Міністерство освіти і науки України

Національний технічний університет України

"Київський політехнічний інститут імені Ігоря Сікорського"

Фізико-технічний інститут

КРИПТОГРАФІЯ

Комп’ютерний практикум

Робота № 4

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

Виконав:

студент гр. ФБ-02

Шубін Д.Ю

Мета роботи:

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.

Порядок виконання роботи:

1. Написати функцію пошуку випадкового простого числа з заданого інтервалу або заданої довжини, використовуючи датчик випадкових чисел та тести перевірки на простоту. В якості датчика випадкових чисел використовуйте вбудований генератор псевдовипадкових чисел вашої мови програмування. В якості тесту перевірки на простоту рекомендовано використовувати тест Міллера-Рабіна із попередніми пробними діленнями. Тести необхідно реалізовувати власноруч, використання готових реалізацій тестів не дозволяється.

2. За допомогою цієї функції згенерувати дві пари простих чисел p, q і p_1, q_1 довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб $pq \le p_1 q_1$; p і q – прості числа для побудови ключів абонента A, p_1 і q_1 – абонента B.

3. Написати функцію генерації ключових пар для RSA. Після генерування функція повинна повертати та/або зберігати секретний ключ (d, p, q) та відкритий ключ (n, e). За допомогою цієї функції побудувати схеми RSA для абонентів A і B – тобто, створити та зберегти для подальшого використання відкриті ключі (e, n), (e_1, n_1) та секретні d і d_1.

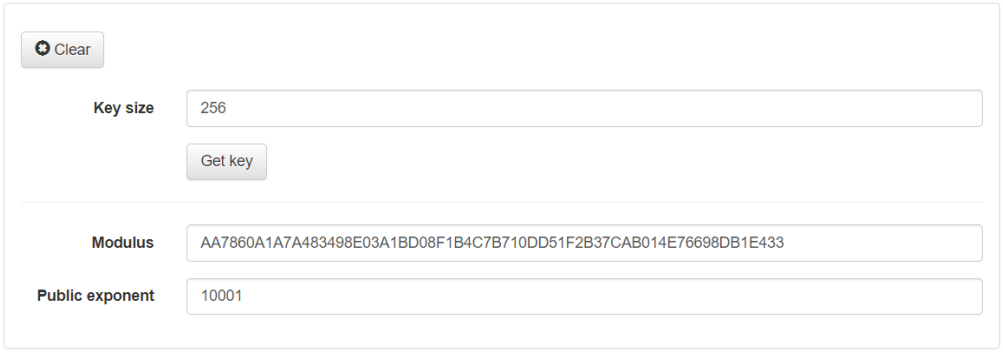
4. Написати програму шифрування, розшифрування і створення повідомлення з цифровим підписом для абонентів A і B. Кожна з операцій (шифрування, розшифрування, створення цифрового підпису, перевірка цифрового підпису) повинна бути реалізована окремою процедурою, на вхід до якої повинні подаватись лише ті ключові дані, які необхідні для її виконання.

За допомогою датчика випадкових чисел вибрати відкрите повідомлення M і знайти криптограму для абонентів A и B, перевірити правильність розшифрування. Скласти для A і B повідомлення з цифровим підписом і перевірити його.

5. За допомогою раніше написаних на попередніх етапах програм організувати роботу протоколу конфіденційного розсилання ключів з підтвердженням справжності по відкритому каналу за допомогою алгоритму RSA. Протоколи роботи кожного учасника (відправника та приймаючого) повинні бути реалізовані у вигляді окремих процедур, на вхід до яких повинні подаватись лише ті ключові дані, які необхідні для виконання. Перевірити роботу програм для випадково обраного ключа $0 < k < n$.

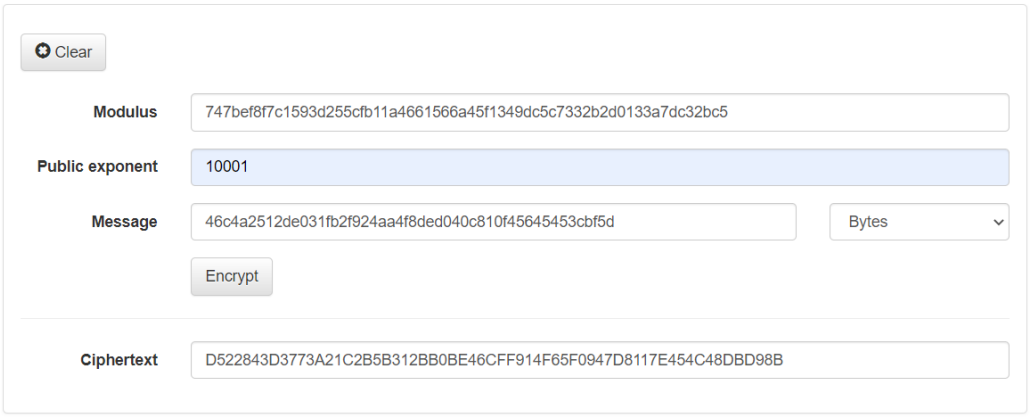
Хід роботи:

Get server key



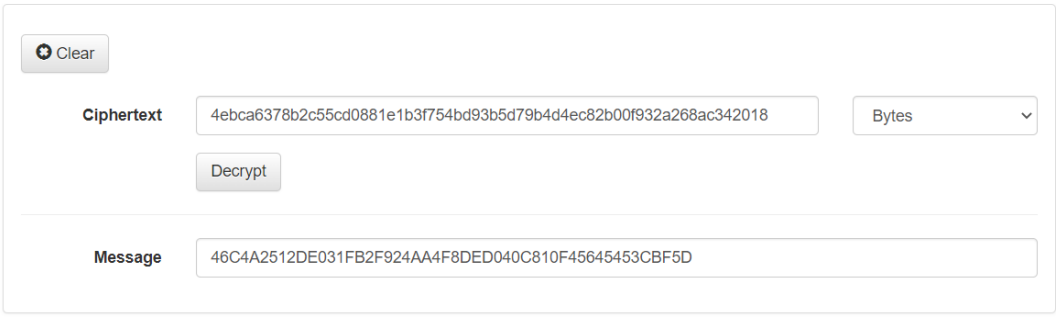

```
Наш відкритий ключ:
 n: 747bef8f7c1593d255cfb11a4661566a45f1349dc5c7332b2d0133a7dc32bc5
 e: 10001
Наш секретний ключ:
 d: 57e104abe87e52e6758cda5d2b49d61f41a77865520775e2c3b27d028dc5045
 p: f37b727258dd080da3d9ccbf68ca0fd3
 q: 7a7905f68a9b114e0064f73bb372f07
Відкритий ключ сайту:
 n: aa7860a1a7a483498e03a1bd08f1b4c7b710dd51f2b37cab014e76698db1e433
 e: 10001
Повідомлення: 46c4a2512de031fb2f924aa4f8ded040c810f45645453cbf5d
```

Encryption



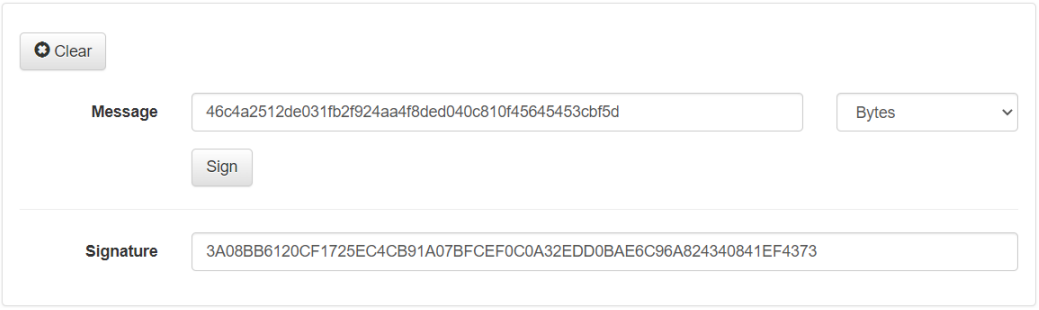

```
------ Сайт шифрує, ми розшифровуємо: ------
введіть шифротекст сайту:D522843D3773A21C2B5B312BB0BE46CFF914F65F0947D8117E454C48DBD98B
C: D522843D3773A21C2B5B312BB0BE46CFF914F65F0947D8117E454C48DBD98B
M: 46c4a2512de031fb2f924aa4f8ded040c810f45645453cbf5d
Правильність повідомлення: True
```

Decryption




```
------ Ми шифруємо, сайт розшифровує: ------
M: 46c4a2512de031fb2f924aa4f8ded040c810f45645453cbf5d
C: 4ebca6378b2c55cd0881e1b3f754bd93b5d79b4d4ec82b00f932a268ac342018
введіть розшифроване повідомлення сайту:46C4A2512DE031FB2F924AA4F8DED040C810F45645453CBF5D
Сайт розшифрував: 46c4a2512de031fb2f924aa4f8ded040c810f45645453cbf5d
Правильність повідомлення: True
```

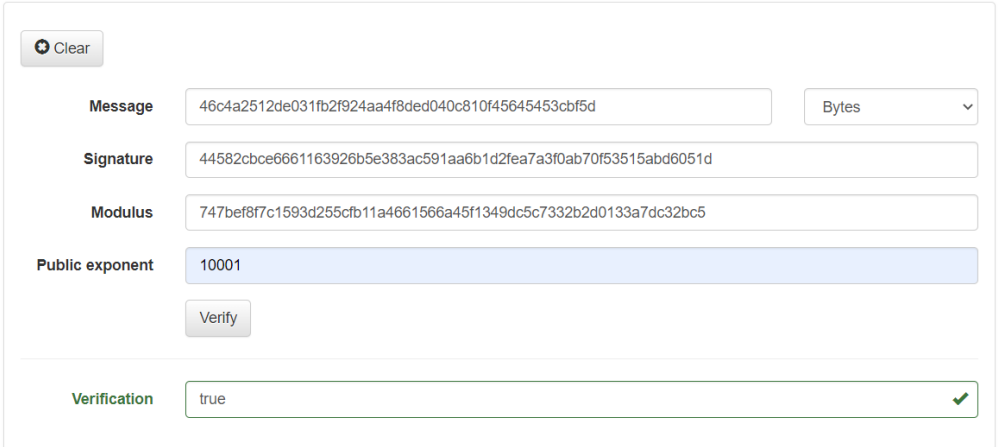
Sign



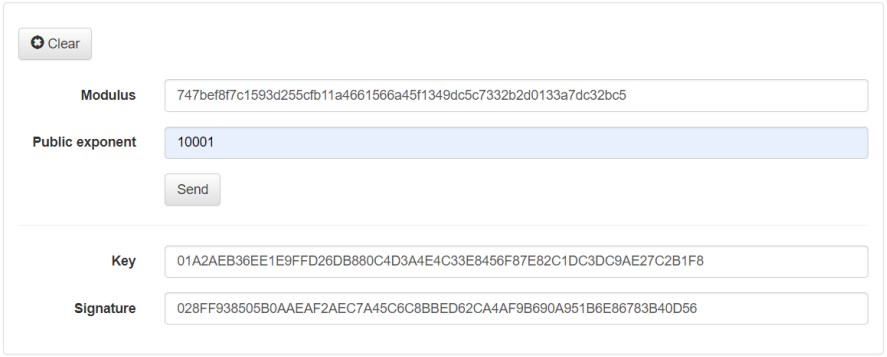

```
------ Сайт підписує, ми перевіряємо: ------
M: 46c4a2512de031fb2f924aa4f8ded040c810f45645453cbf5d
введіть підпис сайту:3A08BB6120CF1725EC4CB91A07BFCEF0C0A32EDD0BAE6C96A824340841EF4373
Verification: True
```

```
------ Ми підписуємо, сайт перевіряє: ------
M: 46c4a2512de031fb2f924aa4f8ded040c810f45645453cbf5d
Підпис: 44582cbce6661163926b5e383ac591aa6b1d2fea7a3f0ab70f53515abd6051d
```

Verify



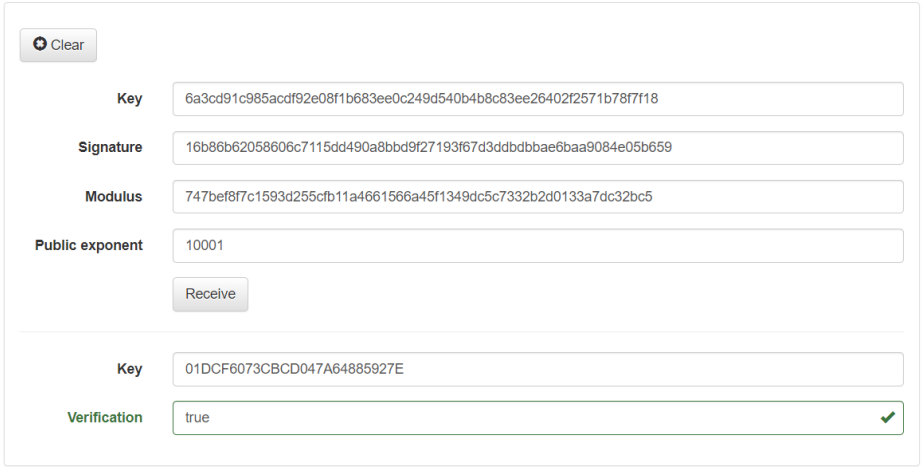
Send key




```
------ Сайт надсилає ключ, ми отримуємо: ------
Наш відкритий ключ:
 n: 747bef8f7c1593d255cfb11a4661566a45f1349dc5c7332b2d0133a7dc32bc5
 e: 10001
введіть ключ сайту:01A2AEB36EE1E9FFD26DB880C4D3A4E4C33E8456F87E82C1DC3DC9AE27C2B1F8
введіть підпис сайту:028FF938505B0AAEAF2AEC7A45C6C8BBED62CA4AF9B690A951B6E86783B40D56
received key: 18288995500720947037
authentication: True
```

```
------ Ми надсилаємо ключ, сайт отримує: ------
Ключ: 1dcf6073cbcd047a64885927e
K1: 6a3cd91c985acdf92e08f1b683ee0c249d540b4b8c83ee26402f2571b78f7f18
S1: 16b86b62058606c7115dd490a8bbd9f27193f67d3ddbdbbae6baa9084e05b659
Наш відкритий ключ:
 n: 747bef8f7c1593d255cfb11a4661566a45f1349dc5c7332b2d0133a7dc32bc5
 e: 10001
```

Receive key



Висновок: у ході лабораторної роботи, я ознайомився з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA; практично ознайомився з системою захисту інформації на основі криптосхеми RSA, організував з використанням цієї системи засекреченого зв'язку й електронного підпису, вивчив протокол розсилання ключів.