ЛАБОРАТОРНА РОБОТА № 6. АСИМЕТРИЧНІ ШИФРИ RSA ТА ЕЛЬ-ГАМАЛЯ. АЛГОРИТМ ОБМІНУ КЛЮЧАМИ ДІФФІ-ХЕЛМАНА

Мета роботи: набути уміння із генерації ключів, зашифрування і дешифрування повідомлення за допомогою алгоритмів RSA та Ель-Гамаля, дослідити алгоритм обміну ключами Діффі-Хеллмана, на практиці здійснити формування спільного ключа між двома абонентами.

Матеріально-технічне забезпечення: ПК зі встановленим програмним забезпеченням MS Excel та доступом до мережі Інтернет.

Теоретичні відомості

КРИПТОСИСТЕМИ З ВІДКРИТИМ КЛЮЧЕМ

Якими б не були надійними та швидкими симетричні криптографічні системи – їх слабким місцем, під час практичної реалізації, є проблема обміну ключами. Для вирішення цієї і ряду інших проблем були запропоновані криптосистеми з відкритим ключем, які називають також асиметричними криптосистемами.

Концепція криптографії з відкритим ключем була висунута Вітфілдом Діффі (Whitfield Diffie) та Мартіном Хелманом (Martin Hellman), і окремо Ральфом Мерклом (Ralph Merkle). У *асиметричних криптосистемах* для шифрування використовується один, відкритий (публічний, загальнодоступний) ключ, а для дешифрування – інший, закритий (секретний, приватний). Закритий ключ та відкритий ключ – це два великі числа, обчислені на основі деякого асиметричного алгоритму. Відкритий може бути доступним будь-якому учаснику процесу інформаційного обміну. При чому, знання відкритого ключа не дозволяє обчислити відповідний закритий ключ.

Ідея криптографії з відкритим ключем дуже тісно пов'язана з ідеєю *однобічних функцій*, тобто таких функцій $f(x)$, що по відомому x досить просто знайти значення $f(x)$, тоді як визначити x з $f(x)$складно (рис. 6.1).

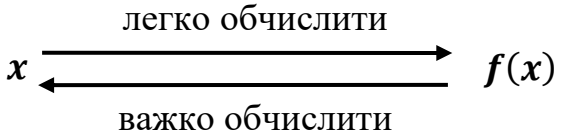

Рис. 6.1. Схема роботи однобічних функцій

Також використовуються *однобічні функції з лазівкою*. Лазівка – це певний секрет, що допомагає розшифрувати. Тобто існує такий y, що знаючи $f(x)$, можна обчислити x.

АЛГОРИТМ ШИФРУВАННЯ RSA

Найбільш простим для розуміння та реалізації є алгоритм з відкритим ключем RSA, названий на честь трьох авторів – Рона Рівеста (Ron Rivest), Аді Шаміра (Adi Shamir) і Леонарда Едлмана (Leonard Adleman).

Безпека RSA заснована на складності розкладання на множники великих чисел. Відкритий і закритий ключі є функціями двох великих простих чисел розрядністю 100…200 десяткових цифр і навіть більше. Відновлення відкритого тексту за шифртекстом та відкритим ключем є рівнозначне до розкладання числа на два великі прості множники.

Генерація ключів

1. Вибираються два великих випадкових простих числа, p і q (для максимальної безпеки p і q варто обирати рівної довжини).

2. Обчислюється добуток (модуль системи): $n = p \cdot q$.

3. Обчислюється функція Ейлера $\varphi(n) = \varphi(pq) = (p-1)(q-1)$. Результат розрахунку даної функції дорівнює кількості додатних чисел, які не більше n і взаємно прості з n.

4. Випадковим чином вибирається число e (ключ шифрування), таке що $1 < e < \varphi(n)$ та взаємно просте з $\varphi(n)$.

5. За допомогою розширеного алгоритму Евкліда знаходиться число d (ключ дешифрування), таке що $ed \equiv 1(mod\ \varphi(n))$.

6. Пара $(e,\ n)$ публікується у якості відкритого ключа.

7. Пара $(d,\ n)$ виконує роль секретного ключа і тримається таємниці.

Два простих числа p і q більше не потрібні. Проте вони не повинні бути розкриті.

Зашифрування

Для шифрування повідомлення *M* воно спочатку розбивається на цифрові блоки, менші n (для двійкових даних вибирається найбільший степінь числа 2,

менший n). Зашифроване повідомлення C буде складатися із блоків c_i. Формула шифрування виглядає наступним чином: $c_i = m_i^e \, mod \, n$.

Дешифрування

Для дешифрування повідомлення візьмемо кожний зашифрований блок c_i і обчислимо: $m_i = c_i^d \, mod \, n$.

Приклад 6.1:

Зашифруємо повідомлення КНИГА, що складається із символів українського алфавіту та представляється як послідовність цілих чисел M = 14 17 10 3 0.

Для простоти обчислень будемо використовувати невеликі числа, проте пам'ятаємо, що на практиці застосовують дуже великі прості числа. Оберемо $p = 3$ і $q = 11$, тоді $n = p \cdot q = 3 \cdot 11 = 33$.

Обчислимо $\varphi(33) = 2 \cdot 10 = 20$.

Виберемо (випадково) $e = 3$ та перевіримо виконання умов: $1 < 3 < 20$, НСД(3, 20) =1.

Визначимо d – ключ дешифрування з рівняння $3d \equiv 1(mod\ 20)$.

Для розв'язання рівняння використаємо *розширений алгоритм Евкліда*:

1) послідовно виконуємо ділення з остачею попереднього значення r_{i-1} на наступне r_i, у відповідністю з рівністю $r_{i-1} = r_i q_{i+1} + r_{i+i}$ (якщо $r_i = 1$, тоді зупиняєио процес);

2) використовуємо рекурентне співвідношення $u_{i+1} = u_{i-1} - q_{i+1} u_i$;

3) використовуємо рекурентне співвідношення $v_{i+1} = v_{i-1} - q_{i+1} v_i$;

4) щоб почати процес виконання алгоритму, використовуємо значення $r_0 = 20$, $r_1 = 3$, $u_0 = 1$, $u_1 = 0$, $v_0 = 0$, $v_1 = 1$.

i	r_i	q_i	u_i	v_i
0	20		1	0
1	3		0	1
2	20 *mod* 3 =2	20 *div* 3 = 6	1-6·0=1	0-6·1=-6
3	3 *mod* 2 =1	3 *div* 2 = 1	0-1·1=-1	1-1·(-6)=7

Виконуємо перевірку $3 \cdot 7 \, mod \, 20 = 1$. Таким чином, $d = 7$.

Опублікуємо відкритий ключ $(e,\ n)\ =\ (3, 33)$.

Зберігаємо в таємниці секретний ключ $(d,\ n)\ =\ (7, 33)$.

Зашифруємо повідомлення *M* = 14 17 10 3 0, що складається із п’яти блоків m_i:

$c_1 = 14^3 \, mod \, 33 = \big((14^2 \, mod \, 33) \cdot (14^1 \, mod \, 33)\big) \, mod \, 33 = (31 \cdot 14) \, mod \, 33 =$
$= 434 \, mod \, 33 = 5;$
$c_2 = 17^3 \, mod \, 33 = \big((17^2 \, mod \, 33) \cdot (17^1 \, mod \, 33)\big) \, mod \, 33 = (25 \cdot 17) \, mod \, 33 =$
$= 425 \, mod \, 33 = 29;$
$c_3 = 10^3 \, mod \, 33 = 1000 \, mod \, 33 = 10;$
$c_4 = 3^3 \, mod \, 33 = 27 \, mod \, 33 = 27;$
$c_5 = 0^3 \, mod \, 33 = 0 \, mod \, 33 = 0.$

Шифротекст: C = 5 29 10 27 0.

Для дешифрування потрібно також виконати піднесення до степеня, використовуючи ключ дешифрування 7:

$m_1 = 5^7 \, mod \, 33 = ((5^4 \, mod \, 33) \cdot (5^3 \, mod \, 33)) \, mod \, 33 = (31 \cdot 26) \, mod \, 33 =$
$= 806 \, mod \, 33 = 14;$
$m_2 = 29^7 \, mod \, 33 = ((29^4 \, mod \, 33) \cdot (29^3 \, mod \, 33)) \, mod \, 33 =$
$= (((29^2))^2 \, mod \, 33) \cdot (29^2 \, mod \, 33) \cdot (29 \, mod \, 33)) \, mod \, 33 = (25 \cdot 16 \cdot 29) \, mod \, 33$
$= 11600 \, mod \, 33 = 17;$
$m_3 = 10^7 \, mod \, 33 = ((10^4 \, mod \, 33) \cdot (10^3 \, mod \, 33)) \, mod \, 33 =$
$= (((10^2))^2 \, mod \, 33) \cdot (10^2 \, mod \, 33) \cdot (10 \, mod \, 33)) \, mod \, 33 = (1 \cdot 1 \cdot 10) \, mod \, 33 =$
$= 10 \, mod \, 33 = 10;$
$m_4 = 27^7 \, mod \, 33 = ((27^4 \, mod \, 33) \cdot (27^3 \, mod \, 33)) \, mod \, 33 =$
$= (((27^2))^2 \, mod \, 33) \cdot (27^2 \, mod \, 33) \cdot (27 \, mod \, 33)) \, mod \, 33 = (9 \cdot 3 \cdot 27) \, mod \, 33 =$
$= 729 \, mod \, 33 = 3;$
$m_5 = 0^7 \, mod \, 33 = 0 \, mod \, 33 = 0.$

Відкритий текст: M = 14 17 10 3 0 $\Rightarrow$ КНИГА.

АЛГОРИТМ ШИФРУВАННЯ ЕЛЬ-ГАМАЛЯ

Алгоритм шифрування Ель-Гамаля (ElGamal) – криптосистема з відкритим ключем, заснована на складності обчислення дискретних логарифмів в скінченному полі. Шифр була запропонована американським вченим єгипетського походження Тахером Ель-Гамалем у 1984.

Генерація ключів

1. Генерується просте випадкове число p.

2. Вибирається генератор g, таке що $1 < g < p - 1$ та $g^{p-1} mod \, p = 1$.

3. Вибирається випадкове число x, таке що $1 < x < p - 1$.

4. Обчислюється $y = g^x \, mod \, p$.

5. Відкритими даними є p, g, y.

6. Закритим ключем є x.

Зашифрування

Повідомлення M шифрується таким чином:

Вибирається сесійний ключ – випадкове число k, таке що $1 < k < p - 1$.

Потім обчислюються $a = g^k \, mod \, p$ та $b = y^k M \, mod \, p$.

Пара чисел $(a, \, b)$ є шифротекстом.

Дешифрування

Для дешифрування $(a, \, b)$ обчислюється:

$M = b(a^x)^{-1} \, mod \, p$ або $M = b(a^x)^{-1} \, mod \, p = = b \cdot a^{(p-1-x)} \, mod \, p$.

Приклад 6.2:

Зашифруємо повідомлення $M = 5$.

Спершу згенеруємо ключі шифрування. Нехай $p = 11, \, g = 2$.

Виберемо $x = 8$ – випадкове ціле число x таке, що таке що $1 < x < p - 1$.

Обчислимо $y = g^x \, mod \, p = 2^8 \, mod \, 11 = 3$.

Отже, відкритим даними є трійка є $11, \, 2$ та 3, закритим ключем є число $x = 8$.

Для шифрування вибираємо випадкове ціле число $k = 9$ таке, що $1 < k < p - 1$.

Обчислюємо $a = g^k mod \, p = 2^9 mod \, 11 = 512 \, mod \, 11 = 6$.

Обчислюємо $b = y^k M \, mod \, p = 3^9 \cdot 5 \, mod \, 11 = 19683 \cdot 5 \, mod \, 11 = 9$.

Пара $(6, \, 9)$ є шифротекстом.

Шифротекст $(6, \, 9)$, закритий ключ $x = 8$.

Для дешифрування обчислюємо M за формулою:

$$M = b(a^x)^{-1} mod \, p == b \cdot a^{(p-1-x)} \, mod \, p = 9 \cdot \, 6^{(11-1-8)} mod \, 11 = 5.$$

Отримали початкове повідомлення $M = 5$.

АЛГОРИТМ ОБМІНУ КЛЮЧАМИ ДІФФІ-ХЕЛМАНА

Протокол обміну ключами Діффі-Хелмана дозволяє двом сторонам отримати спільний секретний ключ, використовуючи незахищений від прослуховування, але захищений від модифікації канал зв’язку. Отриманий ключ можна використовувати для симетричного шифрування повідомлень. Алгоритм заснований на складності обчислень дискретних логарифмів.

Припустимо, користувачі A і B мають намір обмінятися ключами за алгоритмом Діффі-Хелмана, суть якого полягає в наступному (рис. 6.2):

1. A і B спільно обирають просте число p і ціле число g таке, що $1 < g < p - 1$ і g є первісним коренем p.

Первісним коренем за модулем p називається таке число g, що при піднесення до степеню $g^i mod\ p$ всі його степені $i \in \{1, \dots, p-1\}$ за модулем p пробігають по всім числам взаємно простим із p.

Нехай $p = 5$. Усі взаємно прості числа з p: 1, 2, 3, 4.

*Елементи **2** та **3** є первісними коренями 5.*

1
$1^1 mod\ 5 = 1$
$1^2 mod\ 5 = 1$
$1^3 mod\ 5 = 1$
$1^4 mod\ 5 = 1$
2
$2^1 mod\ 5 = 2\ mod\ 5 = \mathbf{2}$
$2^2 mod\ 5 = 4\ mod\ 5 = \mathbf{4}$
$2^3 mod\ 5 = 8\ mod\ 5 = \mathbf{3}$
$2^4 mod\ 5 = 16\ mod\ 5 = \mathbf{1}$
3
$3^1 mod\ 5 = 3 \bmod 5 = \mathbf{3}$
$3^2 mod\ 5 = 9 \bmod 5 = \mathbf{4}$
$3^3 mod\ 5 = 27 \bmod 5 = \mathbf{2}$
$3^4 mod\ 5 = 81 \bmod 5 = \mathbf{1}$
4
$4^1 mod\ 5 = 4 \bmod 5 = 4$
$4^2 mod\ 5 = 16 \bmod 5 = 1$
$4^3 mod\ 5 = 64 \bmod 5 = 4$
$4^4 mod\ 5 = 256 \bmod 5 = 1$

2. Користувач A вибирає випадкове ціле число $x < p$, обчислює $x_A = g^x\ mod\ p$ та відправляє його користувачеві B.
3. Користувач B вибирає випадкове ціле число $y < p$, обчислює $y_B = g^y\ mod\ p$ та відправляє його користувачеві A.
4. Користувач A обчислює закритий ключ за формулою $k_A = y_B^x\ mod\ p$.
5. Користувач B обчислює закритий ключ за формулою $k_B = x_A^y\ mod\ p$.

Ці дві формули обчислення дають однакові результати. Відкритими параметрами є: p, g, x_A та y_B. Закриті параметри: x, y.

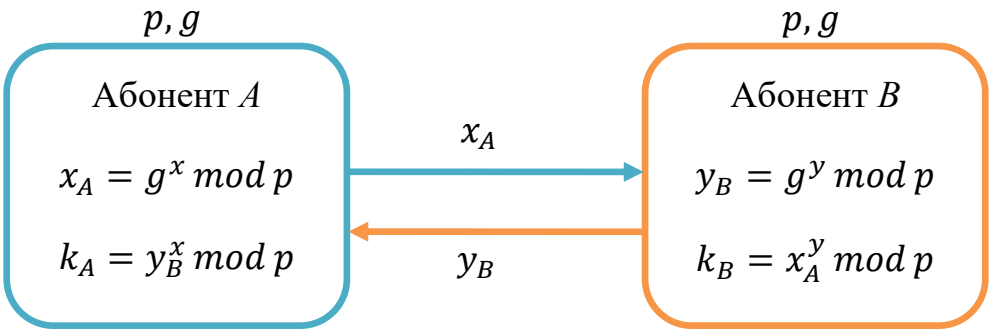

Рис. 6.2. Схема обміну ключами Діффі-Хелмана

Приклад 6.3:

1. Нехай p =11, g =2.
2. x = 4, обчислимо $x_A = 2^4 \, mod \, 11 = 16 \, mod \, 11 = 5$.
3. y = 6, обчислимо $y_B = 2^6 \, mod \, 11 = 64 \, mod \, 11 = 9$.
4. $k_A = 9^4 \, mod \, 11 = (9^2)^2 \, mod \, 11 = 4^2 \, mod \, 11 = 16 \, mod \, 11 = 5$.
5. $k_B = 5^6 \, mod \, 11 = (5^3)^2 \, mod \, 11 = 4^2 \, mod \, 11 = 16 \, mod \, 11 = 5$.

Секретний ключ, обчислений обома сторонами – 5.

Завдання до лабораторної роботи

Завдання 1

Реалізувати в середовищі MS Excel або на будь-якій мові програмування роботу асиметричного криптографічного алгоритму RSA. Кроки алгоритму шифрування зі скріншотами описати у звіті.

Значення параметрів p і q та відкритого ключа e визначається згідно варіанту. Зашифрувати число, що відповідає кількості літер у вашому прізвищі та дешифрувати отриманий шифротекст. Зразок виконання завдання наведено на рисунку нижче (рис. 6.3).

Генерація ключів RSA

p =	47
q =	71
n =	3337
φ(n) =	3220
e =	79
d =	1019

1

$ed \, mod \, \varphi(n) \equiv 1$

Перевірка 1

Розширений алгоритм Евкліда

i	r	q	u	v
0	3220		1	0
1	79		0	1
2	60	40	1	-40
3	19	1	-1	41
	3	3	4	-163
	1	6	-25	1019

Зашифрування

M	10	C	3269

$c = m^e \, mod \, n$

Дешифрування

C	3269	M	10

$m = c^d \, mod \, n$

Степені 79

1	10	10	2089	100	1014		
2	100	20	2462	200	400		
3	1000	30	801	300	1823		
4	3326	40	1452	400	3161		
5	3227	50	3232	500	1734		
6	2237	60	897	600	3014		
7	2348	70	1776	700	2841		
8	121	80	2657	800	943		
9	1210	90	1042	900	1820		
10	2089	100	1014	1000	119		

Степені 1019

1	3269	10	403	100	542		
2	1287	20	2233	200	108		
3	2583	30	2246	300	1807		
4	1217	40	811	400	1653		
5	669	50	3144	500	1610		
6	1226	60	2309	600	1663		
7	57	70	2841	700	356		
8	2798	80	332	800	2743		
9	3282	90	316	900	1741		
10	403	100	542	1000	2588		

Рис. 6.3. Реалізація шифру RSA в MS Excel

Варіант №	*p*	*q*	*e*
1.	41	43	23
2.	53	61	11
3.	29	37	31
4.	37	53	17
5.	67	79	23
6.	19	41	29
7.	23	83	21
8.	31	61	13
9.	17	97	13
10.	59	83	19
11.	103	107	11
12.	73	89	23
13.	53	61	23
14.	29	59	25
15.	37	47	19

Завдання 2

Реалізувати в середовищі MS Excel або на будь-якій мові програмування роботу асиметричного криптографічного алгоритму Ель-Гамаля. Кроки алгоритму шифрування зі скріншотами описати у звіті.

Значення параметрів p і g та закритого ключа x визначається згідно варіанту. Зашифрувати число, що відповідає кількості літер у вашому прізвищі та дешифрувати отриманий шифротекст. Зразок виконання завдання наведено на рисунку нижче (рис. 6.4).

	A	B	C	D	E	F	G	H
1	**Генерація ключів**			**Зашифрування**			**Дешифрування**	
2	*p* =	11		*M*	5		*a* =	6
3	*g* =	2		*k* =	9		*b* =	9
4	*x* =	8		*a* =	6		*M*	5
5	*y* =	3		*b* =	9			

Рис. 6.4. Реалізація шифру Ель-Гамаля в MS Excel

Варіант №	*p*	*g*	*x*	*k*
1.	13	6	10	4
2.	17	3	7	11
3.	11	7	5	6
4.	19	10	6	5
5.	23	5	16	11
6.	13	6	7	10
7.	11	7	9	7
8.	29	8	13	10
9.	23	5	16	9

Варіант №	p	g	x	k
10.	17	8	13	12
11.	19	13	11	9
12.	29	12	10	8
13.	17	6	8	15
14.	23	11	7	8
15.	13	7	10	11

Завдання 3

Реалізувати в середовищі MS Excel або на будь-якій мові програмування алгоритм обміну ключами Діффі-Хеллмана. Кроки алгоритму шифрування зі скріншотами описати у звіті.

Значення параметрів p і g та x і y визначається згідно варіанту. Обчислити значення відкритих параметрів x_A та y_B та здійснити обмін ними між абонентами. Визначити секретні ключі K_A та K_B, якими абоненти не обмінюються. Зразок виконання завдання наведено на рисунку нижче (рис. 6.5).

	A	B	C	D	E	F	G	H	I	J	K
1	p =	23									
2	g =	7									
3											
4	Абонент A						Абонент B				
5	x =	7					y =	8			
6	xA =	5		yB =	12		yB =	12		xA =	5
7	kA =	16					kB =	16			

Рис. 6.5. Реалізація алгоритму обміну ключами Діффі-Хелмана

Варіант №	p	g	Абонент A x	Абонент B y
1.	23	5	7	8
2.	13	6	4	5
3.	11	7	6	8
4.	17	6	4	7
5.	23	7	6	4
6.	19	3	7	5
7.	11	6	8	6
8.	17	3	4	9
9.	13	7	5	8
10.	19	2	8	6
11.	11	8	7	5
12.	23	10	5	4
13.	17	5	6	7

Варіант №	***p***	***g***	Абонент А ***x***	Абонент В ***y***
14.	19	10	7	4
15.	13	11	9	6

ДЗ: Знайти первісні корені 7?

Контрольні запитання:

1. У чому полягає ідея криптосистеми з відкритим ключем?
2. Поняття односторонньої функції.
3. Дайте характеристику алгоритму шифрування RSA.
4. На основі яких операцій відбувається створення закритого ключа із відкритого у RSA?
5. На чому заснована складність зламу алгоритму RSA?
6. Опишіть алгоритм шифрування Ель-Гамаля.
7. Опишіть алгоритм обміну ключами Діффі-Хелмана.
8. На чому базується криптостійкість протоколу обміну ключами Діффі-Хелмана?