Міністерство освіти і науки України
НТУУ«Київський політехнічний інститут»
Фізико-технічний інститут

КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ No4

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

Виконали:
студент групи ФБ-84
Ніколаєнко Едуард
студент групи ФБ-84

Коцюк Роман

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 p1, q1 довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб pq ≤ p1, q1; p і q – прості числа для побудови ключів абонента A, p1, q1– 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), (e1, n1) та секретні d, d1.

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 $0 < k < n$.

Значення вибраних чисел p, q, q1, p1 із зазначенням кандидатів, що не пройшли тест перевірки простоти і параметрів криптосистеми RSA для абонентів A і B:

A:

p = e92dc85f6fbd43ce0275c79481f7c80600fabd429a364af2d6761c1f540db8c9

q = 8e1c0098f0e37598578d3a825badb7d2ee7ed38f577c4953029b094f18388683

публичный ключ:

exponent: 10001,

modulus:
8170e6b229044788dd2929a2ac4ce9e20802d1559c8e4f17953bfa03076ce58f833894d3d933b0d8811068ff41d73f78b97249c313cd748987528d6175b6c4db

секретный ключ:

exponent:
15749058b1a1caf5adaaf802c5ca8dedf063ff2cd0a16a0cbfa8cc5d1a2afbb5dad67f25e6cb7d8687609a5124e2761fd74b89e43641fc305bbeedab04428971

B:

публичный ключ:

exponent: 10001,

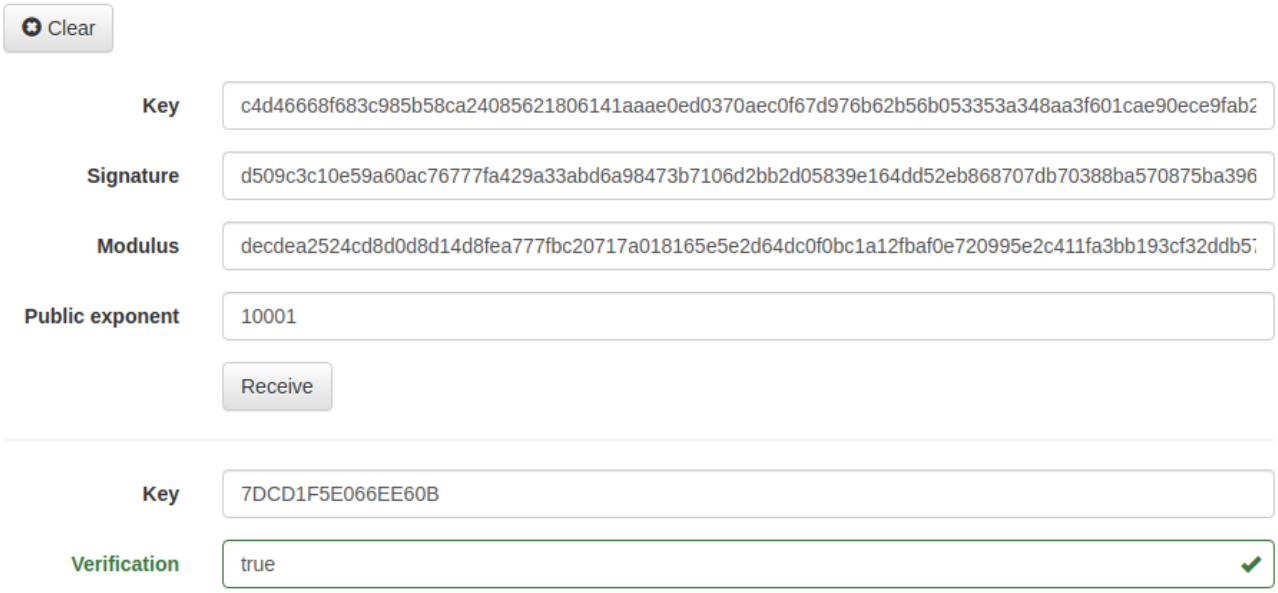
modulus:
b2ea890ddcda93d88f158e03a8bd1ca8ddcafa792644aa03b7c9662dd76ad1800dc9ae80f8f9b19fcdafe692e90cc371a82f7ce7a01b84d0f323bff61a01bd71

отправленный ключ: ff3923077ba7f876

зашифрованный ключ:
313f8a2cc3af37dd1ea631753360529e6f91a0c209fef0bde2be7ad0982a52dbb108793771be435f36cd755f49d498c4efdb5b4d2d9699d1874a6dcd37ed2d48

сигнатура:
4e5ff6f7335d10dddd683c509e44ce5ab7d3f2d2a1de19fd5adddf4948e8b8863408dff59415aaf5dece288ba24b54be3ad5461bc4f4ec50b25eee554f567fdd

полученный ключ: ff3923077ba7f876



Висновки:

В даному лабораторному практикумі ми ознайомились з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA. Також практично ознайомились з системою захисту інформації на основі криптосхеми RSA, організували з використанням цієї системи засекречений зв'язок і електронний підпис. А також вивчили протокол розсилання ключів.