МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, комп’ютерної та програмної інженерії

Кафедра інженерії програмного забезпечення



Лабораторна робота №6

з дисципліни «Безпека ПД»

На тему: «Дослідження асиметричної системи шифрування на основі алгоритму Ель Гамаля»

Варіант №6

Виконав студент:

групи ПІ-421Б

Іванюк Н. О.

Перевірив викладач:

Радішевський М. Ф.

Київ 2022

**Мета лабораторної роботи** – дослідження асиметричної системи шифрування: завдання параметрів системи, генерація відкритої та схованої частин ключа шифрування, сесійного ключа, шифрування та розшифрування повідомлення.

**Зміст звіту по роботі**

1. Титульний лист – назва роботи, група, прізвище студента, прізвище
2. викладача, що приймає роботу, дата виконання.
3. Мета роботи.
4. Номер варіанту завдання, значення p.
5. Розрахунок модуля шифрування m.
6. Таблиця знаходження генератора групи.
7. Таблиця шифрування повідомлення
8. Отримані шифровані дані та їх роз шифровка
9. Висновки по роботі.

**Виконання роботи**

Номер варіанта № = № по списку (mod 10) + 1

5(mod 10) + 1=5+1=6

P=43

m=

1. Знаходження утворюючого елемента групи g

Знайдемо утворюючий елемент g в мультиплікативній групі G(p,\*).

Обрахуємо порядок групи G(p,\*) ord(G(p,\*)) = ф(p).

ord(G(43,\*)) = ϕ(43) = 42.

Порядок групи = 42.

Перевіримо перші чотири кандидати на утворюючий елемент у таблиці 1

 Всього отримали 12 утворюючих елементів: {2,4,12,18,19,20,26,28,29,30,33,34}.

Перевіримо один з утворюючих елементів. Нехай це буде 18

за формулою: gi = (g1)Bi mod p , де Bi – числа, взаємно прості з ϕ(p).

Для p = 43, ϕ(43) = 42. Взаємно прості з 42: 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37,41 тобто 12 чисел.

*,,,*

*,,*

*,,,*

*,,*

Генератор 18 не дорівнює 1 при піднесенні у степінь, тому він є утворюючим.

**2. Знаходження закритої частини ключа x.**

Задаємо закриту частину ключа шифрування за формулою: 𝑥="день місяця дати народження"+3

Дата народження: 3.6.1997 р. 𝑥=3+3=6

Перевіримо умову: 1 < x < p – 1.

1 < 6 < 42. Умова виконується.

**3. Обрахування відкритої частини ключа y.**

Обрахуємо відкриту частину ключа за формулою:

Маємо наступні дані:

Публічні дані: **p** = 43, **g** = 18, **y** = 41;

Приватні дані: **x** = 6.

**4. Шифрування**

Для шифрування методом Ель Гамаля, необхідно обрати деяке слово з трьох літер. Нехай це буде англійське слово «MAY» (укр. «травень»).

Номери букв у слові MAY в англійській абетці: 13-1-25.

**1 сеанс.**

Треба вибрати сесійний ключ k, але який виконує умову: 1 < x < p – 1. Наприклад, нехай k = 28.

Далі рахуємо пару чисел (a, b) за формулами:

, де M – номер літери в абетці.

Шифротекст (a, b) = (36, 13).

**2 сеанс.**

Треба вибрати сесійний ключ k, але який виконує умову: 1 < x < p – 1. Наприклад, нехай k = 17.

Далі рахуємо пару чисел (a, b) за формулами:

, де M – номер літери в абетці.

Шифротекст (a, b) = (33, 35).

**3 сеанс.**

Треба вибрати сесійний ключ k, але який виконує умову: 1 < x < p – 1. Наприклад, нехай k = 31.

Далі рахуємо пару чисел (a, b) за формулами:

, де M – номер літери в абетці.

Шифротекст (a, b) = (26, 25).

|  |  |  |  |
| --- | --- | --- | --- |
| Відкриті параметри | Сеанси шифрування повідомлення “MAY”=13-1-25 | | |
| p = 43 | 1 сеанс, M | 2 сеанс, A | 3 сеанс, Y |
| g = 18 | a1 = 36 | a2 = 33 | a3 = 26 |
| y = 41 | b1 = 13 | b2 = 35 | b3 = 15 |

5. Розшифрування

Отримувач повідомлення може розшифрувати його за допомогою таємної частини ключа x. Вихідне повідомлення обчислюється за наступною формулою:

Розшифруємо повідомлення 1 сеансу (36, 13):

Розшифруємо повідомлення 2 сеансу (33, 25): = 1

Розшифруємо повідомлення 3 сеансу (26, 25): = 25

|  |  |  |
| --- | --- | --- |
| Отримані шифровані данні сеансів | | |
| 1 сеанс | 2 сеанс | 3 сеанс |
| a1 = 36 | a2 = 33 | a3 = 26 |
| b1 = 13 | b2 = 35 | b3 = 15 |
| Розшифровнані данні | | |
| M1 = 13 = “A” | M2 = 1 = “A” | M3 = 25 = “Y” |

**Висновок:** у ході даної лабораторної роботи я дослідив асиметричну систему шифрування Ель Гамаля, обрахував параметри системи, згенерував відкриту та сховану частини ключа шифрування, сесійний ключ та виконав шифрування та розшифрування повідомлення.