МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, комп’ютерної та програмної інженерії

Кафедра інженерії програмного забезпечення



Лабораторна робота №4

з дисципліни «Безпека ПД»

На тему: «Дослідження властивостей циклічних груп»

Варіант №5

Виконав студент:

групи ПІ-421Б

Іванюк Н. О.

Перевірив викладач:

Радішевський М. Ф.

Київ 2022

Мета роботи – дослідження властивостей циклічних груп класів лишків, на яких базується сучасна криптографія. Обчислення утворюючого елемента циклічної групи. Застосування утворюючого елемента в системі відкритого розповсюдження ключів.

**Завдання**

Завдання 1. Знайти утворюючі елементи g i в мультиплікативній групі G(p,\*) у відповідності з варіантом.

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

№ = 6



Обрахувати порядок групи G(p,\*) ord(G(p,\*)) = (р).

Знайти ймовірні порядки підгруп – дільники порядку групи.

Обрахувати кількість генераторів групи K= ( ord(G(p,\*))).

Скласти таблицю піднесення в ступінь для перших 8 елементів групи G(p,\*) у вигляді табл. 2.

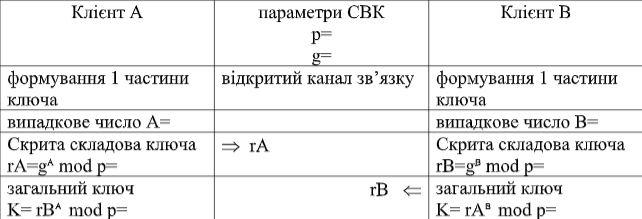
Проаналізувати результати та скласти таблицю (форма табл..3), яка містить підгрупи, їх порядок та порядок генератора групи.

Знайти перший мінімальний утворюючий елемент g групи G(p,\*).

Обрахувати решту утворюючих елементів групи по формулі g i = (g 1 ) Bi mod p , де B i – числа, взаємно прості з φ(p).

Завдання 2. Система відкритого розповсюдження ключів .

Застосувати результати завдання 1 для формування ключа на основі алгоритму Діффі – Хеллмана.



Параметр p заданий в таблиці № 4 варіантів завдання. Параметр g обирається студентом самостійно з знайдених генераторів в завданні №1.

Значення випадкових чисел, скриту складову ключа та загальний ключ записати у таблицю 5. Переконатися, що ключ К однаковий для обох сторін.

**Виконання роботи**

Завдання 1.

p=37



G(p,\*)=[1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36]

K=φ(φ(37))= φ (37-1)= φ (3\*3\*2\*2)=12

|  |  |  |  |
| --- | --- | --- | --- |
| Кандидати в генератори | Згенерована група Hg | Порядок групи Hg | Порядок групи Hg ord g |
| 2 | 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, 34, 35, 36 | 36 | 36 |
| 3 | 1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36 | 18 | 18 |
| 4 | 1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36 | 18 | 18 |
| 5 | 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, 34, 35, 36 | 36 | 36 |
| 6 | 1, 6, 31, 36 | 4 | 4 |
| 7 | 1, 7, 9, 10, 12, 16, 26, 33, 34 | 9 | 9 |
| 8 | 1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36 | 12 | 12 |
| 9 | 1, 7, 9, 10, 12, 16, 26, 33, 34 | 9 | 9 |
| 10 | 1, 10, 26 | 3 | 3 |
| 11 | 1, 10, 11, 26, 27, 36 | 6 | 6 |
| 12 | 1, 7, 9, 10, 12, 16, 26, 33, 34 | 9 | 9 |
| 13 | 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, 34, 35, 36 | 36 | 36 |
| 14 | 1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36 | 12 | 12 |
| 15 | 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, 34, 35, 36 | 36 | 36 |
| 16 | 1, 7, 9, 10, 12, 16, 26, 33, 34 | 9 | 9 |
| 17 | 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, 34, 35, 36 | 36 | 36 |
| 18 | 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, 34, 35, 36 | 36 | 36 |
| 19 | 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, 34, 35, 36 | 36 | 36 |
| 20 | 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, 34, 35, 36 | 36 | 36 |
| 21 | 1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36 | 18 | 18 |
| 22 | 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, 34, 35, 36 | 36 | 36 |
| 23 | 1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36 | 12 | 12 |
| 24 | 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, 34, 35, 36 | 36 | 36 |
| 25 | 1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36 | 18 | 18 |
| 26 | 1, 10, 26 | 3 | 3 |
| 27 | 1, 10, 11, 26, 27, 36 | 6 | 6 |
| 28 | 1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36 | 18 | 18 |
| 29 | 1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36 | 12 | 12 |
| 30 | 1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36 | 18 | 18 |
| 31 | 1, 6, 31, 36 | 4 | 4 |
| 32 | 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, 34, 35, 36 | 36 | 36 |
| 33 | 1, 7, 9, 10, 12, 16, 26, 33, 34 | 9 | 9 |
| 34 | 1, 7, 9, 10, 12, 16, 26, 33, 34 | 9 | 9 |
| 35 | 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, 34, 35, 36 | 36 | 36 |
| 36 | 1, 36 | 2 | 2 |

Перший утворюючий елемент групи це 2.

Інші утворюючі елементи групи це 5,13,15,17,18,19,20,22,24,32,35.

Завдання 2.

|  |  |  |
| --- | --- | --- |
| Клієнт А | Параметри СВК  p=37,  g=15 | Клієнт В |
| Формування 1 частини ключа | Відкритий канал зв`язку | Формування 1 частини ключа |
| Випадкове число А=16 |  | Випадкове число B=3 |
| Скрита складова ключа 12 |  | Скрита складова ключа 8 |
| Загальний ключ  26 |  | Загальний ключ  26 |