МІНІСТЕРСТВО ОСВІТИ І НАУКИ,
МОЛОДІ ТА СПОРТУ
УКРАЇНИНАЦІОНАЛЬНИЙ
ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ
ПОЛІТЕХНІЧНИЙ
ІНСТИТУТ»ФІЗИКО-
ТЕХНІЧНИЙ
ІНСТИТУТ

Криптографія
Комп’ютерний практикум №4

Виконал
и: студенти
групи ФБ-95
Товстенко Артем, Тараканов Егор
Перевірив(ли):

Мета та основні завдання 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 і рекомендації щодо 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 $pq \leq p1q1$; p і q – прості числа для побудови ключів абонента А, p_1 і q_1 – 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) (e_1 n_1) та секретні d та d_1

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 0 < k < n.

Хід роботи:

1. Функція key_generator(), яка генерує випадкові прості числа заданої довжини в бітах, і перевіряється на простоту за допомогою Міллера-Рабіна:

```
Generating key pair for Alice:
228368047737274591160709940237707846422952607811842808801896035021042013335237 Is not a prime number.
228368047737274591160709940237707846422952607811842808801896035021042013335239 Is not a prime number.
228368047737274591160709940237707846422952607811842808801896035021042013335241 Is not a prime number.
228368047737274591160709940237707846422952607811842808801896035021042013335243 Is not a prime number.
```

```
Prime number - last+2
The p is
228368047737274591160709940237707846422952607811842808801896035021042013336351
The q is
144472034388737670135230599188204510269583469029630542664704372843541297301639
```

   І такий самий хід дій для нашого іншого абонента B(Bob)
2. Були сгенеровані p,q для локального кейсу, для отримання чисел e,d,n.
   Для абонента А

```
Public exponent (e) is 0x190dc9f876f451c08bf9c61c9f2b4407a5ff24060fafd182cfc35a277368ebe5294cf187ebf7ee6b45a2f07fb05c367bde14e67dba6da192c0ab41ebd95b58717
Private key (d) is 0x19cb47be03372d902e41b8ce3c95044f509061e89aa8d49fb76be35212f99ca2734cfb067bd7cdeabcea44f7da6bf5be829e3088775a819e4d353dda0a93a1157:
Modulus is (n) is 0x275f16e045f752877a417c9063d53b8dd52e48b99745f68797f2a123bf4b76c924b2697ccbcdc03d613c64b870b38bc0008b04a9f5c69c306a40529c294d4ad59
```

   Для абонента Б

```
Public exponent (e) is 0x3b3e3ecb13e45372b499f7f8471189387a75ff0169eb5aa587ead909962a2e815901b87a8f241a632f6a9e41f43227122013b2d5c44582d39e34ae102f98df2d9
Private key (d) is 0x2432243e3e0e83dedae8833e9d3c5e327eb976d5aa205fd3692959e27acfd845a35eec002a13d24c8d3486436a5dddf59a4f000441b820578c674ffd86b55955d:
Modulus is (n) is 0x53ab90d703c21629d184d05ddf487f16afcde5edcf19557a782a9bd55c4721286efff59cbeac23ae597aac5798fecf9cc9d0c5ee4b6590a9ef148a3c1d931c685
```

3. Функції виконання протоколів Send та Receive

```
Shared key is:  130
Signature is:  3122113700240868626959857710559674181216841061975188087539026344914313793137147665500630141817236904571608209700344771367021145481360645199200581894971620З
Encrypted signature:  1054053406393185623427857954682930942816980419113415387895070194956652236218293169661197544436364165289107737972304464341775110486920007461438599824879258З
Encrypted message:  5592833414355145267310772552931592191560334713287582901287151437375852744782129622760475344784146906937243471397326102721242409916977081948443720555840443б
Starting to receive a key
The key is:  130
Signature is:  3122113700240868626959857710559674181216841061975188087539026344914313793137147665500630141817236904571608209700344771367021145481360645199200581894971620З
The key was successfully received
```

4. Також було виконано шифрування та розшифрування деякого секретного повідомлення яке рандомно генерувалося:

```
Secret message is now  59048
Encrypted message L is:
 104135780969362170534559408240975716169210750822011805571584801215044927432901671091763479673439992771958009517099343539956282114118346855468140018847204ll
Decrypted back message is  59048
```

Висновок:
Під час виконання ми ознайомилися з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA та вивчили протокол розсилання ключів.