

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

КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №4

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

Виконали студенти групи ФБ-32:
Красноок Юлія та Водяник Дмитро

Київ - 2025

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 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.

Результат виконання:

-> Генеруємо пару для Абонента А...

[x] Число

680331305472461907934113790935701230934657688606903237158352117636638303641
43 відсіяно тестом Міллера-Рабіна (складене).

[x] Число

923537912950827234785854389609777040927434421186425796583591307481057908673
93 відсіяно тестом Міллера-Рабіна (складене).

[x] Число

834838479041421052664815587530382448107613470252860863338617309025813908107
99 відсіяно тестом Міллера-Рабіна (складене).

[x] Число

831079060285074308227047324572918088187033609499761889664670615905982620331
49 відсіяно тестом Міллера-Рабіна (складене).

[x] Число

837615873530518486650592441693515332976128574911347979345333657022875108261
63 відсіяно тестом Міллера-Рабіна (складене).

[x] Число

102606902966901272047925539591001491523410856603815039430864988103857733477
643 відсіяно тестом Міллера-Рабіна (складене).

[x] Число

832132324347690245360532968918186798514941016674331164400677852221528712065
69 відсіяно тестом Міллера-Рабіна (складене).

[x] Число

891651266352918782785712561172662311380301367637544962088548456668959441731
23 відсіяно тестом Міллера-Рабіна (складене).

[x] Число

957351982818061650748283747084507246934733149719393399797976524350654737670
07 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
103615602902611376983437524812244638583665598838012871872527928535493307764
077 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
725701770131896892889282301406128341321692526083081631430492215701086462224
89 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
764434959422286338019332962452795261488384555533932599671615503967091908878
07 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
591339842346698758714161069086218537436656027786406600227755641978575778953
61 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
107804456152683946588076616804618013575307096804072797469086950744035787011
093 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
674474525936021998371430823841267317587395868131935911740101493898139519166
53 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
916610772241808051012786063371997315553511471118841615230057545087462112412
43 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
995564156322926113167922000409916711506172730886640696673072836135976390023
07 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
115122386294431907099945929996575225395442486650527418685857890773292497515
147 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
699437151378002126637825634097166383456244704641719346403745673452501531634
99 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
748069494789139892609508430093117908315408683422300628673254073855973241246
39 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
103919353306011688505527446230761224139878488271784204433784502617965888765
351 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
676915269488293088871775900091852822623663237298644718656846842295223107158
11 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
105394284117634297442870652768551874144013115838431962774426913519332375239
797 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
852984354182708844931945128727721626495071422879820029406635979153993304025
57 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
113121182863837500151564368742244468231083495741960614964863873654883700636
183 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
108334967391933611448332224250340244144590440323295533372106152482960634220
441 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
979456271653154467390964739612966112302904047586642817516431527708936529027
21 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
102859323082080599296514614056422610000616845029314849441305444708637677642
541 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
977606693347140705828397376510686491868333629745411237228530058241859688937
29 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
955822371758158537827122902024293030487555113730787877078281997137101201723
67 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
893222858793145369139382312578391225018538288548810320364878615353931918313
83 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
753746939207357685963651685257487897429501601308049382166494594915387344676
41 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
713220876080224630505375206121229234076237670545786608145101635284135263647
11 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
672243300252546699487261540325349818707968296725767336260843425047433763180
47 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
710207220489927683450901857291009324929247431299871481881408860033613796367
71 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
105295290912296807797596163058063044657281271467423787833321289533654163426
819 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
763775298907135747453369576699188356393362873411509518623212527371098670735
49 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
653107127324356644652027753405345762252985862533089268669742257827647010666
73 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
111069340220300031783787779597499081110259820711110080376775467719632970984
463 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
104999540688312335254708089958361569618302310157300715328732321804164183774
557 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
863895834431643328478899789376091267886096652710404339680947614141757618402
67 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
754034729390311327663396248414266597586125957789304312169471178379546541407
11 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
657211197384940676346945203063657283053485476831147991424832353359290618483
67 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
114769400180287159196571455243089808035092448407651631128351746004143452100
837 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
105096471161383613853637263684628384104886224702007729874932913061440163555
541 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
976174871859145833785435511338182543425264019884160517802276601493528035263
23 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
916699895354395241596316357715299298950000603339300822730932510133434762728
39 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
830934290738365088222348635796421214191897545210661553805503714769758340178
59 відсіяно тестом Міллера-Рабіна (складене).

[+] Знайдено прості числа для A:

p =
705405498215540839980345901904852097366801585095415707671474652316819050500
27

q =
746511165727707271878704214493250289387926368029049389421388937100266985983
07

-> Генеруємо пару для Абонента В...

[x] Число
100925140078754077537502252151166969084865282251491536597475441753897063388
159 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
945372308065168852861064920863924301904220716734790087269638123678449913053
93 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
945194140161783462774130566877589617410099980206232121760477101284366791943
87 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
113766429285516950544660088393402484957276969633167639291104622837606107122
149 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
115751878594517031897982033420282724053801338590018494615511431262928458997
767 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
913822003191240154888776723729393165042729541541123013013053275406337906221
49 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
930762484895756262691200460056059163541828765923334344432120031070294925300
89 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
104624453185736475082258772032669094226061779040065880389754019634165105410
341 відсіяно тестом Міллера-Рабіна (складене).

[x] Число
930333834086055220228461514219000194518877071051276145868217902384278325197
91 відсіяно тестом Міллера-Рабіна (складене).

Поточні p, q для B :

$p =$
104606244193095510716990556845544368464934230393691396499653042454743199033
263

$q =$
704968318696644109826967602699185404548056275186361365664830853479225013943
09

[OK] Умова модулів виконана ($n_B \geq n_A$).

2. За допомогою цієї функції згенерувати дві пари простих чисел p, q і $1 \leq p, q$ довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб $pq \leq p_1q_1$; p і q – прості числа для побудови ключів абонента A , $1 \leq p \leq q_1$ – абонента B .

Результат виконання:

Користувач А:

modulus (n) =

526593080783617524233475974993818750779677622750356257245768925196133928342
024200166502839235280746936699977048504705511792408379015390950310118561250
4289

public exp (e) = 65537

private exp (d) =

244490505547765598476833040375847489948029825976896107473248040890916019524
706205249917508288686483910165086699691158440136757708118114947328203253773
3937

primes (p, q) =

705405498215540839980345901904852097366801585095415707671474652316819050500
27,
746511165727707271878704214493250289387926368029049389421388937100266985983
07

Користувач В:

modulus (n) =

737440880939771332717492278843544154851722622466396580516038268735230062434
168724146809631162610861649310888690567385383835108839496649403598121836990
0267

public exp (e) = 65537

private exp (d) =

171754850033792660979291120195734592362431818809635433495533944702603898149
059067824917222535691438263793526746549971460087305256261420362711807723800
0385

primes (p, q) =

104606244193095510716990556845544368464934230393691396499653042454743199033
263,
704968318696644109826967602699185404548056275186361365664830853479225013943
09

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 .

Результат виконання:

Оригінальне повідомлення (число): 5268405863832725338979185567140

Зашифровані дані (для В):

375272047966891600592392724766930062820842162607723324683416166384377341712
191078382737841465335743144751688815128572343673813001842654151225880406858
7347

Розшифровані дані (у В): 5268405863832725338979185567140

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.

Результат виконання:

Текст для підпису: 'LabWork_Done'

Цифровий підпис користувача А:

579363904628634433779972070138364186861051851904662706781144730764444008496
352534417818925816301825870477066580415532438783023674382838058021076103563
648

Перевірка підпису публічним ключем А: True

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 $0 < k < n$.

Результат виконання:

А генерує сесійний ключ $k = 5797294816988489444081011796449812490655085127$

А формує захищений пакет (SendKey)...

Відправлено кортеж (Encrypted_K, Encrypted_Sign)

В отримує та розбирає пакет (ReceiveKey)...

В відновив значення $k' = 5797294816988489444081011796449812490655085127$

Фінальний результат: Протокол виконано успішно. Автентифікація пройшла.

RSA Testing Environment

Server Key

Encryption

Decryption

Signature

Verification

Send Key

Receive Key

Get server key

Clear

Key size512Get key

ModulusC2FD822B2C53EF66ECFDB054CC661294F2F5A7BDF85756F6F16A0E3AD3164577944D633001EC03FB9B4AI

Public exponent10001

RSA Testing Environment

Server Key

Encryption

Decryption

Signature

Verification

Send Key

Receive Key

Encryption

Clear

ModulusC2FD822B2C53EF66ECFDB054CC661294F2F5A7BDF85756F6F16A0E3AD3164577944D633001EC03FB9B4AI

Public exponent10001

MessageTestText

Encrypt

CiphertextAC1307BD18730C02F466C9C0CF1B05174ED823C380B9D2458FEC970314E962F87F33E196191F9BA49345F2

RSA Testing Environment

Server Key

Encryption

Decryption

Signature

Verification

Send Key

Receive Key

Decryption

Clear

CiphertextAC1307BD18730C02F466C9C0CF1B05174ED823C380B9D2458FEC970314E962Text

Decrypt

MessageTest

```
PS C:\Users\PC> & C:/Users/PC/AppData/Local/Programs/Python/Python311/python.exe f:/crypto/lab4/lab4_test.py
Генерація локальних ключів...
Ключі згенеровано. Modulus: 5BEDC7B9B3...B3C22CC685 (Len: 128)
Отримання ключа сервера...
Ключ сервера отримано. Modulus: 8349398DF7...BF4F178371 (Len: 128)

--- Тест 1: Шифрування (Confidentiality) ---
Отримано шифротекст: DB5D9223A1...8DB91F6FC0 (Len: 127)
Дешифрування успішне: SecretMessage

--- Тест 2: Цифровий підпис (Integrity) ---
Локальний підпис: 57267E2437...FFBA39105E (Len: 128)
Сервер підтвердив валідність підпису.

--- Тест 3: Спроба злому (Tampering) ---
Відправляємо ПОШКОДЖЕНИЙ підпис...
УСПІХ: Сервер відхилив підроблений підпис (як і очікувалось).

--- Тест 4: Протокол обміну ключами (SendKey) ---
Згенеровано сесійний ключ k: 80946
Відповідь сервера (Raw): {'key': '013C32', 'verified': True}
УСПІХ: Сервер повернув ключ 80946 (співпадає з 80946)

Всі тести пройдено успішно.
```

Висновки: У ході виконання лабораторної роботи було реалізовано бібліотеку для роботи з криптосистемою RSA "з нуля". Вивчено алгоритм генерації великих простих чисел за допомогою тесту Міллера-Рабіна. Реалізовано та протестовано протокол безпечного обміну ключами, який забезпечує конфіденційність (через шифрування на ключі отримувача) та автентичність (через цифровий підпис відправника). Коректність реалізації підтверджена тестами та зовнішнім верифікатором.