

Міністерство освіти і науки України
Національний технічний університет України
“Київський політехнічний інститут ім. Ігоря Сікорського”
Фізико-технічний інститут

Варіант 7

КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №4
Вивчення криптосистеми RSA та алгоритму електронного
підпису; ознайомлення з методами генерації параметрів для
асиметричних криптосистем

Виконали:
Студенти групи ФБ-05
Акбаров Елшодбек, Олифіренко Іван

Київ - 2023

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.

Постановка задачі

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 $1 < p, q$ довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб $p \nmid q-1$; p, 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 і 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 M 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 $0 < k < n$.

Кожна з наведених операцій повинна бути реалізована у вигляді окремої процедури, інтерфейс якої повинен приймати лише ті дані, які необхідні для її роботи; наприклад, функція Encrypt(), яка шифрує повідомлення для абонента, повинна приймати на вхід повідомлення та відкритий ключ адресата (і тільки його), повертаючи в якості результату шифротекст. Відповідно, програмний код повинен містити сім високорівневих процедур: GenerateKeyPair(), Encrypt(), Decrypt(), Sign(), Verify(), SendKey(), ReceiveKey().

Хід роботи

1. Із тестом Міллера-Рабіна проблем багато не виникло. Для перевірки чи правильно ми зробили тест, використовували: <https://planetcalc.ru/8995/>

2. Згенерував числа, так, щоб $pq \leq p_1q_1$:

$p =$

114893576615012767532631617462266153531956267357783648861491082899
568397195091

$q =$

589001838998181362548031712191794576790204790816979344238632646077
46985268011

$p_1 =$

112988788668750763609699926596140978736789755768783595000344553991
545243073851

$q_1 =$

113329302157219497734891659533221069041902924052190802623646108652
814389334531.

Перша пара
A:p:91673999493245147144527758886851563715665886803784705405923271546739415805469,q:7875470846975499936101996022955568246775
2658231835255868083786720952938725533)
Друга пара
B:p:97530542442237189071776344059835959668229346507265132777457884278429508218817,q:8252177648518530507625200407482755579720
3595749328790307544817182787677070887)e =
2000893336284337951511299111097668374720506197752886790579877313407809927255753169500382343914864948342553707487490004437253
936215191814304482227100199769n =
7219759104346989109155835703796560981667686199076736778146469037848994101299081303092529314509262432505708263256683690488757
928904084146111000585511339977d =
2577262023026309082718325510031535257785945474682518178648469908008158847893158603045879747790408540038898338549343833017152
714073072527044149518907739817e1 =
3466693578345943058834616640310906884181320999105470619442113237214693951443645270962387727889411821605162856994640868978106
398323814795450701051311857235n1 =
8048393623897176244539970168462798061520987583700211480546782049945926212223545860586103665919703416111690765690383215981566
093770678279903999667216280679d1 =
2608077172623790086537582378855022200972003387273642196264771264813524808748904856917309805623961603783756070864208728617982
103221870391440329196789722331-----Ключі А-----Відкриті ключі для А:e =
2000893336284337951511299111097668374720506197752886790579877313407809927255753169500382343914864948342553707487490004437253
936215191814304482227100199769n =
7219759104346989109155835703796560981667686199076736778146469037848994101299081303092529314509262432505708263256683690488757
928904084146111000585511339977Секретний ключ для А:d =
2577262023026309082718325510031535257785945474682518178648469908008158847893158603045879747790408540038898338549343833017152
714073072527044149518907739817p = 91673999493245147144527758886851563715665886803784705405923271546739415805469q =
78754708469754999361019960229555682467752658231835255868083786720952938725533-----Ключі В-----Відкриті ключі для
В:e1 =
3466693578345943058834616640310906884181320999105470619442113237214693951443645270962387727889411821605162856994640868978106
398323814795450701051311857235n1 =
8048393623897176244539970168462798061520987583700211480546782049945926212223545860586103665919703416111690765690383215981566
093770678279903999667216280679Секретний ключ для В:d1 =
2608077172623790086537582378855022200972003387273642196264771264813524808748904856917309805623961603783756070864208728617982
103221870391440329196789722331p1 = 97530542442237189071776344059835959668229346507265132777457884278429508218817q1 =
82521776485185305076252004074827555797203595749328790307544817182787677070887Початковий k =
6123965333015554110879632793724025205558908145065395937016430097635403928048615365726003043340614000030941259164325610444793
981730767671066835254376702626Повідомлення:
1012473901288034478109443929216543239499669752257417870995247002667942466574870526141908023050172780364322443825483189056703
453210516314628600112834074513<class 'int'>Розшифрований k =
6123965333015554110879632793724025205558908145065395937016430097635403928048615365726003043340614000030941259164325610444793
981730767671066835254376702626Ключ отримано
шифрування:
2255452881890545957501750803173214212173212679712402883756227977953939291060632754475284974580121685313981096183137841108590
079041203455014007709995989432Розшифрування:10124739012880344781094439292165432394996697522574178709952470026679424665748705
26141908023050172780364322443825483189056703453210516314628600112834074513Ф-ція Ейлера:
7219759104346989109155835703796560981667686199076736778146469037848994101298910874384566314362756884786591856010500271943722
308942810139052732893156808976перевірка тексту: True

Все виводиться в окремому текстовому файлі.

Зробимо перевірку на сайті:

Get server key

Key size

128

Modulus

8F0F517575814483D0506EC68AF123BF

Public exponent

10001

Створили ключі для Абонента.

Encryption

 Clear

Modulus

8F0F517575814483D0506EC68AF123BF

Public exponent

10001

Message

256


Bytes ▼

Encrypt

Ciphertext

2131E69148CAF5FF86F78DBBCD46FAF0

Decryption

 Clear

Ciphertext

2131E69148CAF5FF86F78DBBCD46FAF0

Bytes ▼

Decrypt

Message

0256

Sign

✖ Clear

Message

256

Bytes ▼

Sign

Signature

266135BEB10C427D9DFABB01C3B47874

Verify

✖ Clear

Message

256

Bytes ▼

Signature

266135BEB10C427D9DFABB01C3B47874

Modulus

8F0F517575814483D0506EC68AF123BF

Public exponent

10001


Verify

Verification

true

✓

Send key

 Clear

Modulus

8F0F517575814483D0506EC68AF123BF

**Public
exponent**

10001

Send

Key

641670B536706351F2A27A46D1B48C37

Signature

347690226CAE7EB0

Receive key

Key

641670B536706351F2A27A46D1B48C37

Signature

347690226CAE7EB0

Modulus

8F0F517575814483D0506EC68AF123BF

Public exponent

10001

Key

347690226CAE7EB0

Verification

true

✓

Висновки

У ході даної лабораторної роботи ми ознайомились з тестами перевірки чисел на простоту, а найбільш із тестом Міллера-Рабіна, і методами генерації ключів для асиметричної криптосистеми типу RSA; практично ознайомились з системою захисту інформації на основі криптосхеми RSA, організували з використанням цієї системи засекречений зв'язок й електронний підпис, вивчили протокол розсилання ключів.