Електронні гроші: криптографічний захист та технології. К.: ТОВ "Техніка", 2004. 256с.
9. Buchmann J. A. Introduction to cryptography, second edition. Springer Verlag, New York, 2004. 386p.
10. Koshy T. Elementary Number Theory with Applications. 2nd edition, Elsevier, Amsterdam, 2007. 812p.
11. Rivest, R.L.; Shamir, A.; Adleman, L.M. A Method for Obtaining Digital Signatures and Public Key Cryptosystems; Routledge: London, UK, 2019. 15p.
12. Rosen K. H. Elementary Number Theory. 6th edition, Addison Wesley, Boston MA, 2011. 616p.