

КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №5
Вивчення криптосистеми RSA та алгоритму електронного підпису;
ознайомлення з методами генерації параметрів для асиметричних
криптосистем

Мета

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 $1 < p, q$ 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 А, $1 < p < q_1$ – 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) , $(,)$ і n_1 e 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 і 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. Написали алгоритм генерації простих чисел на основі тесту Міллера-Рабіна
2. Протестували математичні функцію кількома assert
3. Написали функції генерації пари ключів, шифрування розшифрування, верифікації, відправки та отримання ключів
4. Протестували наші функції за допомогою серверу, який виступав нашим другим абонентом

Результати роботи програми

Кандидати на прості числа:

[596057965026547441777569778727124579853450616395279398806303799688
677002060981210152088104020961022715476909336371153687548221487468
292928004793805553512,
943896007646170278286180545827809569532801069054815680681356509557
470520555057400759099235073311648621393194208602829974275512697340
6791516486819430045825,
452235585127927435715715766463604792868879708689207828372713222390
562440727245097689791159546176992140560459192675052659305654739618
1217573079169653417564]

[389917932519707926996736552709007784800735417237948379213442791297
178505319811421632691334182726234438612940147588094437520361061296
7308060054273152039709,
128635613623131283673657334644994060590393350223385733405953623941
459431154470340105909123455489039933026519254688421699156635651262
49197408715716238114108,
116595358308046116655073584362682959281296468284303828737101054157

498700896814457016910508069966674224667220629464246098119461421431
40513891602593099874409]

[252868954050395392928010956538564312463611468049133432203937062546
594802686182853859623984285146074001688039854793464882171698646456
9301082776520741600255,
677149023407080847215515510905897308949871111049486016859609797827
997951972403676037326227283709021146150236045027901264126631421158
9686031450175838565339,
622608007293282070306361620884098313955783390740385788835682805230
409357613301052881404567445738253500754074047341373989183998950249
670637297053997013374]

[128652024889618150581886207880065575951439125648355087899351479460
329481845840173934552770436328612522295736139412472650141424791153
29254243385398350001915,
827655401063030029670057678841712321497069019056846402514871644701
332551326400962796927632271597321344997273986565320073024408513548
5967790695493210281875,
980728079170060835359842681163854519335359873090078850625465805138
133794326132944016413086856091324108857389145283354192667280975916
2032731437049105125390]

Ключі абонента А:

n=3350683314753981198051005474011513307098414862693999848383671299
253182461817365637064274460976371397082504632794573088041060302425
050173461150354861196076771206404669682034739559337646277604938001
518721483955227099587218967897731533222015415777718493135122128888
6189224604989476129809966983014031796880714581, e=65537
d=7899058121816532570897055796493260386448953969303187154970127038
689849861159085568860802359290925444393960141092230985585910504366
544879987605929872511614529640858103980953520438668277590076514708
088082548043816467583577481437683066826324090075466661053653061546
077353263239507210148372622727320158361303673,
p=5248803078923088809023689887705797657713341447806767914983757644
187393138389182472780597004281514855295769418420744371198113581191
514364999862596168609343,

q=6383709322624178156438635592128601637974478013280825608316375054
868473477668211197418745803592182484711235031181328077614819892858
329862306701160678140267

Ключі абонента В:

n=7898309058895858903056324910789360631663829024390249674547453303
396387324065095808321156827983557974542683844204617377783183949263
573279939654589748434531335824318436524637189155303631387039186231
238757276956417387339468159988777960716502685412225581978887389567
7822701338873791535734370713067281390440396797, e=65537

d=4161203826625512553286369326025528234281225697760754089487991022
775996178118003998805451927256607561301399023035797012681352143066
857778197909481282847054861366067843278143104678418278216631346555
351554931218435689608237588631790622009408807410660979320613862311
3482286321478683770356586203803249276278383617,

p=6828872203385682822569692958483982958391579550960081477151184708
009706723776490358951893160762217383111913610569246576813926268763
452258499330944550997093,

q=1156605193897165122753915922672368858947189187424720868983206372
864743586509730279118124824355783962336198951082711675665125491427
5726435376177165668812729

Згенеровано повідомлення

M=661215467345584684081664834376474863690896076682333731726114414
847718256511906740630581303922467098403655030166829146725096454174
084306076204542067627454210536255449434700792922154551980755704428
969321708142369608014775357086933102167327337900614042729627366250
9948683975992321798081743127645403331750137082

А зашифрував повідомлення відкритим ключем В, і отримав

C=5873111231278655247825263870150227783243871208491356422024999345
895193946861918712378499575996713268320912252111895908420647883770
790540346344199787535070482319184628372061147094875117317866050239
679297109177196665223550135381453299323300512715119316006315599905
5459576100683120566338129297818988986083059403

В розшифрував повідомлення своїм закритим ключем і отримав

M=661215467345584684081664834376474863690896076682333731726114414
847718256511906740630581303922467098403655030166829146725096454174

084306076204542067627454210536255449434700792922154551980755704428
969321708142369608014775357086933102167327337900614042729627366250
9948683975992321798081743127645403331750137082

В зашифрував повідомлення відкритим ключем А, і отримав

C=1622876188733843106463067632820663309238618884734464007194270615
406503423231560223320211559553435682307061664736376117310875715847
585756621551491312995508449132286317956460161725625814856704701112
779418533158179535465808002059269555463493511388901716753830726546
7546616311310731778809615056266444438349268313

А розшифрував повідомлення своїм закритим ключем і отримав

M=661215467345584684081664834376474863690896076682333731726114414
847718256511906740630581303922467098403655030166829146725096454174
084306076204542067627454210536255449434700792922154551980755704428
969321708142369608014775357086933102167327337900614042729627366250
9948683975992321798081743127645403331750137082

А підписав повідомлення, і отримав

S=2643627987037763615950443243930402557067382388485950981406687115
357119109975777533846209293760874189779607625961770584302802019378
556600135793703370352659568261877320913222224299366362714230670315
784900556850444073268259029730678541679933954228932552887340022868
2462725312872865651379222503962257495337861671

В перевірів підпис з результатом True

В підписав повідомлення, і отримав

S=7659974962618386077695229732341673230417117034788544132333177459
475915039861616362089277234051013459190436608769666146520584516178
021991760072196853362653016080129509715863420246842762642565830817
006297113258920114084869498359511028749074233918477333908427059771
0971456470634347202505072035901099810758223958

А перевірів підпис з результатом True

А згенерував певний ключ

k=3161127800939177206414971318462262400027248223854061565986795525
030396559349037835167307044779843962675295102438504652627107868364

918165813326155720992286679377453658753109857754993510252196487052
067302795543306647545943488105556491760901844520808940042293143384
9373410714550808884845268995351223455913715984

send_key...

$s = k^{**}d \bmod n =$

250655054411293320306389518495063846176855562980280769047172580656
630940768907081365018404733971550035261835222916209176768500921499
056636417880708149276212280854260703433050943327512126420269981203
552776858222959885972435944716744433283719606517882403485473288567
0140835016282351872731178733114438764161301

$s1 = s^{**}e1 \bmod n1 =$

404974476059211860204888710403669849459184601790748771815383426943
258265337530001912371368111646377252712470552787147845249230010133
257317200189627995633257986007159981494566270002612661930887642493
414063127795943820187109050836318710034752067451186534492538066930
91072878001226101712131518907012046372291077

$k1 = k^{**}e1 \bmod n1 =$

320272208047726409855608196683866157254862002550779880212116968617
450851112738900707782918920940591887808231416185544903054825120666
988994157250434921972231756056761015159258553116041344156784920011
657305924331866982153793093151956670611147864913076209128075202778
72487311190912983115759314742729880205372613

A зформував повідомлення (k1, S1) =

(320272208047726409855608196683866157254862002550779880212116968617
450851112738900707782918920940591887808231416185544903054825120666
988994157250434921972231756056761015159258553116041344156784920011
657305924331866982153793093151956670611147864913076209128075202778
72487311190912983115759314742729880205372613,
404974476059211860204888710403669849459184601790748771815383426943
258265337530001912371368111646377252712470552787147845249230010133
257317200189627995633257986007159981494566270002612661930887642493
414063127795943820187109050836318710034752067451186534492538066930
91072878001226101712131518907012046372291077)

receive_key...

$k = k1 ** d1 \bmod n1 =$

316112780093917720641497131846226240002724822385406156598679552503
039655934903783516730704477984396267529510243850465262710786836491
816581332615572099228667937745365875310985775499351025219648705206
730279554330664754594348810555649176090184452080894004229314338493
73410714550808884845268995351223455913715984

$s = s1 ** d1 \bmod n1 =$

250655054411293320306389518495063846176855562980280769047172580656
630940768907081365018404733971550035261835222916209176768500921499
056636417880708149276212280854260703433050943327512126420269981203
552776858222959885972435944716744433283719606517882403485473288567
0140835016282351872731178733114438764161301

Checking: $k = s ** e \bmod n$

В отримав повідомлення, після чого знайшов і перевірів ключ

k=3161127800939177206414971318462262400027248223854061565986795525
030396559349037835167307044779843962675295102438504652627107868364
918165813326155720992286679377453658753109857754993510252196487052
067302795543306647545943488105556491760901844520808940042293143384
9373410714550808884845268995351223455913715984

Перевірка коректності операцій шифрування з сервером:


```
pr, pub = generate_key_pair(p, q, 13)
pr, pub
(d=97, p=19, q=11, n=209, e=13)
```

Encryption

Modulus	<input type="text" value="d1"/>
Public exponent	<input type="text" value="d"/>
Message	<input type="text" value="15"/>
	<input type="button" value="Encrypt"/>
Ciphertext	<input type="text" value="62"/>

```
hex(decrypt(98, pr))
'0x15'
```


Get server key

 Clear

Key size

128

Get key

Modulus


9D5ACD006BE870182AAEF3515F8F5D5B

Public exponent

10001

```
int("9D5ACD006BE870182AAEF3515F8F5D5B", 16)
209160259982864571316780480937895877979
int("10001", 16)
65537
pub = PublicKey(209160259982864571316780480937895877979, 65537)
hex(encrypt(55, pub))
'0x513156e1cc6269548de078674d2a6d7f'
```

Decryption

 Clear

Ciphertext

513156e1cc6269548de078674d2a6d7f

Decrypt

Message

37

```
int("37", 16)
55
```

Sign

✖ Clear

Message

123

Sign

Signature

81A6572D0B619F0E86C2A6AEBBD7904F

```
verify((int("123", 16), int("81A6572D0B619F0E86C2A6AEBBD7904F", 16)), pub)  
True
```

```
sign(150, pr)  
(150, 138)  
hex(150), hex(138)  
(0x96, 0x8a)
```

Verify

✖ Clear

Message

96

Signature

8a

Modulus

d1

Public exponent

d

Verify

Verification

true

```

send_key(5050, pr, pub)
(64175798577819004000730523428347984471, 70606774045179535361525975323676258772)
hex(64175798577819004000730523428347984471)
'0x3047cf28f3380bc84c6753d1fc483a57'
hex(70606774045179535361525975323676258772)
'0x351e5ebb021cd2e3f0d296c64fbc31d4'

```

Receive key

Key	3047cf28f3380bc84c6753d1fc483a57
Signature	351e5ebb021cd2e3f0d296c64fbc31d4
Modulus	d1
Public exponent	d
<input type="button" value="Receive"/>	
Key	13BA
Verification	false

```

int("13BA", 16)
5050

```

Send key

Modulus	36340751c299bbd134d3091dd3355fed408f51631b1e61ea0dc007c750d8e664eed62834cf3925a633a6fd8a3ebb4
Public exponent	10001
<input type="button" value="Send"/>	
Key	10221F8AD29E0CBF619919267B7D710CF00D33352183485CF8316E7705E07A0648E8683EF51118F5B2D7F3F
Signature	2D59B54DA8C95CEE0EC31F04039C1F83CA8B9C12365CB385E357C5D5AD15BEDB91636796B4000CB0E0

```

send_key((int("10221F8AD29E0CBF619919267B7D710CF00D33352183485CF8316E7705E07A0648E8683EF51118F5B2D7F3F", 16), int("2D59B54DA8C95CEE0EC31F04039C1F83CA8B9C12365CB385E357C5D5AD15BEDB91636796B4000CB0E0", 16)), pr, th_pub)
6166671626116485822

```

Висновок: ми ознайомилися з тестами перевірки чисел на простоту та використали тест Міллера-Рабіна. Навчилися генерувати ключі для асиметричної криптосистеми RSA, та користуватися ними на практиці