МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, комп’ютерної та програмної інженерії

Кафедра інженерії програмного забезпечення



Лабораторна робота №5

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

**Завдання**

Розрахувати параметри системи шифрування RSA у відповідності з варіантом завдання (номер варіанту дорівнює номеру студент у списку групи). Зашифрувати та розшифрувати повідомлення з 3 літер.

**Програмні засоби**

Калькулятор в класі лишків, що був розроблений в попередньої лабораторної роботі.

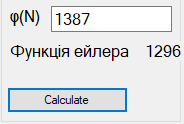
**Порядок виконання роботи**

1. Знайти модуль кільця m=p\*q, в якому буде виконуватися шифрування. Числа p, q задані в таблиці «Варіанти завдань». Перевірку простоти чисел зробити за допомогою калькулятора на основі малої теореми Ферма.
2. Знайти модуль кільця n=f(p\*q)=(p–1)\*(q-1) в якому будуть вибиратися ключі.
3. Знайти кількість чисел, взаємно простим з n за допомогою функції Ейлера f(n). Ця величина поділена на 2 вказує на кількість можливих ключів.
4. Вибрати сховану частину ключа x, який є взаємно простим з n. Взаємну простоту перевіряти шляхом знаходження НОД(x, n). Він повинен бути рівним 1.
5. Знайти відкриту частину ключа y з рівняння x\*y  1 mod n. Тобто y = x -1 зворотне число в мультиплікативній групі. Це можна зробити застосував функцію Ейлера.
6. Знайти другу пару ключів.
7. Задати слово в якому 3 різних літери (англійське або українське). Замінити кожну літеру її порядковим номером у вибраному алфавіті. Зашифрувати послідовність чисел шляхом піднесення їх в степінь e (відкрита частина ключа) за допомогою калькулятора.
8. Розшифрувати повідомлення відкритою частиною ключа.

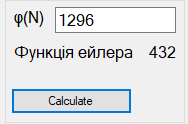
**Виконання**

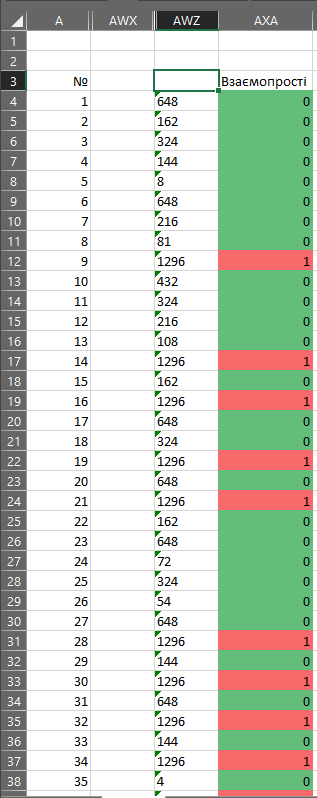
Варіант 5

1. Знайдемо модуль кільця



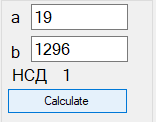
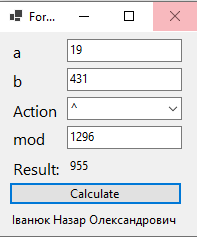
1. Знайдемо модуль кільця в якому будуть вибиратися ключі
2. Знайдемо кількість чисел, взаємно простих з n за допомогою функції Ейлера

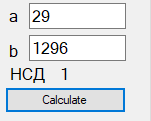
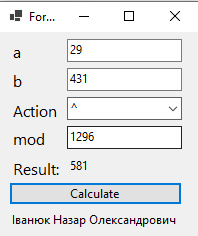


\

1. Виберемо сховану частину ключа ***x***, який є взаємно простим з ***n***.

**X = 19; НОД (19, 955) = 1**

** **

** **

1. Знайдемо відкриту частину ключа **y**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| х | 9 | 14 | 16 | 19 | 21 | 28 | 29 | 30 | 32 | 34 | 36 | 42 | 43 | 44 | 50 |
| y | 729 | 272 | 400 | 955 | 1053 | 784 | 581 | 0 | 848 | 112 | 0 | 0 | 211 | 1088 | 128 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| прості числа | | модуль шифрування | модуль групи вибору ключів | 1 пара ключів | | 2 пара ключів | |
| p | Q | M | N | x | y | X | Y |
| 19 | 73 | 1 387 | 1 296 | 19 | 955 | 29 | 581 |

***Результати шифрування***

Відкриті параметри системи:

модуль шифрування n =

відкрита частина ключа y = 955

b1 = 16955 mod = 16

b2 = 12955 mod = 791

b3 = 22955 mod = 136

|  |  |  |  |
| --- | --- | --- | --- |
| Вихідне повідомлення | Л | І | С |
| Числовий код букв повідомлення | 16 | 12 | 22 |
| Зашифрований числовий код повідомлення | 16 | 791 | 136 |

***Результати розшифрування:***

модуль шифрування n =

схована частина ключа x = 19

a1=1619 mod = 16 = «Л»

a2=79119 mod = 12 = «І»

a3=13619 mod = 22 = «С»

|  |  |  |  |
| --- | --- | --- | --- |
| Зашифрований числовий код повідомлення | 16 | 791 | 136 |
| Розшифрований числовий код повідомлення | 16 | 12 | 22 |
| Розшифроване текстове повідомлення | Л | І | С |

***Результати шифрування***

Відкриті параметри системи:

модуль шифрування n =

відкрита частина ключа y = 581

b1 = 16955 mod = 4

b2 = 1281 mod = 559

b3 = 2281 mod = 927

|  |  |  |  |
| --- | --- | --- | --- |
| Вихідне повідомлення | Л | І | С |
| Числовий код букв повідомлення | 16 | 12 | 22 |
| Зашифрований числовий код повідомлення | 4 | 559 | 927 |

***Результати розшифрування:***

модуль шифрування n =

схована частина ключа x = 29

a1=429 mod = 16 = «Л»

a2=55929 mod = 12 = «І»

a3=92729 mod = 22 = «С»

|  |  |  |  |
| --- | --- | --- | --- |
| Зашифрований числовий код повідомлення | 1 127 | 1 129 | 1 020 |
| Розшифрований числовий код повідомлення | 16 | 12 | 22 |
| Розшифроване текстове повідомлення | Л | І | С |

**Висновки:** Під час виконання лабораторної роботи я дослідив асиметричні системи шифрування, генерацію відкритої та схованої частин ключа шифрування.