

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «КИЇВСЬКИЙ
ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. І. СІКОРСЬКОГО»

Комп'ютерний практикум №4

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

Виконала:

Студентка групи ФБ-83

Захаряш Ксенія

Перевірив:

Чорний О.М.

Київ

2020

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.

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 $1 < p, q$ довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб $p \leq q$; p і q – прості числа для побудови ключів абонента А, $1 < p < q$ – 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) , (d, n) і 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 $0 < k < n$.

Хід роботи

1. $p = 0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c8859$
 $q = 0xd5f364d172a78ab7b3498dd1a2af7c60eecd88e457a14c2067f9b52b5ef1f6d9$
 $p1 = 0xd9394bb47f3da7b175c5f208a8a8560f28ea355057b927a3d06c8a86ad69d097$
 $p2 = 0x8cf2a6543c7ebeced479db1648310ed826fdda121a0077d6d667de6494a4f77f$

2. Кандидати, що не пройшли перевірку

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c8813

Divisible by 3

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c8815

Divisible by 7

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c8817

MillerRabin test is failed

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c8819

Divisible by 3

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c881b

Divisible by 5

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c881d

MillerRabin test is failed

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c881f

Divisible by 3

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c8821

MillerRabin test is failed

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c8823

Divisible by 7

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c8825

Divisible by 3

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c8827

MillerRabin test is failed

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c8829

MillerRabin test is failed

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c882b

Divisible by 3

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c882d

MillerRabin test is failed

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c882f

Divisible by 5

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c8831

Divisible by 3

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c8833

MillerRabin test is failed

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c8835

Divisible by 11

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c8837

Divisible by 3

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c8839

Divisible by 5

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c883b

MillerRabin test is failed

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c883d

Divisible by 3

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c883f

Divisible by 7

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c8841

MillerRabin test is failed

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c8843

Divisible by 3

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c8845

MillerRabin test is failed

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c8847

MillerRabin test is failed

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c8849

Divisible by 3

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c884b

Divisible by 11

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c884d

Divisible by 5

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c884f

Divisible by 3

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c8851

MillerRabin test is failed

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c8853

MillerRabin test is failed

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c8855

Divisible by 3

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c8857

Divisible by 5

0x8b0007d5a83e31e0e41af9b169dba5b84e86dfdee34eb499d93408ee1e5c8859

0xd5f364d172a78ab7b3498dd1a2af7c60eecd88e457a14c2067f9b52b5ef1f6b1

MillerRabin test is failed

0xd5f364d172a78ab7b3498dd1a2af7c60eecd88e457a14c2067f9b52b5ef1f6b3

Divisible by 3

0xd5f364d172a78ab7b3498dd1a2af7c60eecd88e457a14c2067f9b52b5ef1f6b5

MillerRabin test is failed

0xd5f364d172a78ab7b3498dd1a2af7c60eecd88e457a14c2067f9b52b5ef1f6b7

MillerRabin test is failed

0xd5f364d172a78ab7b3498dd1a2af7c60eecd88e457a14c2067f9b52b5ef1f6b9

Divisible by 3

0xd5f364d172a78ab7b3498dd1a2af7c60eecd88e457a14c2067f9b52b5ef1f6bb

Divisible by 7

0xd5f364d172a78ab7b3498dd1a2af7c60eecd88e457a14c2067f9b52b5ef1f6bd

Divisible by 5

0xd5f364d172a78ab7b3498dd1a2af7c60eecd88e457a14c2067f9b52b5ef1f6bf

Divisible by 3

0xd5f364d172a78ab7b3498dd1a2af7c60eecd88e457a14c2067f9b52b5ef1f6c1

Divisible by 11

0xd5f364d172a78ab7b3498dd1a2af7c60eecd88e457a14c2067f9b52b5ef1f6c3

MillerRabin test is failed

0xd5f364d172a78ab7b3498dd1a2af7c60eecd88e457a14c2067f9b52b5ef1f6c5

Divisible by 3

0xd5f364d172a78ab7b3498dd1a2af7c60eecd88e457a14c2067f9b52b5ef1f6c7

Divisible by 5

0xd5f364d172a78ab7b3498dd1a2af7c60eecd88e457a14c2067f9b52b5ef1f6c9

Divisible by 7

0xd5f364d172a78ab7b3498dd1a2af7c60eecd88e457a14c2067f9b52b5ef1f6cb

Divisible by 3

0xd5f364d172a78ab7b3498dd1a2af7c60eecd88e457a14c2067f9b52b5ef1f6cd

MillerRabin test is failed

0xd5f364d172a78ab7b3498dd1a2af7c60eecd88e457a14c2067f9b52b5ef1f6cf

MillerRabin test is failed

0xd5f364d172a78ab7b3498dd1a2af7c60eecd88e457a14c2067f9b52b5ef1f6d1

Divisible by 3

0xd5f364d172a78ab7b3498dd1a2af7c60eecd88e457a14c2067f9b52b5ef1f6d3

MillerRabin test is failed

0xd5f364d172a78ab7b3498dd1a2af7c60eecd88e457a14c2067f9b52b5ef1f6d5

MillerRabin test is failed

0xd5f364d172a78ab7b3498dd1a2af7c60eecd88e457a14c2067f9b52b5ef1f6d7

Divisible by 3

0xd5f364d172a78ab7b3498dd1a2af7c60eecd88e457a14c2067f9b52b5ef1f6d9

0xd9394bb47f3da7b175c5f208a8a8560f28ea355057b927a3d06c8a86ad69d07f

MillerRabin test is failed

0xd9394bb47f3da7b175c5f208a8a8560f28ea355057b927a3d06c8a86ad69d081

Divisible by 3

0xd9394bb47f3da7b175c5f208a8a8560f28ea355057b927a3d06c8a86ad69d083

MillerRabin test is failed

0xd9394bb47f3da7b175c5f208a8a8560f28ea355057b927a3d06c8a86ad69d085

Divisible by 5

0xd9394bb47f3da7b175c5f208a8a8560f28ea355057b927a3d06c8a86ad69d087

Divisible by 3

0xd9394bb47f3da7b175c5f208a8a8560f28ea355057b927a3d06c8a86ad69d089

MillerRabin test is failed

0xd9394bb47f3da7b175c5f208a8a8560f28ea355057b927a3d06c8a86ad69d08b

MillerRabin test is failed

0xd9394bb47f3da7b175c5f208a8a8560f28ea355057b927a3d06c8a86ad69d08d

Divisible by 3

0xd9394bb47f3da7b175c5f208a8a8560f28ea355057b927a3d06c8a86ad69d08f

Divisible by 5

0xd9394bb47f3da7b175c5f208a8a8560f28ea355057b927a3d06c8a86ad69d091

Divisible by 11

0xd9394bb47f3da7b175c5f208a8a8560f28ea355057b927a3d06c8a86ad69d093

Divisible by 3

0xd9394bb47f3da7b175c5f208a8a8560f28ea355057b927a3d06c8a86ad69d095

MillerRabin test is failed

0xd9394bb47f3da7b175c5f208a8a8560f28ea355057b927a3d06c8a86ad69d097

0x8cf2a6543c7ebee4d479db1648310ed826fdda121a0077d6d667de6494a4f77d

MillerRabin test is failed

3. Secret A:

0xd52b0263df9b736d38d8158f34cf0129e64560ed754ec8e0c47f9377786ff3c0f02aec185659d2154d1695adcb68bce0d521194ced2b95dd0e58a9fe6da40c5

PublicA:

0x742b2e49f12149842069b7c356e8ee4da7f5f641dfcdc847070a8bec667e82a039da9adf4a4f48e88562504574908c246b0835f5d8be97d7e883c624b13e1971,
0x46588a0ef96e7b1331aa143f7ea4c515495cece23b2e866da1ea6569e5da57279637bc11505adede529c52a7a1591bb3226650a5d1c01c27cadb5d0192f0e6f3

SecretB:

0x1efdf3bcf82171c6291d4cdb090cdf86206e7e301c48fb4fcf8d6be813eedc07aa033808a151fda76f80ce366c4f84f471fcd778dab16afdb1b93381dd0ccd5f

PublicB:

0x77993ab2e76edbaaa6a4c3d3e7b4bb668f2c1d4a2b129a2eab77afc47c73708e4867ffbc4c535117712932a231af94ecd0b0be399ba1ae2461025b7e0c7c2be9,

0x3382781fd575c887978a093497f18d2345945ccfdec46515eaedd7ba479c6625c354bcc8ffaaab63a6e0f0734cd373c1cc88cbbb0ccee1a135902c9f92fdd0d

Message M:

0x4a5758bbb7206ed11c1e5c8de1825f1361e4a3742e6f3fc659700f03fd8bc006ca0f3cf0f4fd8cc0d84c4cd0bbc2a3955a2ca71dbebeb4dd5b00b595aa6ddac

Encrypted message A:

0x147225c363a843a04ce8aeb76ca6caa4d6661ccf81a76f4ed040099fc6b38c7a0183f4edf0b5ea7a7f9c8805ea1723193ceabf883c8b36b6a2ab8232453b49

Encrypted message B:

0x62969dfe1333a749e58549cc986f2ce10e47047046ef80e750d2a4f1519b8620c458094ab8eead63edaf53da5295a1b96fae5c0177409988817fec276603c1b

Decrypted message A:

0x4a5758bbb7206ed11c1e5c8de1825f1361e4a3742e6f3fc659700f03fd8bc006ca0f3cf0f4fd8cc0d84c4cd0bbc2a3955a2ca71dbebeb4dd5b00b595aa6ddac

Decrypted message B:

0x4a5758bbb7206ed11c1e5c8de1825f1361e4a3742e6f3fc659700f03fd8bc006ca0f3cf0f4fd8cc0d84c4cd0bbc2a3955a2ca71dbebeb4dd5b00b595aa6ddac

Signed message A:

0x4a5758bbb7206ed11c1e5c8de1825f1361e4a3742e6f3fc659700f03fd8bc006ca0f3cf0f4fd8cc0d84c4cd0bbc2a3955a2ca71dbebeb4dd5b00b595aa6ddac

0x5d8497f2b3b5900be0947f5ad71544572067f7c8139310e958a5a2c133d6090f6eab67048744d0a26ead9c57a320f480af654df131a3f81748968abdb02b716a

Signed message B:

0x4a5758bbb7206ed11c1e5c8de1825f1361e4a3742e6f3fc659700f03fd8bc006ca0f3cf0f4fd8cc0d84c4cd0bbc2a3955a2ca71dbebeb4dd5b00b595aa6ddac

0x46c4b0def73f3793aad295134170e10ff7fc54b80f02f637234c1a142e51686d535c4599d3ce0afefbd39071149b3578b0e300a84e7fab49b274cc90b8cfb54c

A verified

B verified

4. Реалізація протоколу RSA

Отримали секретний та публічний ключі для абонентів

$d = 0 \times \text{df}2291\text{c}46\text{d}48109\text{c}5\text{e}41\text{ce}6\text{e}413\text{d}5\text{b}3179\text{f}94577469\text{ca}228\text{a}7\text{bb}1\text{fb}96182\text{e}512\text{a}622\text{cb}72964\text{bdf}74\text{d}5\text{ccb}3234908147\text{d}4\text{db}420\text{a}46\text{b}1483\text{b}8\text{ddc}31\text{ddc}69\text{b}4\text{fdd}$

$n = 0 \times 84\text{aa}43\text{aae}56\text{ac}1\text{b}cf\text{d}73\text{ba}4\text{b}70\text{c}174\text{c}271\text{c}2\text{cd}45\text{f}3\text{a}0843\text{ab}67\text{bc}5\text{bc}13\text{c}666\text{e}34\text{b}4\text{c}7152\text{b}33\text{c}49\text{e}cf\text{d}199\text{dfb}43\text{a}140093\text{d}3\text{f}2520\text{a}686\text{e}16\text{fb}323726\text{e}8\text{af}9\text{fff}$

$e = 0 \times 81422\text{e}828\text{df}38\text{a}3\text{bd}6677\text{a}0\text{fd}633277\text{f}9\text{af}40\text{cf}405\text{e}3\text{f}03\text{b}91\text{b}7\text{b}2786\text{a}9\text{b}97\text{a}845\text{ff}78\text{c}34\text{f}2\text{dbc}4\text{be}788\text{d}095\text{cf}961602\text{b}42187\text{c}3\text{e}2\text{a}5855\text{c}3130\text{d}7\text{c}667737\text{d}$

Згенерували секретне значення для передачі

Key:

0x3d72a131eb3a9952d872dc31dbfde9c11a2a556faf7cf9a40b6809336899f39c6d4a615eca8a5814794eace67bad7fb628f455d216f7f6a3411e557800012f6

Згенерували повідомлення, відправлене абонентом А

$k1 =$
0x20df938d246922e7b97a8e3a66d38bdbaa9d3c64d78e15c5aacbc93cec3eaca4d92f0e0633dfb681786c6dc65ece74d70df7a97760ee388077c5d5d20533377f

$S1 =$
0x3c26e9e14b5b8e15558658e367db0b9bdd23542e35f0806b7b74dc215f36e53b21b39f8ddc143607354c8e30a35dd2578649540adcf64961b5733727e8aa4062

Отримали повідомлення від лиця абонента В

Sign verified

Recieved:

$k =$ 0x3d72a131eb3a9952d872dc31dbfde9c11a2a556faf7cf9a40b6809336899f39c6d4a615eca8a5814794eace67bad7fb628f455d216f7f6a3411e557800012f6

$S =$ 0x240c45942a5b0481d03d73f52cd40df0cb82bc61a2abe7d51c76dbfddbd79c39bb254789dc5ad26692654f4aa686dcaa43cc6bbefe20fba2ffac8c1ba1117461e

Секретне значення співпало, цифровий підпис перевірено, отже передача ключів за протоколом RSA відбулася успішно.

5. Обмін ключом із сайтом

Receive key

Clear

Key

808a9b0454c6964fe3ccdc1bc3e62309c4d4ee01cc4dd4c350094c513a1799c718d89bf169d91745f82948cad6debfi

Signature

1732815bf2f35b70fc62e10b41f390a94442cd62b0496639b88fde17ff504b186108e9dcadf044dff46949c7d9ed8d6az

Modulus

83488961b77b8bb162362da8717ac5d9537504af64652d53ac20ad0ffedf110aae4b2a0b539c3a8872551f60be2a8e

Public exponent

2dea9420eeb6fb3dfcff69f6e915c6c059f26e383788ede30d1603da70002e2541d95c69ce70f2bf636aad3ebf8b0316

Receive

Key

01D7

Verification

true

✓

Висновки: в даному практикумі ознайомилися із поняттям псевдопростих чисел, тестами перевірки числа на простоту, був реалізований тест Міллера-Раббіна. Також практично реалізували протокол передачі ключів RSA із виконанням функцій генерації ключів, цифрового підпису, зашифрування та розшифрування повідомлення.