Міністерство освіти і науки України
НТУУ «Київський політехнічний інститут»

Фізико-технічний інститут
Кафедра інформаційної безпеки

Криптографія

Лабораторна робота №4

Виконали:

Студент
3 курсу ФТІ групи
ФБ-95
Прохоренко
Ярослав

Студент
3 курсу ФТІ
групи ФБ-95
Тригубенко
Олександр

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.

Хід роботи:

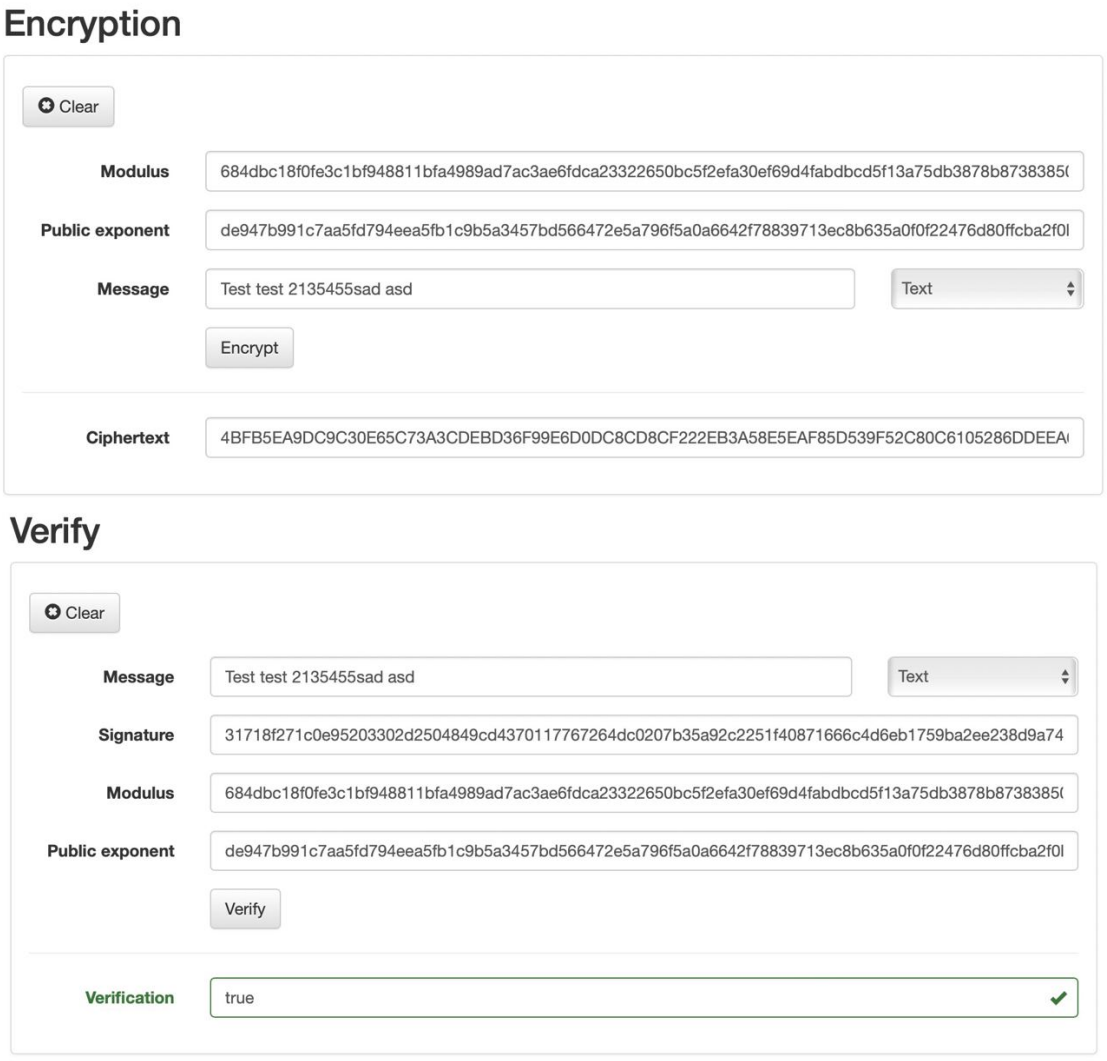
1. При запуску програма створює двох персон “First User” і “Second User”, які обмінюються повідомленнями:
2. Разом зі створенням персон, генеруються псевдопрості числа, що в подальшому використовуються для шифрування;
3. Персона “First User” генерує повідомлення для персони “Second User”. Для вона має:
    1. Згенерувати відкритий ключ, менший ніж у “Second User” inf < sup;
    2. Закодувати і зашифрувати повідомлення;
    3. Згенерувати підпис.
4. Персона “Second User” отримує пакет даних, що містить повідомлення з підписом та відкритий ключ “First User”;
5. Персона “Second User” розшифровує повідомлення:
    1. Розшифровує повідомлення своїм секретним(d) та відкритим ключем (inf);
    2. Розшифровує підпис своїм секретним(d) та відкритим ключем (inf);
    3. Перевіряє підпис з повідомленням;
    4. Виводить повідомлення або помилки;

Результат виконання програми:

```
/usr/bin/python3 /Users/augfitzr/Desktop/gh/yaebaltvoyutelku/crypto-FB-9/cp4/Prokhorenko_Tryhubenko_FB95_cp4/Mydoom.py
Encrypted message: 0x8b97728c990c839980418e251aa4f173dd9c213b17511e2135da781cffa7481a0f305d4064e152a4fa991ff533123af5503c597070e4551cc38e68b3ed06f03f
Signature of the message: 0x4c0e849d6a0144980d6bd8a502c8205cf6900481a0e2ccb242d2d487ab1d039b58ca340b5bf70605dd139b7a1a416cdc4878078ac54f7f8a50c1fe84f2da8807

Ok!
Msg: Test text 1234
```

Перевірка на сайті:




```
/usr/bin/python3 /Users/augfitzr/Desktop/gh/yaebaltvoyutelku/crypto-FB-9/cp4/Prokhorenko_Tryhubenko_FB95_cp4/Mydoom.py
Mod: 684dbc18f0fe3c1bf948811bfa4989ad7ac3ae6fdca23322650bc5f2efa30ef69d4fabdbcd5f13a75db3878b87383850e2d81e74846b0d1a680fd3233120c097
Pub exp: de947b991c7aa5fd794eea5fb1c9b5a3457bd566472e5a796f5a0a6642f78839713ec8b635a0f0f22476d80ffcba2f0b49f2b91d0a1e55fe0c39762c61dfb05
CT: 4bfb5ea9dc9c30e65c73a3cdebd36f99e6d0dc8cd8cf222eb3a58e5eaf85d539f52c80c6105286ddeea68eae065e3dd2917c94f4534a10d325b2ac43ee50f89b
Sign: 31718f271c0e95203302d2504849cd4370117767264dc0207b35a92c2251f40871666c4d6eb1759ba2ee238d9a74d07ab5a210bcdaf4112c5766ef9d648aa4f9
```

Висновки: Виконавши лабораторну роботу, ми ознайомились з різними тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA; ознайомились з системою захисту інформації на основі криптосхеми RSA на практиці, організували засекречений зв'язок та електронний підпис, вивчили основні принципи протоколу розсилання ключів.