



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

# Криптографія

## Лабораторна №4

Виконали:  
Студенти групи ФБ-84  
Ярмоленко Владислав  
Горянський Євген  
Перевірів:  
Чорний. О.

Київ – 2020

## 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.

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  $d_1$ .

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().

Кожну операцію рекомендується перевіряти шляхом взаємодії із тестовим середовищем, розташованим за адресою <http://asymcryptwebservice.appspot.com/?section=rsa>

## Хід роботи

Для генерації використовували простий перебір чисел від  $n$  до  $n*2-1$ .  
Генерується послідовність біт заданого розміру після чого алгоритм перевіряє це число на простоту, якщо число складене, то додати 2 та перевірити знову, і так поки не знайдеться число просте.

Генерація простого числа 'p' ...

```
[*] Number 0x32b84d32f15c8f3befe61840efdab3aaa33437eb4d10a4498b0ad0d7a19f2747 is not prime
[*] Number 0x32b84d32f15c8f3befe61840efdab3aaa33437eb4d10a4498b0ad0d7a19f2749 is not prime
[*] Number 0x32b84d32f15c8f3befe61840efdab3aaa33437eb4d10a4498b0ad0d7a19f274b is not prime
[*] Number 0x32b84d32f15c8f3befe61840efdab3aaa33437eb4d10a4498b0ad0d7a19f274d is not prime
[*] Number 0x32b84d32f15c8f3befe61840efdab3aaa33437eb4d10a4498b0ad0d7a19f274f is not prime
[*] Number 0x32b84d32f15c8f3befe61840efdab3aaa33437eb4d10a4498b0ad0d7a19f2751 is not prime
[*] Number 0x32b84d32f15c8f3befe61840efdab3aaa33437eb4d10a4498b0ad0d7a19f2753 is not prime
[*] Number 0x32b84d32f15c8f3befe61840efdab3aaa33437eb4d10a4498b0ad0d7a19f2755 is not prime
[*] Prime number 0x32b84d32f15c8f3befe61840efdab3aaa33437eb4d10a4498b0ad0d7a19f2757
```

Просте число сгенеровано 'p'

Генерація простого числа 'q' ...

```
[*] Number 0x4a10008035598b8d37ee014105966ac21e4f81fccce642c56a8cfe39ccf2b603 is not prime
[*] Number 0x4a10008035598b8d37ee014105966ac21e4f81fccce642c56a8cfe39ccf2b605 is not prime
[*] Number 0x4a10008035598b8d37ee014105966ac21e4f81fccce642c56a8cfe39ccf2b607 is not prime
[*] Number 0x4a10008035598b8d37ee014105966ac21e4f81fccce642c56a8cfe39ccf2b609 is not prime
[*] Number 0x4a10008035598b8d37ee014105966ac21e4f81fccce642c56a8cfe39ccf2b60b is not prime
[*] Number 0x4a10008035598b8d37ee014105966ac21e4f81fccce642c56a8cfe39ccf2b60d is not prime
[*] Number 0x4a10008035598b8d37ee014105966ac21e4f81fccce642c56a8cfe39ccf2b60f is not prime
[*] Number 0x4a10008035598b8d37ee014105966ac21e4f81fccce642c56a8cfe39ccf2b611 is not prime
[*] Number 0x4a10008035598b8d37ee014105966ac21e4f81fccce642c56a8cfe39ccf2b613 is not prime
[*] Number 0x4a10008035598b8d37ee014105966ac21e4f81fccce642c56a8cfe39ccf2b615 is not prime
[*] Number 0x4a10008035598b8d37ee014105966ac21e4f81fccce642c56a8cfe39ccf2b617 is not prime
[*] Number 0x4a10008035598b8d37ee014105966ac21e4f81fccce642c56a8cfe39ccf2b619 is not prime
[*] Number 0x4a10008035598b8d37ee014105966ac21e4f81fccce642c56a8cfe39ccf2b61b is not prime
[*] Number 0x4a10008035598b8d37ee014105966ac21e4f81fccce642c56a8cfe39ccf2b61d is not prime
[*] Number 0x4a10008035598b8d37ee014105966ac21e4f81fccce642c56a8cfe39ccf2b61f is not prime
[*] Number 0x4a10008035598b8d37ee014105966ac21e4f81fccce642c56a8cfe39ccf2b621 is not prime
[*] Number 0x4a10008035598b8d37ee014105966ac21e4f81fccce642c56a8cfe39ccf2b623 is not prime
[*] Number 0x4a10008035598b8d37ee014105966ac21e4f81fccce642c56a8cfe39ccf2b625 is not prime
```

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]



[illegible]

[illegible]

[illegible]

[illegible]

Просте число сгенеровано 'q'

q=0x4a10008035598b8d37ee014105966ac21e4f81fccce642c56a8cfe39ccf2b967

n=0xeac71eef3ac565d648f207af41d49b51bd9a78225d0085b7ee9a858b37e23190fabebf81f5e54e57eaab7867e29f66f9cca9e5033fbbd5c71f38ab98eb4b301

f=0xeac71eef3ac565d648f207af41d49b51bd9a78225d0085b7ee9a858b37e231892e39e44f8a83a1c56d69e0488b8d802db46e4681a04d64d7c5bbba82022d244

e=0x10001

d=0x77aa5e7e193a9c1988bcb46603ebd5eee7f15fe243fd0c2b2016ea92773d777a3071998961548e940e9cb490c570ae309d92c7a5328bc026aac670ddeb360f1

Генерація простого числа 'p' ...

[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec1d9 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec1db is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec1dd is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec1df is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec1e1 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec1e3 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec1e5 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec1e7 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec1e9 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec1eb is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec1ed is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec1ef is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec1f1 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec1f3 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec1f5 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec1f7 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec1f9 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec1fb is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec1fd is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec1ff is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec201 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec203 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec205 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec207 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec209 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec20b is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec20d is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec20f is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec211 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec213 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec215 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec217 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec219 is not prime

[illegible]

[illegible]



[illegible]

[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec317 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec319 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec31b is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec31d is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec31f is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec321 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec323 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec325 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec327 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec329 is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec32b is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec32d is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec32f is not prime  
[\*] Number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec331 is not prime  
[\*] Prime number 0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec333

Просте число сгенеровано 'p'

Генерація простого числа 'q' ...

[\*] Number 0x232f1ba7717637fdb9afc11e74cc126f9061ea7a8b4dfdc09dbcd232b287d39 is not prime  
[\*] Number 0x232f1ba7717637fdb9afc11e74cc126f9061ea7a8b4dfdc09dbcd232b287d3b is not prime  
[\*] Number 0x232f1ba7717637fdb9afc11e74cc126f9061ea7a8b4dfdc09dbcd232b287d3d is not prime  
[\*] Number 0x232f1ba7717637fdb9afc11e74cc126f9061ea7a8b4dfdc09dbcd232b287d3f is not prime  
[\*] Number 0x232f1ba7717637fdb9afc11e74cc126f9061ea7a8b4dfdc09dbcd232b287d41 is not prime  
[\*] Number 0x232f1ba7717637fdb9afc11e74cc126f9061ea7a8b4dfdc09dbcd232b287d43 is not prime  
[\*] Number 0x232f1ba7717637fdb9afc11e74cc126f9061ea7a8b4dfdc09dbcd232b287d45 is not prime  
[\*] Number 0x232f1ba7717637fdb9afc11e74cc126f9061ea7a8b4dfdc09dbcd232b287d47 is not prime  
[\*] Number 0x232f1ba7717637fdb9afc11e74cc126f9061ea7a8b4dfdc09dbcd232b287d49 is not prime  
[\*] Number 0x232f1ba7717637fdb9afc11e74cc126f9061ea7a8b4dfdc09dbcd232b287d4b is not prime  
[\*] Number 0x232f1ba7717637fdb9afc11e74cc126f9061ea7a8b4dfdc09dbcd232b287d4d is not prime  
[\*] Number 0x232f1ba7717637fdb9afc11e74cc126f9061ea7a8b4dfdc09dbcd232b287d4f is not prime  
[\*] Number 0x232f1ba7717637fdb9afc11e74cc126f9061ea7a8b4dfdc09dbcd232b287d51 is not prime  
[\*] Number 0x232f1ba7717637fdb9afc11e74cc126f9061ea7a8b4dfdc09dbcd232b287d53 is not prime  
[\*] Number 0x232f1ba7717637fdb9afc11e74cc126f9061ea7a8b4dfdc09dbcd232b287d55 is not prime  
[\*] Number 0x232f1ba7717637fdb9afc11e74cc126f9061ea7a8b4dfdc09dbcd232b287d57 is not prime  
[\*] Number 0x232f1ba7717637fdb9afc11e74cc126f9061ea7a8b4dfdc09dbcd232b287d59 is not prime  
[\*] Number 0x232f1ba7717637fdb9afc11e74cc126f9061ea7a8b4dfdc09dbcd232b287d5b is not prime  
[\*] Number 0x232f1ba7717637fdb9afc11e74cc126f9061ea7a8b4dfdc09dbcd232b287d5d is not prime  
[\*] Number 0x232f1ba7717637fdb9afc11e74cc126f9061ea7a8b4dfdc09dbcd232b287d5f is not prime  
[\*] Number 0x232f1ba7717637fdb9afc11e74cc126f9061ea7a8b4dfdc09dbcd232b287d61 is not prime  
[\*] Number 0x232f1ba7717637fdb9afc11e74cc126f9061ea7a8b4dfdc09dbcd232b287d63 is not prime  
[\*] Number 0x232f1ba7717637fdb9afc11e74cc126f9061ea7a8b4dfdc09dbcd232b287d65 is not prime  
[\*] Number 0x232f1ba7717637fdb9afc11e74cc126f9061ea7a8b4dfdc09dbcd232b287d67 is not prime  
[\*] Number 0x232f1ba7717637fdb9afc11e74cc126f9061ea7a8b4dfdc09dbcd232b287d69 is not prime

[illegible]

p=0xa2e7cd9b5c9541dc49aff069953bf5bfd44313f4a8ad4c1972e8eb41660ec333

n=0x1663ab43fd4876c0f4bb44e1523ee0392febb5d0fe2d24f4606146334f8ba740cb2c857b5768255302f695c  
f91e204bfc994d719dc27fa352bb10ea63ad57075

f=0x1663ab43fd4876c0f4bb44e1523ee0392febb5d0fe2d24f4606146334f8ba74005159c38895cab78ff96e44  
787d9fc9064efd8aaa82cb04eaec5641a99e2f8c

e=0x10001

d=0x14af5897a3f5c2e15a3979d5c22a9cf5b8b4487221a28bb5cb2593b9ec0fd6216b911f978c30b5ab4057a3e  
80236ff04587ccec3c1bad77c45c4d04b5349431

Testing RSA

Відкритий текст: 123554323

[-] Шифрований текст:  
4225738511959622419285247916610390328996966299149529576195059263904875989047176426952433127  
78625686135350408290304694157149020445580514132910969499245468

[-] Розшифрований текст: 123554323

Підготовка даних до відправки ...

[\*] Відправка ...

[\*] Отримання ...

!!!! Верифіковано! !!!!

## Get server key

Key size

256

Get key

Modulus

BEB955648DEF70195AA70C0CF237F7125C756D9B73EB734DA3207CDDA2F3E269

Public exponent

10001

## Decryption

Ciphertext

309cec5fc1b32419322b8b828a65c115e0cec66d01d617d1bbc1b1365b102ba2

Bytes

Decrypt

Message

102410240124

# Перевірка підпису

## Sign

Clear

Message

ffffff

Sign

Bytes

Signature

0BCDA2FB48D952659F452DE39D6D39D211B5394B7D5C1B286B8AB2A49A59F368

```
[*] Number 0x8e67200f1f47f705 is not prime
[*] Number 0x8e67200f1f47f707 is not prime
[*] Number 0x8e67200f1f47f709 is not prime
[*] Number 0x8e67200f1f47f70b is not prime
[*] Number 0x8e67200f1f47f70d is not prime
[*] Number 0x8e67200f1f47f70f is not prime
[*] Number 0x8e67200f1f47f711 is not prime
[*] Number 0x8e67200f1f47f713 is not prime
[*] Prime number 0x8e67200f1f47f715
```

Просте число сгенеровано 'q'

p=0x1957bb954fac4e77

q=0x8e67200f1f47f715

f=0xe18df85c1f4090ff64806bd85e3fb38

n=0xe18df85c1f409109e06e261f4d840c3

e=0x10001

d=0x3db01a70f78b2d1cec5bc3231603ce1

0x39d8e325679340dedd52c8983f6ccc962901dbb57b9a3ba7104c80d8297b15a6

0x4060bc4729e4117f543c96dc20ca65d93e92a265ab0af9fe629c353bd0a5592b

Скрипт показав True, а отже верифікація успішна.

# Перевірка відправки секрету

## Receive key

✖ Clear

Key

39d8e325679340dedd52c8983f6ccc962901dbb57b9a3ba7104c80d8297b15a6

Signature

4060bc4729e4117f543c96dc20ca65d93e92a265ab0af9fe629c353bd0a5592b

Modulus

e18df85c1f409109e06e261f4d840c3

Public exponent

10001

Receive

Key

FFFFFF

Verification

true

✓

Наша програма успішно обмінялася секретом з сайтом, що свідчить про правильність роботи скрипта.

## Висновки

Ми засвоїли основні принципи роботи протоколу RSA та навчились програмувати його самотужки. Навчилися генерувати великі прості числа за кількістю біт в них, робити перевірку на простоту за допомогою алгоритму Міллера-Рабіна.