Національний технійчний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

«Криптографія»

Комп’ютерний практикум №4

Вивчення криптосистеми RSA та електронного підпису; ознайомлення з методами генерації параметрів для асиметричних криптосистем

Виконали:

ФБ-21 Жиговець Олександр

ФБ-21 Альгішиєв Дмитро

Мета: Ознайомлення з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA; практичне ознайомлення з системою захисту інформації на основі криптосхеми RSA, організація з використанням цієї системи засекреченого зв'язку й електронного підпису, вивчення протоколу розсилання ключів.

Варіант: 3

Хід роботи

(В прикладах вказані значення на момент скріншотів, код писався походу і після кожного запуску значення змінюються)

1. Написати функцію пошуку випадкового простого числа з заданого інтервалу або заданої довжини

   В функції num_generator генерується випадкове число в заданому інтервалі до тих пір, поки згенероване число не пройде тест Міллера-Рябіна.

2. За допомогою цієї функції згенерувати дві пари простих чисел.

```
p = 783025403896939424740768132783727523844376375312979765487922358295792623902 59
q = 968800601864095330262081803667531458011055444189650761059759765477468811377 39
p1 = 765261431886040527572708251143559464740606009947040115279521683649519223418 69
q1 = 107119939379738677568589884199808458527975582492265400186448070546953987009831
```

3. Написати функцію генерації ключових пар для RSA.

   В функцію для генерації на вхід передається об’єкт Pair із значеннями p, p1, q, q1. В самій функції обчислюються потрібні значення, після чого повертається результат.

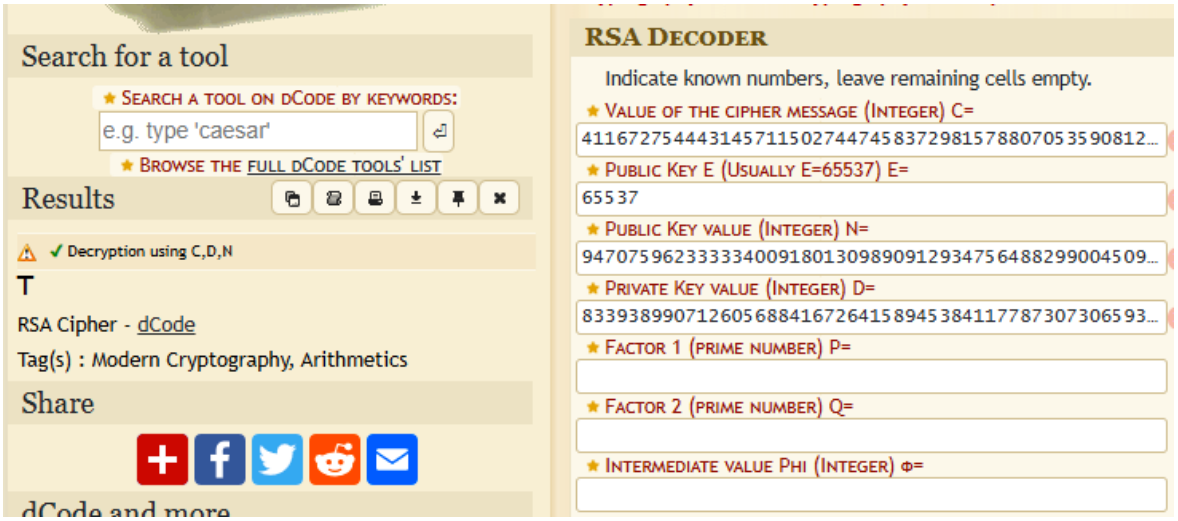
4. Написати програму шифрування, розшифрування і створення повідомлення з цифровим підписом для абонентів A і B.

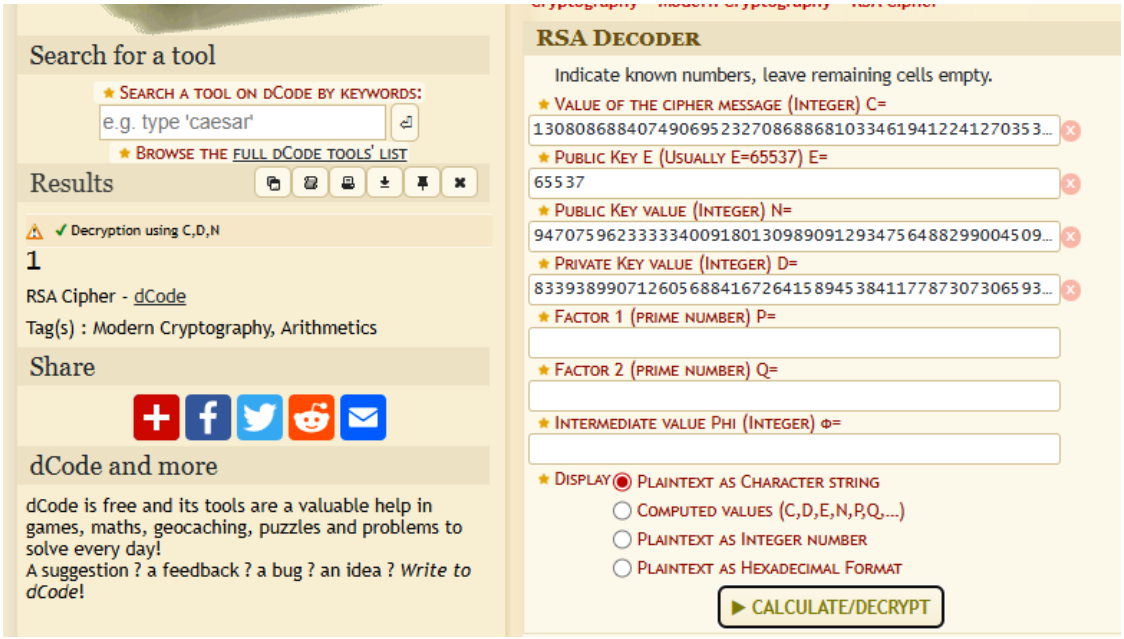
   В коді є реалізовано 4 функції: Encrypt, Decrypt, Sign та Verify. Дві перші для шифрування/дешифрування, дві інші для роботи з цифровим підписом.

5. За допомогою раніше написаних на попередніх етапах програм організувати роботу протоколу конфіденційного розсилання ключів

   Ключ k шифрується публічним ключем отримувача, потім підписується приватним ключем відправника. Ключ k дешифрується приватним ключем отримувача, після чого виконується функція Verify, що перевіряє підпис.

Перевірка за допомогою онлайн інструменту, було зашифровано повідомлення “Test1”, за допомогою онлайн інструменту спробували розшифрувати першу букву повідомлення, отримали T





І останній символ повідомлення – отримали 1, як і початковому повідомленні

Висновки

Під час виконання завдань у цій роботі ми навчились перевіряти числа на простоту за допомогою тесту Міллера-Рябіна. Попрацювали із криптосистемою RSA, навичлись шифрувати, дешифрувати та перевіряти підпис.