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

Криптографія

Лабораторна робота №4.

Виконали:

студенти гр. ФБ-94

Дум’як М.Р.

Мельниченко О. Г.

Київ 2021

Мета: 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. Постановка задачі:

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 p1 , q1 довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб pq <= p1q1; p і q – прості числа для побудови ключів абонента A, p1 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) , (e1 ,n1) 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.

Get server key

Clear

Key size 256

Get key

Modulus C606EB2ED40AC9D3591308000A1E05CA79CABBD890BC8D704CB7172E67D4A22B

Public exponent 10001

Encryption

Clear

Modulus C606EB2ED40AC9D3591308000A1E05CA79CABBD890BC8D704CB7172E67D4A22B

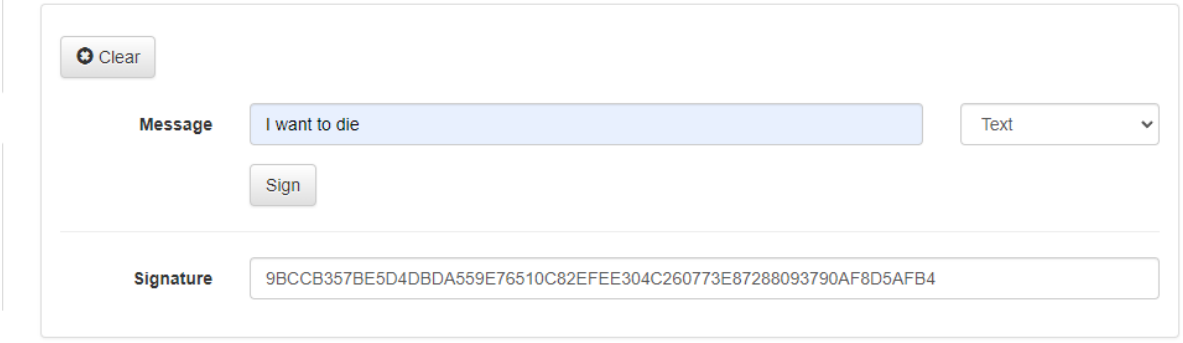
Public exponent 10001

Message I want to die Text

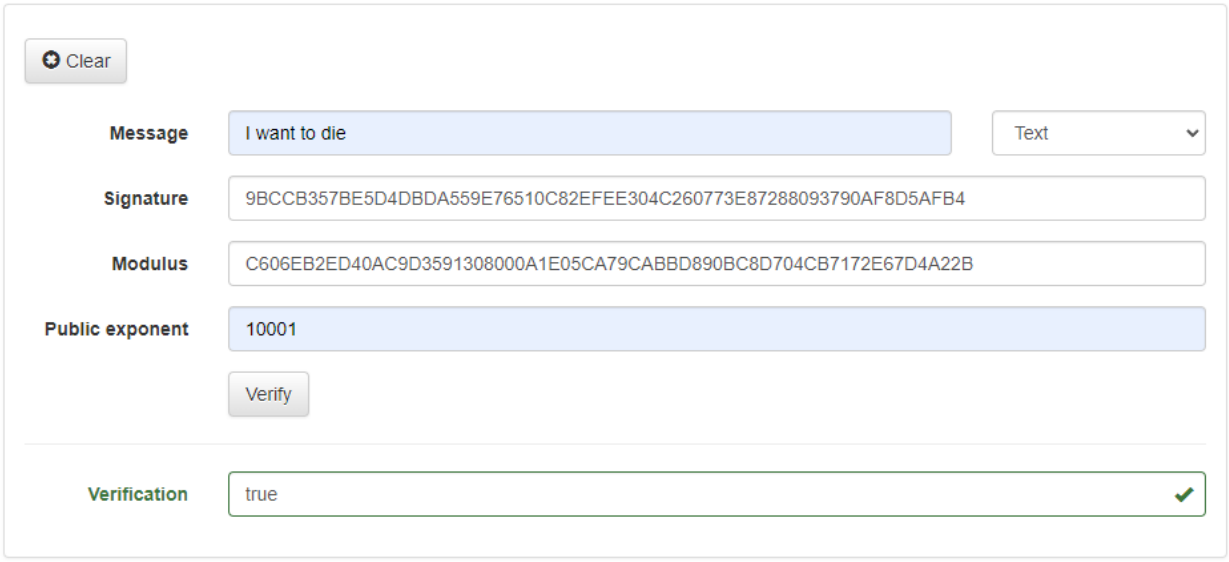
Encrypt

Ciphertext A15DF4786E52323B3119D3E1B95389B6396E1534B02518C5DF57D2CBB4B42EB7

Sign



Verify



p = 187156463707002327242518278048595454514917679063365971927821472291072504766441

q = 127959056034053068909358638400152563064201296452461878347117921496951779449943

p1 = 171609582938160317934866051290435176704795499855788447312475043502134297275223

q1 = 195675775422407457345536838409950592640387574122239004231901911557680475080 71

Повідомлення: 111333555777999 Повідомлення верифіковане!

Публічний ключ Олександра: (e,n)
[855601350823450830187332378518979405267731989116035112986949029495
457717444668856940682957252993780380441614390419628564589408174526
867632078710283548934 1,
239483644266195303392021512519787299097273993666288233537823716369
407169084031305131273407168458957010933410534244479175630567075550
5425789187046066576286 3]

Приватний ключ Олександра: (d,p,q)
[500250274025580680145786102409305829096972515879165173304160640006
066104339819463543655048114470135591588724171910811441310572790116
113512318713420179762 1,
187156463707002327242518278048595454514917679063365971927821472291
072504766441,
127959056034053068909358638400152563064201296452461878347117921496
951779449943]

Публічний ключ Максима: (e1,n1)
[595611568942916634153428837208709878551210444049306914096494725455
845750186319694898877167684939101550325408662270993282945965131738
217924333965100613163,
335798382113404648711876349939260296747539686246565158348817128410
763535451998055239010970775752992462072873900582322483975790783164
085830447827504008248 33]

Приватний ключ Максима:
(d1,p1,q1)[362627786935924149638307018954938912683336348735703867738
820620456026357704991929585413541115378774005865058989762883532942
475158627929003067887421138226 7,
171609582938160317934866051290435176704795499855788447312475043502
134297275223,
195675775422407457345536838409950592640387574122239004231901911555
768047508071]

Зашифроване повідомлення Олександра:
284249438670287436004160850257687837810297174223859942495461297155

237947012873767105645212921896267132088501856458871770028233407288
922140598601568634380 7

Розшифроване повідомлення Олександра: 111333555777999

Підпис Олександра:
206663910822048974097826227086954247683189795632288987631719251474
755561475568280276891046580616764986111791979957977211548617948685
7514732434037695458215 9

Перевірка підпису: True

Зашифроване повідомлення Максима:
992350103338128350188387242239295848252985804010039420184900322429
323835304466681620089670820557038861368920724564548471731011857565
0979736703097632796982

Розшифроване повідомлення Максима: 111333555777999

Підпис Максима:
206785534552784307137902188667054330802696816229841914878592469400
703091813300471500459870623159480991265260616388559237143206241038
3529745502720438722583 6

Перевірка підпису: True

mod =
1C9412ABC218EF4969CE74625CE6E93808A3C09A524F7976E7161E3D6AED
7CD9EA087109F7D5966D35C9631406B48EAE13E8ABBCC5A5735D02976E0
FA2DC9942F

e =
23EC57DE68C137CC9B9C00DBD977F4A3385837492A453FAF3C43642C9159
59D825AF3490B161AE8AB1120A2BADABC0C7DAE20DA06196B179E5FE71
3DE8718459

enc=
160A8640ECFA8D7B3B916BFCAB9E9AE57306E947FCEA89BA6B5C047D79
2EB5080065E88931A8E3C6B2A59052D73C48CAFB243BEDC18C1BC2FFBD
0B6A7B93C219B

Зашифроване =
A15DF4786E52323B3119D3E1B95389B6396E1534B02518C5DF57D2CBB4B4
2EB7

True

Мій підпис =
D71857A78A056FEC9E6D136DB7872D4EBC1A7CBB073B6FE253F48A014485A8F6A2ACB12B262140F119630EA53FF002BF304CFD59A2155673ED0BB1A853C062F6

Висновок: при виконанні даної лабораторної роботи ми ознайомились з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA, практично ознайомилися з системою захисту інформації на основі криптосхеми RSA, організація з використанням цієї системи засекреченого зв'язку й електронного підпису і вивчили протокол розсилання ключів.