Міністерство освіти і науки України
НТУУ«Київський політехнічний інститут» Фізико-технічний інститут

Лабораторна робота №4

з предмету «Криптографія»

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

Виконали

Студенти III курсу

ФТІ группиФБ-82

Ясинський Нікіта
Кравчук Владислав

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 1 p , q довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб pq < p1q1 ; p і q – прості числа для побудови ключів абонента A, 1 p і q1 – абонента B.
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 A і B – тобто, створити та зберегти для подальшого використання відкриті ключі (e,n) , (,) 1 n1 e та секретні d і d1 .
4. Написати програму шифрування, розшифрування і створення повідомлення з цифровим підписом для абонентів A і B. 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 A и B, перевірити правильність розшифрування. Скласти для A і B 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.

Опис кроків протоколу

1. **Генеруємо 2пари простих чисел. Для абонента Alice p, q та для Bob p_1,q_1 довжиною 256 біт:**

   p= 0xeb0fa137b90afd2d7780ba3220671c9335b8fcb9a667e5087e65060ea52894bd
   q= 0x9e1b3173c0a2166091250194048eabfd215747e8f8624e6607f4859bc877a417
   p_1= 0xc9835b2ce72b6d1844c86c3366bd8798203242cd4509fecb8f0baf461334a8a9
   q_1= 0xfcba3151b3a8d88ab8c08adb8c4ca32402197f56c9c481b18f03a1e5a68b727f

2. **Кандидати, що не пройшли тест перевірки простоти:**

   - **ALICE:**

0xc9d9bb6469edbd3f862cbca40fd0ec5f216c985d92f4eea9661d19c0515a7c91 is not prime number
0xd6ccc4c01f9aff5a9361a835f686c62507bee6ed3a710e5b34f3bdfdca75fd9d is not prime number
0xa68a03fd4e1552c3ab03496c94c8783f0a998051f97bdbe6f93bd267696ddd1f is not prime number
0x85e9d4baf5bce08718fba24a9cdd2ba1601e54b4640a81f02bf517cda7f56bd3 is not prime number
0x9e0de1b6c2169b969432ecf3f8ac36306d3fcfeb88f365fd3d47bb2a115e046b is not prime number
0xdb6df6c08c43e9a5954205b7c63496c2af59921a89e0a5f5bf354e231e22f229 is not prime number
0x91af6be6905c3ee8355e8b35c00526f1f8db5f140f143a4d291f8ba6f079d01b is not prime number
0x8166d60011ea706cbbfd0faa286ae370b2ad1b949adb51b1ea5da960e624167b is not prime number
0xed932cc2a3ecab30393a17e99df6edc95b417abaac56f7363ec25b56f5fec211 is not prime number
0xbfb8cc834c2f7fe9cab55116126761b1e742d8a08cd9f126c0cf8b3230cdd2bb is not prime number
0xd22de8d76446dfb6188fdd7e9c733841403d4d9403fef135ba38aac61a47e589 is not prime number
0xe099287ca546c76fbb2d2db0ea607ed44bc8af2a9f25c3aa816a6e18fdf66c1f is not prime number
0xeedfb2013f6b330cc1bd6f5d79b1d5f9a4c95e532250bb59af366edde70dc7ef is not prime number
0xf72146f529395c52f1a9244b4ebf6c7e61aca0e9ffc00122858405cbf9581fe3 is not prime number
0xb13a5cdcfca2a1c1bcfcc8552f0bc76c2196630dc59256a6b96bf995922ecac5 is not prime number
0xc6fa8c286f53f8217c367bb81d54caa0a19a1fb009a0c35763177549154c4acd is not prime number
0xcb8a66bd35edfd8a58abf3b30993cb0566ce39af1208537898249606e1337dc9 is not prime number
0xfdfb95d2520d7cdbd3cd339e98e166f979794360689845803 7d944528e385db5 is not prime number
0xc1992dce1601cb3787fe7d7847229a0de8654deb508451dba532108abbf806df is not prime number
0xa7bcb3fcda2fd721b885502c4bde0e2b6f53f64361223db423e8482d3e993ab5 is not prime number
0xe5609bf03fa102b73a546a78c14d417431cadb9e6546859fb4e6bc08312bbc21 is not prime number
0x8a2708432e01b86b206add86d059d79ff4851936e4814f2884ffa810d2eb8d0d is not prime number
0xd4511626143f9ceecf265601ee840393901285f9939dd960bfc64a1388f8697b is not prime number
0xbe3469eeffb4751b7dd6fb3b48d04e8322c3577c9c070c7c4026ca38f028e941 is not prime number
0xeaf1e844734bf57c2ba24fe00b1a0d28eade757b5bb3b5519d86a6232bf4f46f is not prime number
0xf8c23c8b5f637978e4f14426ebde22d9f97a9a48a2ce7daeef1a46d021ab3687 is not prime number
0xc36f47043b768378eaf113138eb87c7866b011ca2171063d0ac4e9901ed2aed7 is not prime number
0x90ba682c53bfa432c4bde17beef25a0bbd3492d57a0b040cf3f859c5748ebccf is not prime number
0x8311e69494fa7d4f9571a3e622dbfc735e50ed770e8496fcd382ee3659bae63f is not prime number
0xa351cc0e425a3338fd202184d288ce8da43b3a7824f7cb70369cc4e3002113f7 is not prime number
0xa9f19196ac6cdd7022106966d708411a97891947b2b6bfe5859dc2d219b36523 is not prime number
0x80a6c3c8d13dc34bbf93adb7218272c883968f9deea9f47b633d85acb21e6e77 is not prime number
0xa142d7fd33033a52bff0562f4edf0920fa31af155d65ea42914db8f361ecb419 is not prime number

- **BOB:**

0xff1ac86cbea77bb1038e44a2aede80abeca29c791208e11b844cdbd06fb526f3 is not prime number
0xb17f01e040c0b210b90087b52011741898ef453aae29c89d39fd74129a69ea55 is not prime number
0xf5170c2a9d4cb26f69e3333cd747f30f7e42ba22fd656d6cbbc16471c52462c7 is not prime number
0xad6b5145df0c3791f3e53fd9a3f928bac36035d4958cd3dbe69d0de90d252ea7 is not prime number
0x9931a2d6da7731c8b09aa5f4c7d217677db624886c0ee852f0beadc03ddf584d is not prime number
0xacc01a0e012049569d73eec75a3614418692ca04c816436a9afcf87413a34a7f is not prime number
0xb86f04db1906208dddeb8e9808d33623e4dc5c911fd80fb9510f49dacfaed76d is not prime number
0xf4031d9a3b784744c902c1608257e85d40f5558e226aaf25df01efd00b2e60ed is not prime number
0xe0a3370444051f01b959ecf56fea4c7ce5a41335e2e6e319e02936d0bdc96f3b is not prime number
0xab30328201625e205f2fa9e393f6dcb1755977256102ef23ef7db18402b9c129 is not prime number
0xc6f88377b1dd826efeac79ef5c3af6d01fb3b73136f76d09a11ea175bb12cfc5 is not prime number
0x87370b1dce19e82eb32dbd129159a3df879df55d64782f2c1eb9c980b49e66e7 is not prime number
0xa3533deef2eee66da54366fc92394b1a4d618bad2fa453d5fc46aa004e779e89 is not prime number
0xfe00b2a0721dff225d69ee9d9ac77e4b967ba78423a5c97aee9a8eda5625d095 is not prime number
0xe430789957a19819b00f292c33213b277f0c4095b436cb65a98ba58dd1b2b2fd is not prime number
0x8d7659151be24c4548e21c07d0ee9c24a51a19c5b343233bea7634d8043d3453 is not prime number
0xbd734b7a8039dc0d453436529a544f9527db9f700544e36ae04b548136128fed is not prime number
0x9a982d53e8e0c4e6d9533e083c27808aa633ca5083b4b811ec23f1eef881a513 is not prime number
0xc0d0774c4ba5a17a34ff2ad9a904cc972b907eac9c5ccd44917e61e7683d0baf is not prime number
0xec90742546ab1ea81d7580d2cbd12d3e9cf8dc2ad67249b6828cce6643ae14d3 is not prime number
0xdf86122321997f8bdf08bda2fe35cca4f16818bd032ab13bcfc01583f18409af is not prime number

3. **Генеруємо ключові пари RSA для AliceiBob, де(n,e)-open key, (d,p,q)-secret key**

- *Абонент Alice формує повідомлення, використовуючи функцію SendKey(), де ще використовуються функції Encrypt(), Sign().*

  k1:0x55dfcb80b1a243ccf8bac6166d37e21199714b35c8b34b84172f159378deddceb7019037434756bd2af4f58152a38098257d8f5e876f8c8e43fe52e201f8272e

  S:0x7129c80c9b5cb17716910b37cd7132ecdc13ab46130634f46ff04ec41eba9b0c02ee32dea57abd3b3b629ec17b0c61671b25f8b123a96095917568b873945831

  S1:0x2446e2fc62d4fda5e28bb5ded4eb098d246f09a8bafb9f31dda9cab7f782f6c8d4fb9eeed32408bbb9936ae76a99fc57d6a3fc0f11b1d0a35352a9664f288c66

- *Абонент Bob приймає повідомлення і за допомогою свого таємного ключа перевіряє підпис Alice.*

  k:0x2726847778b74722b11f948191a9e4770ea541cf42b79ca1bc46077320ba5991ab3888b5322fbfb53da863a8bbc43eb8373216a0bfb87190126ca96c974fd87c

  S:0x7129c80c9b5cb17716910b37cd7132ecdc13ab46130634f46ff04ec41eba9b0c02ee32dea57abd3b3b629ec17b0c61671b25f8b123a96095917568b873945831

  S^emod(n):0x2726847778b74722b11f948191a9e4770ea541cf42b79ca1bc46077320ba5991ab3888b5322fbfb53da863a8bbc43eb8373216a0bfb87190126ca96c974fd87c

  ***S^emod(n)=k**, отриманий підпис правильний.*

Параметри криптосистеми RSA для абонентів Alice і Bob

	Alice	Bob
	Open key	
n	0x840bf814041a0b93d897fe25ab911c8f85184643667acca48197ad08567448c4db6aa3aae03c4a8558 6e8ae9bab8214203fbe06d9f7870be33aefac0d3a74833	0x6333f3f1fa50a54206f509bf1a14751fba65a41e54e25cc0fe94b8d5d5d818f035a8307bf4fa65dabb7f4669edfcb83e285768c26f745b1a0007305115ba2985
e	0x912c9d8eabd6f037d0fae77361bdf2b1fceb11d4c0dee997d565c4001100c5eab006ccb297861822734dbfdd0170877b993b19d5ff61592658c7a69ea1c970fb	0xc6efde02e69de7cdde3c825c70dfceb2389377ea96a7280d11e8d7be32644ccb426370bf62b1d1de5686ca1f67210493d65fb4f62eb9911f7381e37323fdedd7
	Secret key	
d	0x8ec7158f4ba13cb7b9aba89dcd9a1a31d618356f66e70ead457e67e9c3b17d67c92433b989d15d89aaf91b5c8a7b59aaea493bd2ee3d5a98d68fc1414c34905b	0x6a9e8c337f7029fa4fa019c6e70eaafd0638927852a9789eebc23841568d15ce1714ac09c318b2764a29a63c0c7a01fadb7c65204cbabf211c7475e4629154bd
p	0xeb0fa137b90afd2d7780ba3220671c9335b8fcb9a667e5087e65060ea52894bd	0xc9835b2ce72b6d1844c86c3366bd8798203242cd4509fecb8f0baf461334a8a9
q	0x9e1b3173c0a2166091250194048eabfd215747e8f8624e6607f4859bc877a417	0xfcba3151b3a8d88ab8c08adb8c4ca32402197f56c9c481b18f03a1e5a68b727f

4. Чисельні значення прикладів ВТ, ШТ

ВТ	ШТ
0xabfc3834e92a7abf1f1b21c9f38ded97b4bd192ff765116f45a8aa625f68f018bb8c961a28eabe65752c11d9ac6f77e347dab7306e7f3c53e19e86a7477c569	0x63e1da0366e5b999edd564ca0a520a64300574bc8aa1a66a0013ceb0e53cd2849478d9777e4e1ea368cdf4bef3d88c9eb45e1d256b3a9ec9283ebef5491efd74

Цифровий підпис для Alice і Bob

Alice	Bob
0xa4b09bb0270af652422f71ce71c04570e911dc976abdba71d674154c34a710ab7f43c6935e1970d940bc1db14f04c8a91b4d1062c3ba1049c35a03ad1a7b5c3	0xa4b09bb0270af652422f71ce71c04570e911dc976abdba71d674154c34a710ab7f43c6935e1970d940bc1db14f04c8a91b4d1062c3ba1049c35a03ad1a7b5c3

5. Опис кроків протоколу конфіденційного розсилання ключів з підтвердженням справжності, чисельні значення характеристик на кожному кроці

- *Згенеруємо пару ключів (e, n), d довжиною 256:*

e	0x50d8a9c8d0130340309285be759985fe539b28ae9fa9f12e3681813ab57825ed4bbec252ce28e5e584bfe47309eadbbddb62b082db5e0b58a73d4f02e31fd823
n	0x8f3b7483872cb4c27a636fd119ea9fae28ab965c8c8aa910a700bde8cb01f982b44fc9ba144c3f8726fc8fb640ad2c1773177fea32d77c0fed845c2e3775f519
d	0x78ab2bc164264b4ec948df28e26f987445d8ae664437195d3c5f8af0ef01d39a80758356273f6964355dcb30ed0825071211accf45bf5d2c270965420416e18b

- *Надішлемо сайту запит на отримання його вікритого ключа:*

keySize=512

Відповідь:

n1:B1072EDDA4D375F6C762271D04149A1FD2AA979B8A122D5577A5F5B6114C9433498C188BC013343D15288F8EE290E7F244417D8C2696B9A6751F4E814B81F8CD
e1:10001

- *Функція SendKey поверне нам значення:*

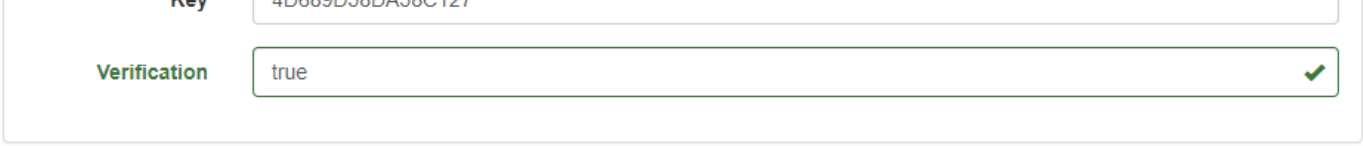
- **(S)** цифрового підпису ключа k = 1234, який створено за допомогою нашого закритого ключа d.
= ( )

- **(k1)** зашифрований відкритим ключем ключ підпис k

- **(S1)** зашифрований відкритим ключем сайту підпис S

-

S	0x50126476b119b388471faa04037d0a8f97344bb787431e9ed694b0f17394a44a6f19fde190afefdf6b00b2f1c9b0c3128e4dcc104a350b8630d2d1aba91644ab
S1	0xa704ea3a6de5d69bca7fe78e19dc7cce7a990c8177b0d422ea7a6dd2c076dcf30180acb0e9553dbdffc5c26d7537fe6d69b61afe5b99fe05dd2cf41dc770649f
k1	0x18d87c963cb6f6e6af705ab9877b69d7f3c92aed28e8c680a231d36896d0ee46b1ac1804102497934d1f896fb0610559d8231bfb5ce677e7534b09d7cf404e62



Висновки: в даному практикумі ми 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.