Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

Лабораторна робота №5

З предмету «Криптографія»

Виконали:
студенти 3 курсу ФТІ
групи ФБ-73
Пазон Б.Р.
Лутак А.О.
Перевірили:
Чорний О.
Савчук М. М.
Завадська Л. О.

Київ 2019

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 1 1 p , q довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб p1q1 □pq ; p і q – прості числа для побудови ключів абонента А, 1 p і q1 – абонента В.

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 А і В – тобто, створити та зберегти для подальшого використання відкриті ключі (e,n) , (,) 1 n1 e та секретні d і d1 .

4. Написати програму шифрування, розшифрування і створення повідомлення з цифровим підписом для абонентів А і В. 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 М і знайти криптограму для абонентів А и В, перевірити правильність розшифрування. Скласти для А і В 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 n.□ k □0

Результати:

p=8853538799782236604719345228255728233751499288144787821527987472609466493995 1

q=10888587692092211679317090144787315041127885849056612724289688248167432364976 9

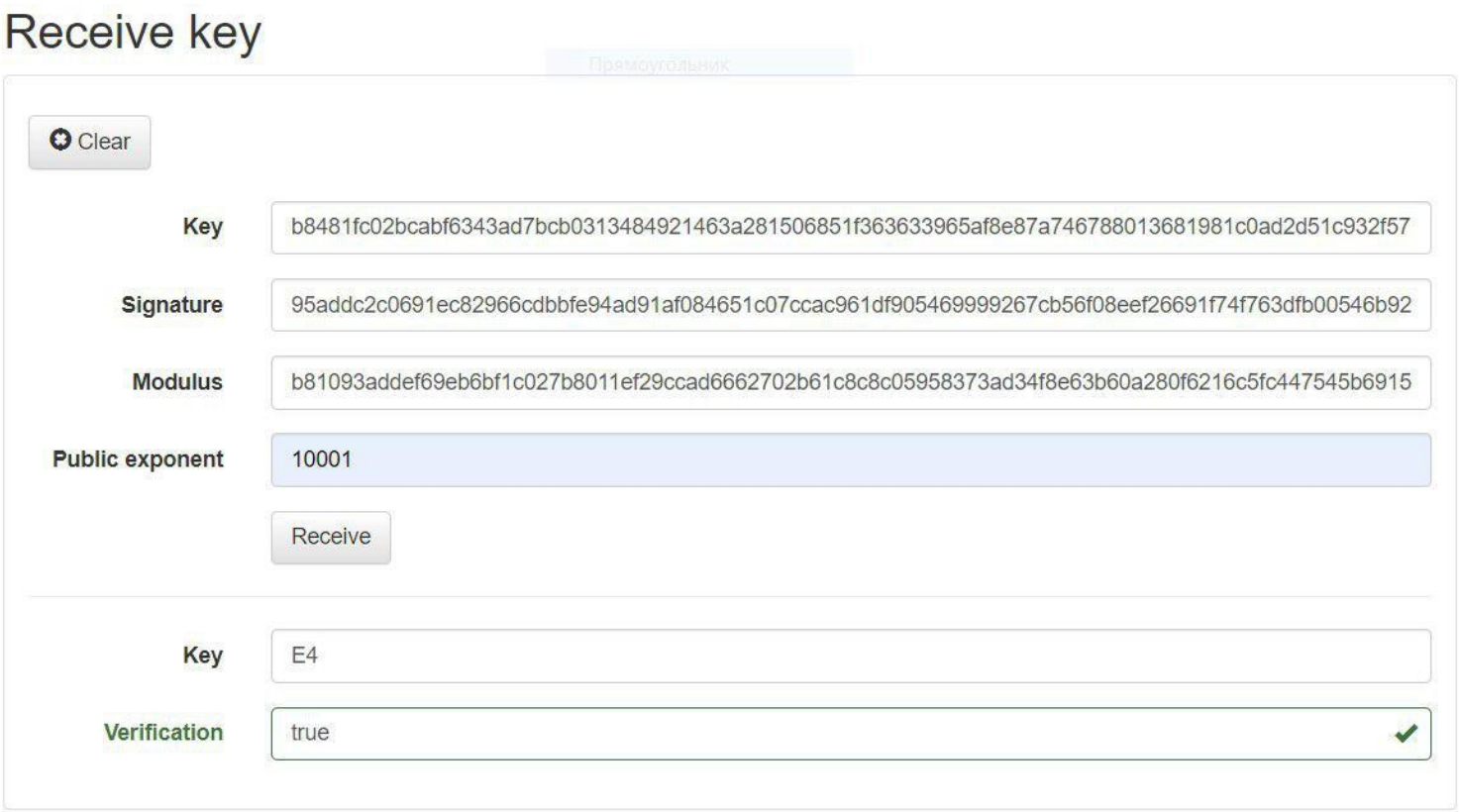
d=70517989244374018692234634363143303633406970291168022218451670864063476844425929545407884255985234463371324374523190901598861338511090522154600838200654 73

e=65537

n=96402533606769713455005866338283744059711986065337477516284254347478683394936103220104266929277805208534519271643432079483360848064622225445379215400213 19

key=b8481fc02bcabf6343ad7bcb0313484921463a281506851f363633965af8e87a746788013681981c0ad2d51c932f5723e1759397ca4255ef793901c26e70db08

signature=95addc2c0691ec82966cdbbfe94ad91af084651c07ccac961df905469999267cb56f08eef26691f74f763dfb00546b92a6eb49b9c345798eecf952e2da9b3dc1



Висновок:

У ході комп’ютерного практикуму було набуто навичок роботи з числами великої розрядності, написання тестів перевірки чисел на простоту та методів генерації ключів для асиметричної криптосистеми RSA. Також набуто навичок побудови цифрового підпису на основі криптосистеми RSA.