

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

Виконав: ФБ-11 Тимощук Ілья

Київ – 2023

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 використовувати вбудований генератор псевдовипадкових чисел мови програмування Python. В якості тесту перевірки на простоту використати тест Міллера-Рабіна із попередніми пробними діленнями. Тести необхідно реалізовувати власноруч.
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 $pq \leq p_1q_1$; 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, n) та секретні d і d .
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 $0 < k$

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

Значення кандидатів, що не пройшли тест перевірки простоти записані в `invalid_prime_numbers.txt`

Вивід значень згенерованих ключів для А та В, а також перевірка функцій encrypt_message(), decrypt_message(), sign_message(), verify_signature(), send_key() та recive_key() для випадково згенерованих М та k. Логи цих та інших значень, виведених в консоль записані в console_log.txt

```
n_A: 60377976905568912727850968590527967597895389029546747435361543365583430272204016346452157863240871620588080887573105978745789348024126484797816735967729
e_A: 86328388835147498696938016780144260757921157135934742558442918606811265828390154129023380219572739015573806245547077874670341969990177825396588477922901
d_A: 2584683499142646184650022786393286605826699000360490000729774804081525608830000316942507365024454193245223540476982481761422743783167978944165376830203061
p_A: 58000748396816552215973275146692474618404746186423750942920547422809706458691
q_A: 104098616956602953743080566929964398533983051992355428827954096162859437618619
=====
n_B: 607246989644114237941889765409734495110933147059006499361291456351168493457358665735739857908505020536409916960258692104344853413564038352151600855478593
e_B: 4597536068355349844123604535961420099576759720109752252604079836774983239363810871513093302307978316878150786480602818743766014868175204766969448721064903
d_B: 477310437345787741611531345402021114150733855869133712111071136611937816363839988918771918540279217584942760704189650761545177003944755239620749306279047
p_B: 9763293526312551784981282324945033036507549307006722272171942866699081200953
q_B: 62196940817927271345756671546175315620382296894451068370283999111717230880181
Check for encrypt/decrypt:
M: 2419940918905776399336068504274048299082503995165698570030247955738634425175615363050584486809391576046702232178818078072704566548488249551630541908963752
C: 3630527293012899610982751861455433930761883616977530555123415600436792772090518875121949729567621738906709207852218967227374834010133136072408456260161698
M_decrypted: 2419940918905776399336068504274048299082503995165698570030247955738634425175615363050584486809391576046702232178818078072704566548488249551630541908963752
Check for sign/verify sign:
Цифровий підпис: 4389811444344224472332604857398959943372490622149240551502881212683532093701827731124923535250367134316484119788686056958004871980961839837057429385742230
S: 4389811444344224472332604857398959943372490622149240551502881212683532093701827731124923535250367134316484119788686056958004871980961839837057429385742230
Перевірка цифрового підпису вірна.
Check for Send/Recive Key:
k: 4999204099866700081529667742015786974880425042733045865328068147203122105974286425429709002403787399512116103651818094891306009509530961712021474122054115
Цифровий підпис: 3531463271494143857346517418240089399542393305971811171895572515788884216062004428658838885174721005707526182376961580438858438856047532717876812568729274
Send_key function:
k_1: 5726396593741718934385001751121901210703006756955711462550402929877336597206539426246953833029911552083726564124357186053087498249866643246055186944555337
s: 3531463271494143857346517418240089399542393305971811171895572515788884216062004428658838885174721005707526182376961580438858438856047532717876812568729274
s_1: 44476089866996773216627428740482519953498284047969201640393925163168262758936137748410902210025093009663423867149174365890093434018574435325960103420113786
Recive_key function:
k_decrypted: 4999204099866700081529667742015786974880425042733045865328068147203122105974286425429709002403787399512116103651818094891306009509530961712021474122054115
s_decrypted: 3531463271494143857346517418240089399542393305971811171895572515788884216062004428658838885174721005707526182376961580438858438856047532717876812568729274
Перевірка цифрового підпису вірна.
```

Генерація публічного ключа сервера:

RSA Testing Environment

Server Key

Encryption

Decryption

Signature

Verification

Send Key

Receive Key

Get server key

Clear

Key size256

Get key

ModulusA299D50551C08C396DB6FD18EFC6D1F29F061B7A09E532572ADDD59748990BC5

Public exponent10001

Test #1 Decryption:

RSA Testing Environment

Server Key

Encryption

Decryption

Signature

Verification

Send Key

Receive Key

Decryption

✖ Clear

Ciphertext

a1472b011b944a1b76b8432f60540962c88f6e3e96fb691dc79ffe523e7f54ea

Bytes

Decrypt

Message

06B00535258A15CC647C03D9A0EFB399CB5F847044E93384367899313A3182E8

Test #1:

server_key_n : 73546479286781352620460425288022330068717863260284414915166947141938998479813

server_key_e : 65537

test1_3_message : 3024878116462861011705203732683992790895339644609381717512023354376027472616

server_key_n_hex : a299d50551c08c396db6fd18efc6d1f29f061b7a09e532572add59748990bc5

server_key_e_hex : 10001

test1_3_message_hex : 6B00535258A15CC647C03D9A0EFB399CB5F847044E93384367899313A3182E8

test1_3_message_hex (encrypted) : a1472b011b944a1b76b8432f60540962c88f6e3e96fb691dc79ffe523e7f54ea

TEST #1 COMPLETED!

Test #2 Encryption:

RSA Testing Environment

Server Key

Encryption

Decryption

Signature

Verification

Send Key

Receive Key

Encryption

✖ Clear

Modulus

c373302bf6c1e2ae5ffa080d5c425e3a084556d0bd0aab2ef3651f202956f72e6ba998a16336c0c6314b747f767a4a05

Public exponent

a339372f632594795b8727b11277d6baacc3cc38a2cb67aa5ee16beee1a19b06d79b149b840d26a7ff47b734b128224a321f14f1be5e68c44264f9a86a6e7c7

Message

4a8eac46a0e7d9e93033641785fa06b21b87aa431ad87ff7bd47bcc791760b5c9d7a:

Bytes

Encrypt

Ciphertext

6049D202C5EE86776141527EB255076A432A8C796D87F00C279EF97E4CB061F86EF228977A77D5FC0F723C

Test #2:

n_test2_4_5 : 10236544688920630908733659127201053523952666795702849569064738572394506857359238537273473274621675584210073177730092082623878982352980305106439936466201519

e_test2_4_5 : 8548708261584567102091536396918272265649306769833764159348143686627060716741896190909071080925202509241814596015681645067384665979655190870000929213966279

d_test2_4_5 : 318693226333418535651189478929294389333850536881554094920090930524706901059653540961380457755928320151895849962742541550842429532851011351833978899469479

n_test2_4_5_hex : c373302bf6c1e2ae5ffa080d5c425e3a084556d0bd0aab2ef3651f202956f72e6ba998a16336c0c6314b747f767a4a052dca20ab0653be48cf2bd144e659fabaf

e_test2_4_5_hex : a339372f632594795b8727b11277d6baacc3cc38a2cb67aa5ee16beee1a19b06d79b149b840d26a7ff47b734b128224a321f14f1be5e68c44264f9a86a6e7c7

test2_4_message : 3904883498710813137572740169872784211699685537669784500874517353088765008785075699732306647666267512308709597110656714572561368517837596841463469502402309

test2_4_message_hex : 4a8eac46a0e7d9e93033641785fa06b21b87aa431ad87ff7bd47bcc791760b5c9d7a9d42917c084b0554a698503a3976ce0314feee06ef7cdf85b85b2188f05

server_ciphertext : 5043030652236207148779660098229269277511583771056022097196145805912658988806428169599355724797035843619047211772934190364289734682358449728330700259339587

server_ciphertext_hex : 6049D202C5EE86776141527EB255076A432A8C796D87F00C279EF97E4CB061F86EF228977A77D5FC0F723C

Decrypted message from server: 3904883498710813137572740169872784211699685537669784500874517353088765008785075699732306647666267512308709597110656714572561368517837596841463469502402309

TEST #2 COMPLETED!

Test #3 Sign:

RSA Testing Environment

Server Key

Encryption

Decryption

Signature

Verification

Send Key

Receive Key

Sign

✖ Clear

Message

6b00535258a15cc647c03d9a0efb399cb5f847044e93384367899313a3182e8

Bytes

Sign

Signature

3A4396CA9198896E607F0E843EEADE2D213B4DFE453C62061AE5549876AC980A

Test #3:
server_test3_signature: 26353564694363879933210571000124562666501839848422595326922552682544018266122
server_test3_signature_hex: 3a4396ca9198896e607f0e843eeade2d213b4dfe453c62061ae5549876ac980a
Перевірка цифрового підпису вірна.
TEST #3 COMPLETED!

Для тесту №3 було взято значення повідомлення test1_3_message з тесту №1.

Test #4 Verify:

RSA Testing Environment

Server Key

Encryption

Decryption

Signature

Verification

Send Key

Receive Key

Verify

✖ Clear

Message

4a8eac46a0e7d9e93033641785fa06b21b87aa431ad87ff7bd47bcc791760b5c9d7a4

Bytes

Signature

8e25dd10d244b8ad75de3e5f7b604cbad5bc35aa71af145497464a8f3ab3c8e29680e0cbffbc84162385cf60e8676de

Modulus

c373302bf6c1e2ae5ffa080d5c425e3a084556d0bd0aab2ef3651f202956f72e6ba998a16336c0c6314b74f767a4a05

Public exponent

a339372f632594795b8727b11277d6baacc3cc38a2cb67aa5ee16beee1a19b06d79b149b840d26a7ff47b734b128

Verify

Verification

true

Test #4:
Цифровий підпис: 7444889845478836479126049292748815047601190685519921797556857416016467616134281729635446005240466759639144175518749151327727335633133762712615071590658620
signed_test2_4_message: 7444889845478836479126049292748815047601190685519921797556857416016467616134281729635446005240466759639144175518749151327727335633133762712615071590658620
signed_test2_4_message_hex: 8e25dd10d244b8ad75de3e5f7b604cbad5bc35aa71af145497464a8f3ab3c8e29680e0cbffbc84162385cf60e8676de3c5baacff691a244ddad5e6672588323c
TEST #4 COMPLETED!

Для тесту №4 було взято значення повідомлення test2_4_message, d_test2_4_5 та n_test2_4_5 з тесту №2.

Test #5 Send key:

RSA Testing Environment

Server Key

Encryption

Decryption

Signature

Verification

Send Key

Receive Key

Send key

Clear

Modulus

c373302bf6c1e2ae5ffa080d5c425e3a084556d0bd0aab2ef3651f202956f72e6ba998a16336c0c6314b74f767a4a05

Public exponent

a339372f632594795b8727b11277d6baaacc3cc38a2cb67aa5ee16beee1a19b06d79b149b840d26a7ff47b734b128:

Send

Key

49B58C551918F4479BCF648D66B31425673AB32988F8D9D594C22F525891E8988012E1F9634D92DC213BCC

Signature

834BD35D70EBA9E6AC64C3B1F3011FE06A767C0119EEDE390E9C093B296AFD3D1C74CF2F0BFD744879F

```
Test #5:
test5_k1: 386046261039723583973289084636288613997497347977582172781946268289684752978539504152441654502410677128083828343368781685944639785624191480349911378013550
test5_s1: 6876539648694126191082491356207795968740119651957208136569113576358496435291150065042647636138745929354981828101804353819044660205675906484095228431574384
test5_k1_hex: 49b58c551918f4479bcf648d66b31425673ab32988f8d9d594c22f525891e8988012e1f9634d92dc213bcd2cff414279f44b834b624a500221ac6c1b5e2fad6e
test5_s1_hex: 834bd35d70eba9e6ac64c3b1f3011fe06a767c0119eede390e9c093b296afd3d1c74cf2f0bfd74487f9f6d8e344449450c24505bc3f20edbe0e5fa3514e82570
Recive_key function:
k_decrypted: 13011951155952883268
s_decrypted: 666242611379598002242732458022156872341072871420333303357180893336394892788
Перевірка цифрового підпису вірна.
TEST #5 COMPLETED!
```

Для тесту №5 було взято значення d_test2_4_5 та n_test2_4_5 з тесту №2.

Test #6 Recive key:

RSA Testing Environment

Server Key

Encryption

Decryption

Signature

Verification

Send Key

Receive Key

Receive key

Clear

Key

5d54fdaa3ad7d99c85694a5e8f6220626eb75ed48e0c8ba3ed08134483bf0354

Signature

923baa680470e54666e5f3f2ba8af44c959a996880ee61fa0737387c8922eb7b

Modulus

538c155f91f148f0edceab5dfa637ec2cf85e431d9d4e8a1168eeca29e63283

Public exponent

10779904d424ef30f54f6eb4882bbc4b647ce1675d4c8d03e3fceb0cc10d4451

Receive

Key

19114DB938498200683BF7A8DA3C79BE1DAF0477E2275389F10A55F69C38B6F3

Verification

true

```
Test #6:
server_key_n : 73546479286781352620460425288022330068717863260284414915166947141938998479813
n_test6 : 37789472534717841175671899531567148998404644961434738557158556010066982875779
e_test6 : 7448316475413135314314101930182047750256351473044609170788801387148232967249
d_test6 : 3870781795797834802343229346210114294609541564756553406129702208214699568849
n_test6_hex : 538c155f91f148f0edceab5dfa637ec2cf85e431d9d4e8a1168eeca29e63283
e_test6_hex : 10779904d424ef30f54f6eb4882bbc4b647ce1675d4c8d03e3fceb0cc10d4451
Цифровий підпис: 32433658878485871339833116174611632982560364973302311744962060917070884750912
Send_key function:
k_1: 42215260802898738305438171886668886390594010538610982042503382223610254918484
s: 32433658878485871339833116174611632982560364973302311744962060917070884750912
s_1: 66143095971159916882472681632954070643723094040336873871268021640520498604923
test6_k1_hex : 5d54fdaa3ad7d99c85694a5e8f6220626eb75ed48e0c8ba3ed08134483bf0354
test6_s1_hex : 923baa680470e54666e5f3f2ba8af44c959a996880ee61fa0737387c8922eb7b
TEST #6 COMPLETED!
```

Труднощі, які виникли під час виконання роботи

Під час перевірки функції Receive Key на сайті, ключ ніяк не підтверджувався, допоки я не згадав, що для перевірки треба згенерувати нові ключі, щоб **n_test6 < server_key_n**.

Висновок: в цій лабораторній роботі було вивчено тести перевірки чисел на простоту і методи генерації ключів для асиметричної криптосистеми типу RSA; практичне ознайомлено з системою захисту інформації на основі криптосхеми RSA, організовано з використанням цієї системи засекреченого зв'язку й електронного підпису, вивчено протокол розсилання ключів.