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-92
Сьомченко Дмитро

Студент
3 курсу ФТІ
групи ФБ-94
Стражник Богдан

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 “A” і “B”, які обмінюються повідомленнями:
2. Разом зі створенням персон, генеруються псевдопрості числа, що в подальшому використовуються для шифрування;
3. Персона “A” генерує повідомлення для персони “B”. Для вона має:
    1. Згенерувати відкритий ключ, менший ніж у “B” n < n1;
    2. Закодувати і зашифрувати повідомлення;
    3. Згенерувати підпис.
4. Персона “B” отримує пакет даних, що містить повідомлення з підписом та відкритий ключ “A”;
5. Персона “B” розшифровує повідомлення:
    1. Розшифровує повідомлення своїм секретним(d) та відкритим ключем (n);
    2. Розшифровує підпис своїм секретним(d) та відкритим ключем (n);
    3. Перевіряє підпис з повідомленням;
    4. Виводить повідомлення або помилки;

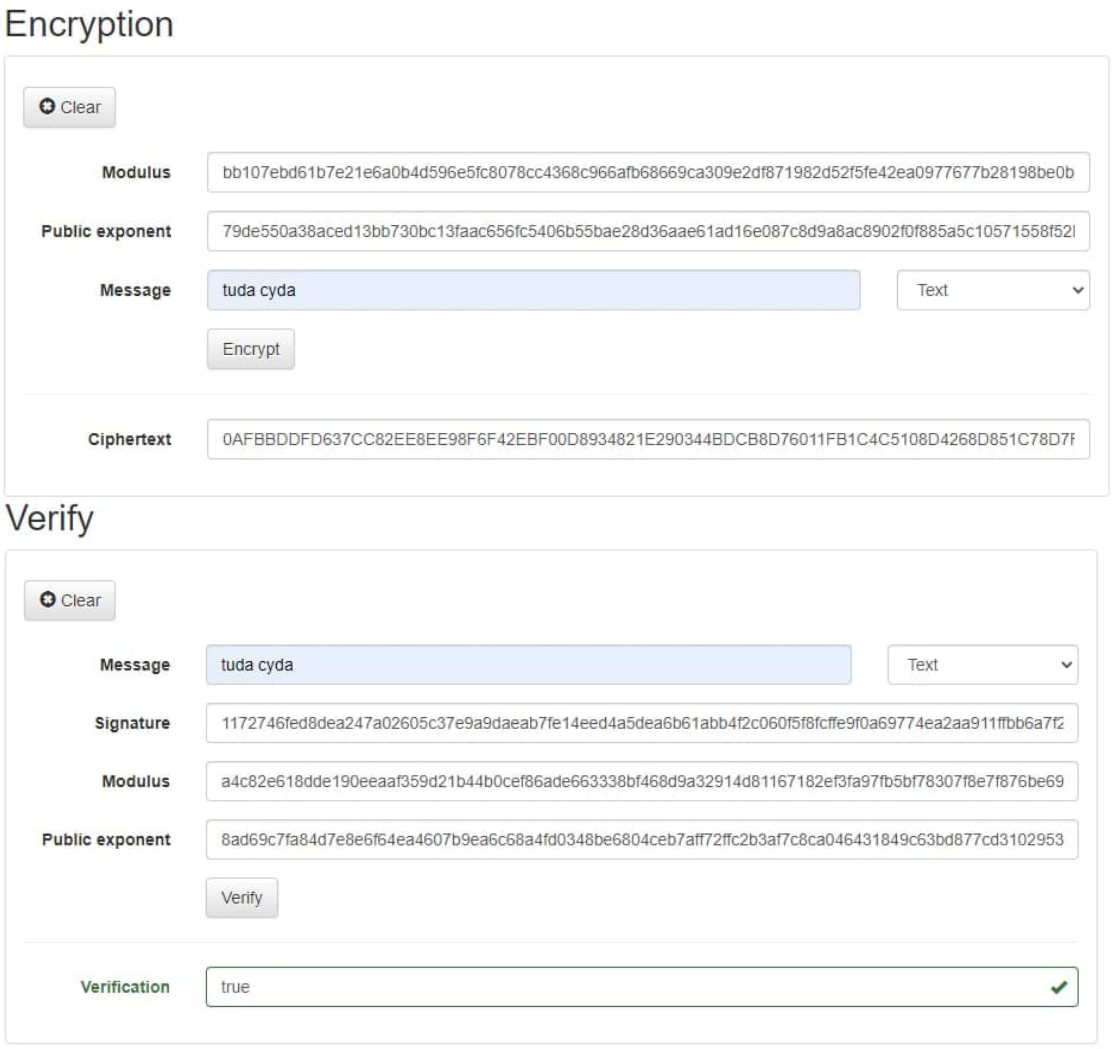
Результат виконання програми:

```
/usr/local/bin/python3.9 /Users/smchnk/Documents/Univ/Crypto/crypto-FB-9/cp4/somchenko_fb92_strazhnik_fb94_cp4/deadinside.py
Encrypted message: 0x5921a1fb08356c90980f7da79bfecbf62ed4c0553988678039cb5ad2b5793c83912039e8f046d24de9c16930464b52bd13967b896d7de24041de00caf0a874c5
Signature of the message: 0x563a4300add0c5b48ca077a7eeaf5455b2cd7245a0600a888122f5f6e4090145d9fa17e575e135c67dace23ec3bba2a638f56bc310e6532fd34abb37111cd251

Verification passed
Received message: ny kak bu da

Process finished with exit code 0
```

Перевірка на сайті:




```
modulus: a4c82e618dde190eeaaf359d21b44b0cef86ade663338bf468d9a32914d81167182ef3fa97fb5bf78307f8e7f876be69fd949d867ec9f57e57c820237a07bd61
public exponent: 8ad69c7fa84d7e8e6f64ea4607b9ea6c68a4fd0348be6804ceb7aff72ffc2b3af7c8ca046431849c63bd877cd31029537007ea6435f197e91894836752a8cb67
ciphertext: dc8f1d8b3bafcf254bf70c26e2f37571a8df486a803e125b5ecd50332083f09ac211183feff5f983e20537d142148ae81335575d3cbbb5ee2074235835a1848
signature: 1172746fed8dea247a02605c37e9a9daeab7fe14eed4a5dea6b61abb4f2c060f5f8fcffe9f0a69774ea2aa911ffbb6a7f2948e53759d501adde6182332156e2
```

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.