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

Лабораторна робота №4

RSA

Виконали:
Дяковський Кирило
Щербаков Олег

Група:
ФБ-82

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 криптосистеми RSA, організація з використанням цієї системи засекреченого зв'язку й електронного підпису, вивчення протоколу розсилання ключів.

Задача

Реалізувати механізми перевірки чисел на простоту, за допомогою їх знайти пари простих чисел та реалізувати алгоритм RSA. Здійснити обмін ключами по протоколу RSA/

Хід роботи:

1. Реалізація та тетстування функцій на знаходження простих чисел
2. Реалізація користувацього класу з методами, що здійснюють шифрування алгоритмом RSA.
3. Реалізація високорівневих функцій для роботи з сайтом

Труднощі, що виникли були пов'язані з алгоритмом пошуку простих чисел та з під'єднанням до сайту.
Розв'язання труднощів здійснено методом аналізу та тестування кожної функції окремо від інших.

Результат роботи програми. Абонент А та В створюються програмою.

```
263785723218093510166226540739468964302931508969042141738356458283679233
7817343 Faild!
115542625977379042590878856315180549839962152100662899283649192818556915
257259  Faild!
716644247399943126861074360880776045854720136383468162938785364158449767
60241   Faild!
409236646044715967687770507165421453615784201316872861368355370722842532
5903    Faild!
498194667820074507717849628242027850071340570303543221119176944629614219
67351   Faild!
116677449967445940662477621766298535926917268858271686627044685273645464
26099   Faild!
397191973459197816082003186863619519654633201909904337491615053901776972
50869   Faild!
672708995021773442362320323341966909620023690921561552347702331320656551
43049   Faild!
934111930024307776563148761216004037188938780292421960412630232434267501
78581503        Faild!
149457908803889244250103801794560645950230204846787513666020837189482800
2857304063      Faild!
979487351137168551117480275440832649299428670483906649561634158604994479
95256279138303  Faild!
250748761891115149086074950512853158220653739643880102287778344602878586
86785607459405823       Faild!
```

```
673098582396769173934285125910951713880013352194102328669464231603988523
785085571260260385449574 3       Faild!
180683524898630306131793141807923738709362913482312459107049504286306270
801016291320268491246892269069926 3      Faild!
462549823740493583697390443028284771095969058514719895314046730972944053
250601705779887337592044208819011583    Faild!
740079717984789733915824708845255633753550493623551832502474769556710485
200962729247819740147270734110418534 3   Faild!
485018643978511800019074881188826732136726851501130928948821864976685783
581302934239851144902915348306603890704383     Faild!
317861818517757493260500914135909487173125309399781165595899897431120795
127842690983428846323574602666215925812025098 23
Faild!
130196200864873469239501174430068525946112126730150365428080597987787077
684364366226812455454136157252082043212605480239103     Faild!
218432978428936900610046693566693655459952751037110639326584065785026916
431936079489033755664442040362814688869921606 4755179454463      Faild!
349492765486299040976074709706709848735924401659377022922534505256043066
291097727182454009063107264580503502191874570360828712714 23     Faild!
366469726062561503190528514805422986348120665394382921188019541383360614
279254090378068895007356763064766040314347069490676328263046922 23
Faild!
938162498720157448167752997901882845051188903409620278241330025941403172
554890471367856371218833313445801063204728497896131400353400120934 3
Faild!
150105999795225191706840479664301255208190224545539244518612804150624507
608782475418857019395013330151328170112756559663381024056544019349503
Faild!

##########################################################################
###########
###########   My Keys!    #############
p:
113178022654792066559390596765989047752590928794248404195619000520553065
736129
q:
675805089981887441545451033203771023684762532052309404993373330495465326
7816619169361690623
##########################################################################
###########
###########   My Keys!    #############
p:
652972983685091438136104990432262031411871010056699124264682937978655465
97789
q:
593455436717092572097672210070045362355678733556669679152453072263170982
33075290757367070719
Signing ...
Decrypting:1337
Decrypt!
res = :1337
Signing done!
Encrypting [1337] ...
```

```
Ciphertext:
9f220dbd9b90bfeb541f298e0ce4ff85f23f5369ff3c31cf795d6d01f3388dd6e80c9abc
e5c3af5c16c4aca532eeaf5e9bcf7c3fa8b8c445c51e3a94fa500e77416b18b6b899
Encrypting
[504c13119c9477851e18d03fcef0238d1d870d23eb3d7a345842bfcead63582e63b0011
457fba29d4604761c4d571906acfa095a753a649aae168a69281c50e8041215b2641] ..
.
Ciphertext:
9b03954c4c084eb9f44636c6191bb77ecf3098e5ba97c3d09c6ba025b9f83a02f2401d52
c7be37185e5c62a528b837ac65505623f8b88a54a81f68f660c7282583c2d963d3f0
B.e = 41e64354f3c712a95a3372aa4942ea29c0a6a8ae0710a31e53b3d4e694b9b90b
B.n =
33e2132143a316025ac79518b94a10bdbafe760d2ca9d6b748367fb6f18959164141263e
f07876f614dc73d06cafd212f8d624184b3f130226dc7514d951f207cac3a4c2183f
Decrypting:9f220dbd9b90bfeb541f298e0ce4ff85f23f5369ff3c31cf795d6d01f3388
dd6e80c9abce5c3af5c16c4aca532eeaf5e9bcf7c3fa8b8c445c51e3a94fa500e77416b1
8b6b899
Decrypt!
res
= :9f220dbd9b90bfeb541f298e0ce4ff85f23f5369ff3c31cf795d6d01f3388dd6e80c9
abce5c3af5c16c4aca532eeaf5e9bcf7c3fa8b8c445c51e3a94fa500e77416b18b6b899
Decrypting:9b03954c4c084eb9f44636c6191bb77ecf3098e5ba97c3d09c6ba025b9f83
a02f2401d52c7be37185e5c62a528b837ac65505623f8b88a54a81f68f660c7282583c2d
963d3f0
Decrypt!
res
= :9b03954c4c084eb9f44636c6191bb77ecf3098e5ba97c3d09c6ba025b9f83a02f2401
d52c7be37185e5c62a528b837ac65505623f8b88a54a81f68f660c7282583c2d963d3f0
Verifying ...
Encrypting
[504c13119c9477851e18d03fcef0238d1d870d23eb3d7a345842bfcead63582e63b0011
457fba29d4604761c4d571906acfa095a753a649aae168a69281c50e8041215b2641] ..
.
Ciphertext: 539 // 1337 у хексі
Verifying done!
The Connection between A and B is established!
```

Опис кроків протоколу конфіденційного розсилання ключів:

Абонент A(d, n, e) формує повідомлення (k, S) і відправляє його B(d1, n1, e1), де

k1 = k^e1 mod n1

S1 = S^e1 mod n1

S = k^d mod n

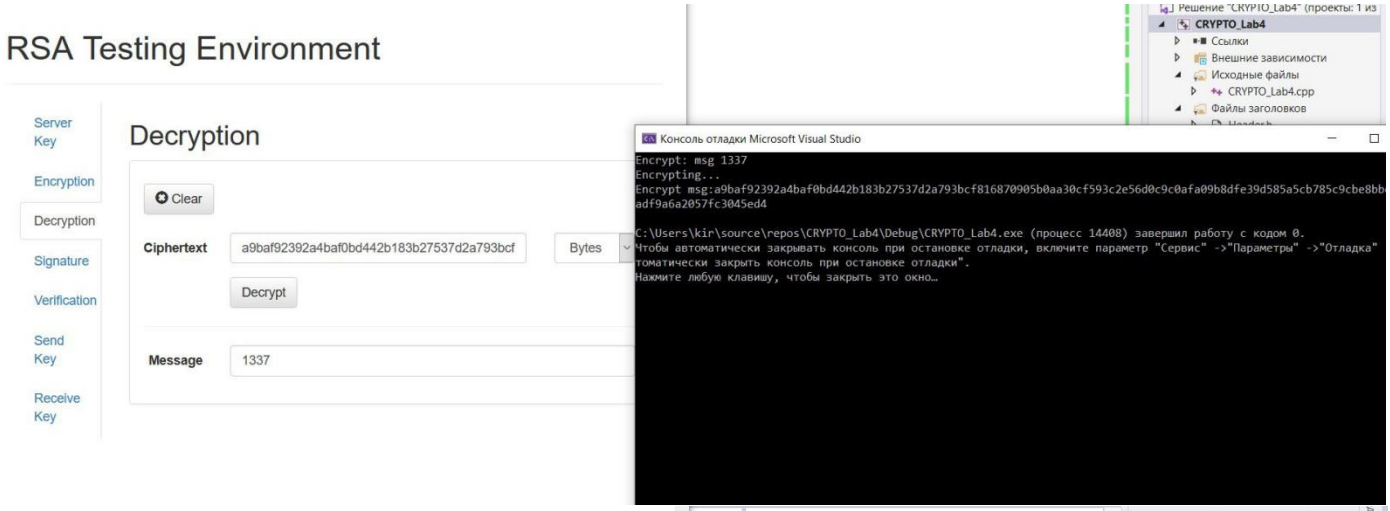
Абонент B за допомогою свого секретного ключа d1 знаходить (конфіденційність):

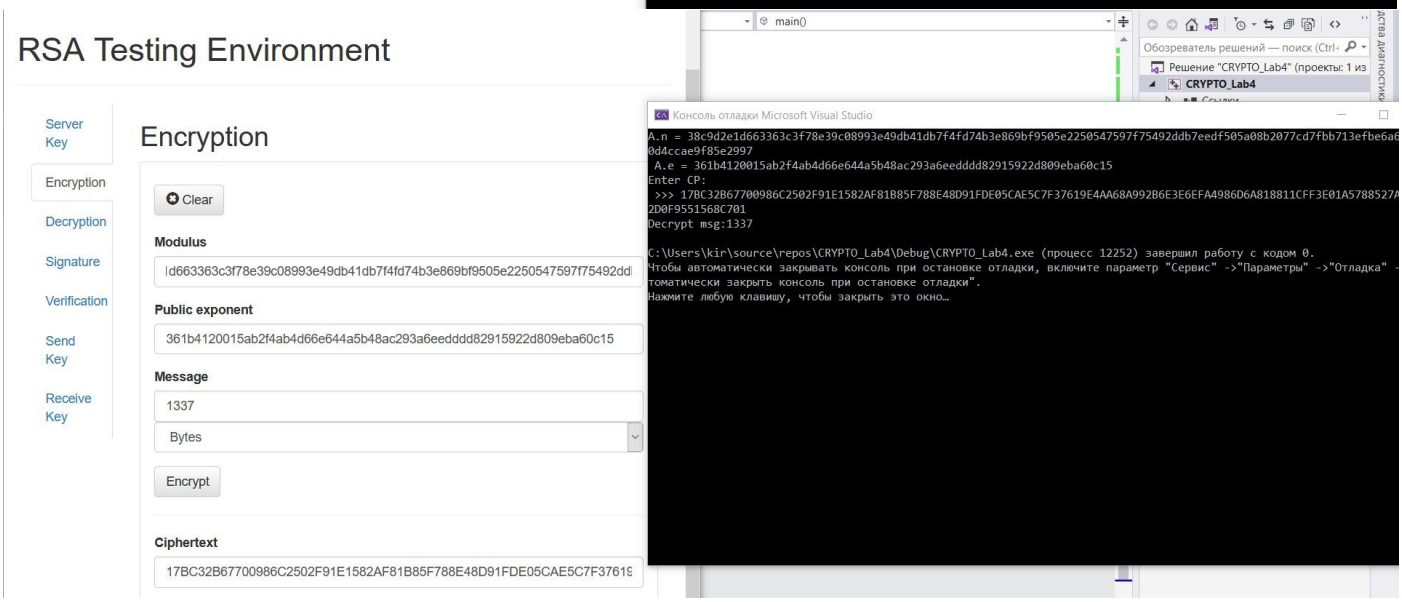
k = k1^d1 mod n1

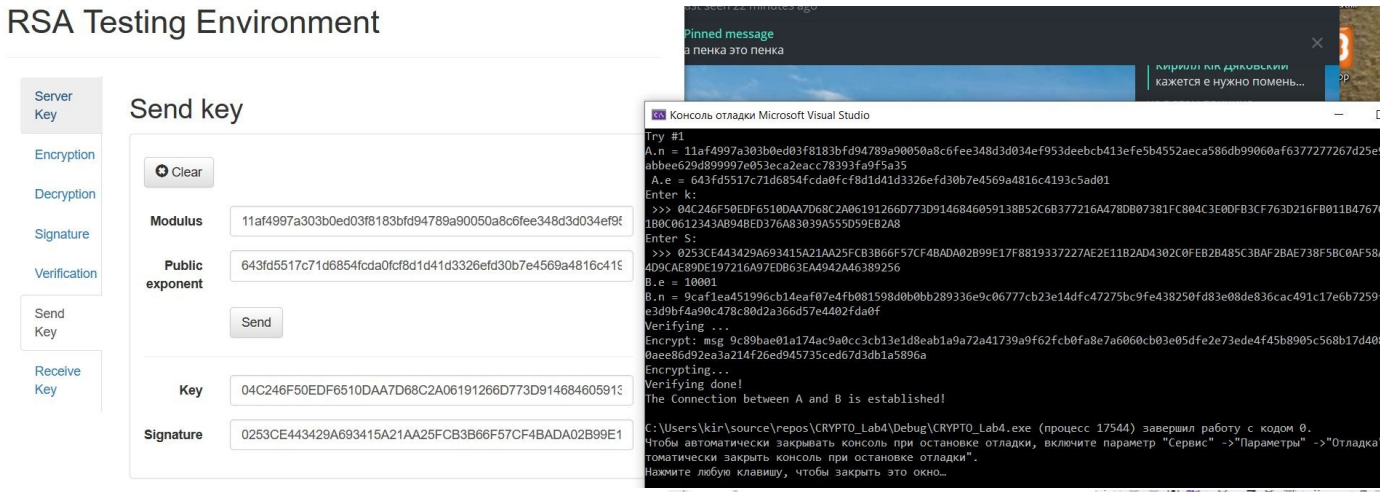
S = S1^d1 mod n1

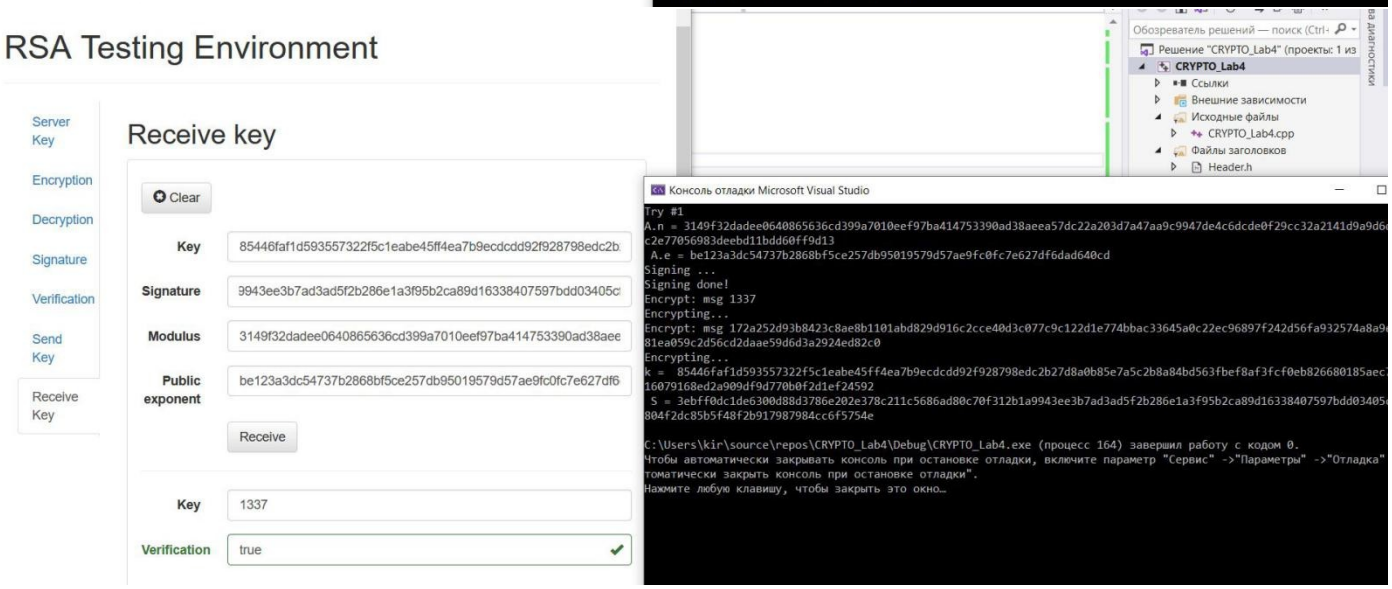
І за допомогою відкритого ключа e абонента A перевіряє підпис A (автентифікація):

k = S^e mod n


RSA Testing Environment
Server Key
Encryption
Decryption
Signature
Verification
Send Key
Receive Key
Decryption
Clear
Ciphertext
a9baf92392a4baf0bd442b183b27537d2a793bcf
Bytes
Decrypt
Message
1337
Решение "CRYPTO_Lab4" (проекты: 1 из
CRYPTO_Lab4
Ссылки
Внешние зависимости
Исходные файлы
CRYPTO_Lab4.cpp
Файлы заголовков
Консоль отладки Microsoft Visual Studio
Encrypt: msg 1337
Encrypting...
Encrypt msg:a9baf92392a4baf0bd442b183b27537d2a793bcf816870905b0aa30cf593c2e56d0c9c0afa09b8dfe39d585a5cb785c9cbe8bb
adf9a6a2057fc3045ed4
C:\Users\kir\source\repos\CRYPTO_Lab4\Debug\CRYPTO_Lab4.exe (процесс 14408) завершил работу с кодом 0.
Чтобы автоматически закрывать консоль при остановке отладки, включите параметр "Сервис" ->"Параметры" ->"Отладка"
томатически закрыть консоль при остановке отладки".
Нажмите любую клавишу, чтобы закрыть это окно…


RSA Testing Environment
Server Key
Encryption
Decryption
Signature
Verification
Send Key
Receive Key
Encryption
Clear
Modulus
d663363c3f78e39c08993e49db41db7f4fd74b3e869bf9505e2250547597f75492ddl
Public exponent
361b4120015ab2f4ab4d66e644a5b48ac293a6eedddd82915922d809eba60c15
Message
1337
Bytes
Encrypt
Ciphertext
17BC32B67700986C2502F91E1582AF81B85F788E48D91FDE05CAE5C7F3761
main()
Обозреватель решений — поиск (Ctrl
Решение "CRYPTO_Lab4" (проекты: 1 из
CRYPTO_Lab4
Консоль отладки Microsoft Visual Studio
A.n = 38c9d2e1d663363c3f78e39c08993e49db41db7f4fd74b3e869bf9505e2250547597f75492ddb7eedf505a08b2077cd7fbb713efbe6a
0d4ccae9f85e2997
A.e = 361b4120015ab2f4ab4d66e644a5b48ac293a6eedddd82915922d809eba60c15
Enter CP:
>>> 17BC32B67700986C2502F91E1582AF81B85F788E48D91FDE05CAE5C7F37619E4AA68A992B6E3E6EFA4986D6A818811CFF3E01A5788527
2D0F9551568C701
Decrypt msg:1337
C:\Users\kir\source\repos\CRYPTO_Lab4\Debug\CRYPTO_Lab4.exe (процесс 12252) завершил работу с кодом 0.
Чтобы автоматически закрывать консоль при остановке отладки, включите параметр "Сервис" ->"Параметры" ->"Отладка"
томатически закрыть консоль при остановке отладки".
Нажмите любую клавишу, чтобы закрыть это окно…





Висновок:

Метод пошуку простих чисел такий як узгодження тесту простих дільників та тесту Міллера-Рабіна з високою точністю та швидкістю шукають пари простих чисел.
За допомогою алгоритма шифрування RSA та протоколу обміну секретними ключами, ми успішно з’єднали двох абонентів А та Б чим продемонстрували працездатність алгоритму..