

МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Лабораторна робота №4
З дисципліни «Криптографія»

Виконали:

Пасько Олександр ФБ-84

Завгородня Анастасія ФБ-81

Перевірив:

Чорний О. М.

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 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 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_1, n_1) 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 $0 < k < n$.

TESTING ON LOCAL MACHINE

Info about Alice

Name: Alice

Public key:

[10729185138981678894691289091197050375576012001576476346526875663559441722601826204306580468789479432551450782124736747440401943507391648584957040331340221,65537]

Private key:

[359674988942776577073054337753634125381700388596724270767956205392985541977138953723176677739894088400192052649103952636931271495642896315608289937332973,112100905106543215571141397725314857196943979138203960130836357125004401561871,95710067004226420772710141715201239171235429145059524525948397144508563828851]

Geted key:

[7705750750558847542058921584160623548739813768157291839403178516896892659475418176599700577111487259946222461584337251271266448064832711204368957060800319,65537]

Info about Bob

Name: Bob

Public key:

[7705750750558847542058921584160623548739813768157291839403178516896892659475418176599700577111487259946222461584337251271266448064832711204368957060800319,65537]

Private key:

[2225528330661731026383436345041614393862202954112657276595257075664500728726479988164216320584531102078546317382669516778668448977963891928843358131956097,108237829475461003775805862600667565402446425559317027823799246478734490248547,71192768627218699194186706102246137066032596996536115790632935246141743522677]

Geted key:

[10729185138981678894691289091197050375576012001576476346526875663559441722601826204306580468789479432551450782124736747440401943507391648584957040331340221,65537]

Test encryption and decryption

Open text: 6967707817

Encrypted by Alice:

4551713662606982919647938181697035947603972980861117959841434071402789095833919235922266372098043165063916908033599682042942804182261499600902902804249596

Decrypted by Bob: 6967707817

Test signature and verification

Message: 6967707817

Signature:

15178793602750943842516798574586611357170690392105993300557803614808362862640339
80467262394596453969246056653536654206435411650881878657517454098132297084

Verification: True

Test for sending keys

k:

0x8e0bc11dc015bc53978e22149b2aad028760dcd32ff91b99f652e5a520744c16c66d2f0087fccc655
8b69f777d370f0d3cc511c7f21df4b5787f85a809881f1a

s:

0x57be199871033dfc6599a14136d59f7e65fedcafe4d49e72dd4a7866b8f7bf3c8ce1241b6ab49084aa
bd902262630653162db8ec87ca31962e89006ea38bd828

[7439548249408391668857916866565834515367261986075478706986068600385016442130229
570433627243626259542900175180415155990820842254987017864767948084866457370,
True]

Key from Bob to Alice

Key:

74395482494083916688579168665658345153672619860754787069860686003850164421302295
70433627243626259542900175180415155990820842254987017864767948084866457370

Validation: True

FINISH TESTING ON LOCAL MACHINE

Усі відсіяні ключі можна знайти у файлі test.txt

Modulus:

C55E48E7EA3D59427BACE7850FBCEDB3CC4293B4C9F907CFB6A1E0BEEED8CA3D6E3D6
9C405A2563392952B590CDA259D7A3D56C56B27E610AD531D3796F6C2B3

Public exponent: 10001

Me.hexinfo()

Name: me

Public key:

['9462e6da32248e33d67cfa2e5b67ad448d0772d22e488951e65080a7819d2c241a4090812a4baa7a2
45de259028ac0af884d95ebf8e9a6a0a2774f4f1f21908d', '10001']

Private key:

['b8c16c2ec1c0424ec901537fe4cf722da86b5dcdb554fba5bddefe519250e0631ec920728e98bffa9fe
82fc5cc775f53e678fb575bfa2d8865bc853192d07cff',
'fa16315726d10f3790dc9b2a470cc7f47c73cfc80b9896521b6e3695ad2ce013',
'97e51a8269711fb7888dad70332b1c6f5518b6d457e0cba16415691823d820df']

Geted key:

['c55e48e7ea3d59427bace7850fbcedb3cc4293b4c9f907cfb6a1e0beeed8ca3d6e3d69c405a2563392952b590cda259d7a3d56c56b27e610ad531d3796f6c2b3', '10001']

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

Процедура SendKey працює зі змінними public_key, private_key, geted_key

public_key = [n, e]
private_key = [d, p, q]
geted_key = [n1, e1]

Де:

n, e – значення відкритого ключа користувача

n = 98db444a27c80a21c0d7e84a5c9a1da4ffc96cd1525b8edf0142b9bbf8620e27614108386cbe05c8c8cf8e4c8d776055644fc2803ffa47fe58d1514037dde34eb

e = 10001

d, p, q – значення закритого ключа користувача

d = 4f4cf210c6b2b10ef1cd116602c4b1bc7837378d20fcff1212c55b367995e5611b7bbbed8d895112c365a7a9281b8341f36f58df79516bf2b611bc04aa142179

p = c2ab3d7825072ce32f9e7c5f2a0e8196b34019e9075b3d8944d0498ddc1797d5

q = c903b430430817695a523579f803f6428eceb0e1f6da64eb663652e795dfb9bf

n1, e1 - значення відкритого ключа сайту

n1 = 83e80c80e070f7992121265a7ac9bb11f711cb974d1df43d9013cab5d044a59c94e297ac083eb4457bd3d9bac0ee6b7e5b5372b443d7f839a935016d2953492d28c02ef6f7441d9c27df6deefb2458713e417861dc10a3046513d32986623dfaab8ae2c176aa46a12b33cfc9403af55869610202fdff8942e68aa1dfb0c3b80b

e1 = 10001

Генерується випадкове число k, $0 < k < n$

k = 0x85eb5794a3dde283feb606b04a44afd79011674228341e9920cb1ff065991d744d644f490bd45fb9c11b7783d51d996d62636bf877ef4de180a0b73cd0cc1fa5

Змінна k підписується за допомогою секретного ключа та модуля відправника.

Результат зберігається в змінній s

s = 0x29c97b5b4386180ee8921ca9661a4356053ece8990e864394f9860a636a25e426633ee785472e023fe8935d77294eed56842fc69356759a0b42c3ae6b183036b

Змінна k зашифровується за допомогою відкритого ключа отримувача та зберігається в змінній k1

k1 = 0x6677bf67be2681bc35d00e44020b440aa08c365c49ad4f603a2aa7cd8287d4a883b346fbbfab83176683a455c1cb1a3d7b58967941eb080467a69738ca9ac7850a0f9b24142e56c3ec7f9737b67f658c7793175807d9435e988333e90e3966d0f30469af5dd66df6971df6c8123cbf5ee04f252acd2288300493cec458ef74e5

Підписується s за допомогою відкритого ключа отримувача та зберігається в змінній s1

s1 = 0x45c9cb9592ff11beab61fdcb234ae24d1ab4c49a367e8401edc6662917f29ef85ed355d7a9a8a0364fc9a714d8306b4cfc98bdb2b0349e2958714ba72db022eb56fb0f468299ea9ba5c559e4270605c0


2adac132c64cbf4900cbbea658f6ee066dfab483dadb57172f9d47f39e50e3e407c1ecf72abf08aad65f092a10b53951

Повертає масив [k1, s1]

Verification from site:

key = 85EB5794A3DDE283FEB606B04A44AFD79011674228341E9920CB1FF065991D744D644F490BD45FB9C11B7783D51D996D62636BF877EF4DE180A0B73CD0CC1FA5

Get server key

 Clear

Key size

1024

Get key


Modulus

83E80C80E070F7992121265A7AC9BB11F711CB974D1DF43D90

Public exponent

10001

Receive key

 Clear

Key

6677bf67be2681bc35d00e44020b440aa08c365c49ad4f603a2aa7c

Signature

45c9cb9592ff11beab61fdb234ae24d1ab4c49a367e8401edc66629

Modulus

98db444a27c80a21c0d7e84a5c9a1da4ffc96cd1525b8edf0142b9bt

Public exponent


10001

Receive

Key

85EB5794A3DDE283FEB606B04A44AFD79011674228341E9920C

Verification

true

Висновки

В ході виконання лабораторної роботи ми ознайомились з тестом перевірки числа на простоту, методами генерації ключів для асиметричної криптосистеми типу RSA, системою захисту інформації на основі криптосхеми RSA.