

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.

2637857232180935101662265407394689643029315089690421417383564582836792337817343 Faild!

115542625977379042590878856315180549839962152100662899283649192818556915257259 Faild!

71664424739994312686107436088077604585472013638346816293878536415844976760241 Faild!

4092366460447159676877705071654214536157842013168728613683553707228425325903 Faild!

49819466782007450771784962824202785007134057030354322111917694462961421967351 Faild!

11667744996744594066247762176629853592691726885827168662704468527364546426099 Faild!

39719197345919781608200318686361951965463320190990433749161505390177697250869 Faild!

67270899502177344236232032334196690962002369092156155234770233132065655143049 Faild!

93411193002430777656314876121600403718893878029242196041263023243426750178581503 Faild!

1494579088038892442501038017945606459502302048467875136660208371894828002857304063 Faild!

97948735113716855111748027544083264929942867048390664956163415860499447995256279138303 Faild!

25074876189111514908607495051285315822065373964388010228777834460287858686785607459405823 Faild!

6730985823967691739342851259109517138800133521941023286694642316039885237850855712602603854495743 Faild!

1806835248986303061317931418079237387093629134823124591070495042863062708010162913202684912468922690699263 Faild!

462549823740493583697390443028284771095969058514719895314046730972944053250601705779887337592044208819011583 Faild!

7400797179847897339158247088452556337535504936235518325024747695567104852009627292478197401472707341104185343 Faild!

485018643978511800019074881188826732136726851501130928948821864976685783581302934239851144902915348306603890704383 Faild!

31786181851775749326050091413590948717312530939978116559589989743112079512784269098342884632357460266621592581202509823

Faild!

130196200864873469239501174430068525946112126730150365428080597987787077684364366226812455454136157252082043212605480239103 Faild!

2184329784289369006100466935666936554599527510371106393265840657850269164319360794890337556644420403628146888699216064755179454463 Faild!

34949276548629904097607470970670984873592440165937702292253450525604306629109772718245400906310726458050350219187457036082871271423 Faild!

36646972606256150319052851480542298634812066539438292118801954138336061427925409037806889500735676306476604031434706949067632826304692223 Faild!

9381624987201574481677529979018828450511889034096202782413300259414031725548904713678563712188333134458010632047284978961314003534001209343 Faild!

150105999795225191706840479664301255208190224545539244518612804150624507608782475418857019395013330151328170112756559663381024056544019349503 Faild!

###################################################################################

########### My Keys! #############

p: 113178022654792066559390596765989047752590928794248404195619000520553065736129

q: 6758050899818874415454510332037710236847625320523094049933733304954653267816619169361690623

###################################################################################

########### My Keys! #############

p: 65297298368509143813610499043226203141187101005669912426468293797865546597789

q: 59345543671709257209767221007004536235567873355666967915245307226317098233075290757367070719

Signing ...

Decrypting:1337

Decrypt!

res = :1337

Signing done!

Encrypting [1337] ...

Ciphertext: 9f220dbd9b90bfeb541f298e0ce4ff85f23f5369ff3c31cf795d6d01f3388dd6e80c9abce5c3af5c16c4aca532eeaf5e9bcf7c3fa8b8c445c51e3a94fa500e77416b18b6b899

Encrypting [504c13119c9477851e18d03fcef0238d1d870d23eb3d7a345842bfcead63582e63b0011457fba29d4604761c4d571906acfa095a753a649aae168a69281c50e8041215b2641] ...

Ciphertext: 9b03954c4c084eb9f44636c6191bb77ecf3098e5ba97c3d09c6ba025b9f83a02f2401d52c7be37185e5c62a528b837ac65505623f8b88a54a81f68f660c7282583c2d963d3f0

B.e = 41e64354f3c712a95a3372aa4942ea29c0a6a8ae0710a31e53b3d4e694b9b90b

B.n = 33e2132143a316025ac79518b94a10bdbafe760d2ca9d6b748367fb6f18959164141263ef07876f614dc73d06cafd212f8d624184b3f130226dc7514d951f207cac3a4c2183f

Decrypting:9f220dbd9b90bfeb541f298e0ce4ff85f23f5369ff3c31cf795d6d01f3388dd6e80c9abce5c3af5c16c4aca532eeaf5e9bcf7c3fa8b8c445c51e3a94fa500e77416b18b6b899

Decrypt!

res = :9f220dbd9b90bfeb541f298e0ce4ff85f23f5369ff3c31cf795d6d01f3388dd6e80c9abce5c3af5c16c4aca532eeaf5e9bcf7c3fa8b8c445c51e3a94fa500e77416b18b6b899

Decrypting:9b03954c4c084eb9f44636c6191bb77ecf3098e5ba97c3d09c6ba025b9f83a02f2401d52c7be37185e5c62a528b837ac65505623f8b88a54a81f68f660c7282583c2d963d3f0

Decrypt!

res = :9b03954c4c084eb9f44636c6191bb77ecf3098e5ba97c3d09c6ba025b9f83a02f2401d52c7be37185e5c62a528b837ac65505623f8b88a54a81f68f660c7282583c2d963d3f0

Verifying ...

Encrypting [504c13119c9477851e18d03fcef0238d1d870d23eb3d7a345842bfcead63582e63b0011457fba29d4604761c4d571906acfa095a753a649aae168a69281c50e8041215b2641] ...

Ciphertext: 539 **// 1337 у хексі**

Verifying done!

The Connection between A and B is established!

Опис кроків протоколу конфіденційного розсилання ключів:

Абонент А(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

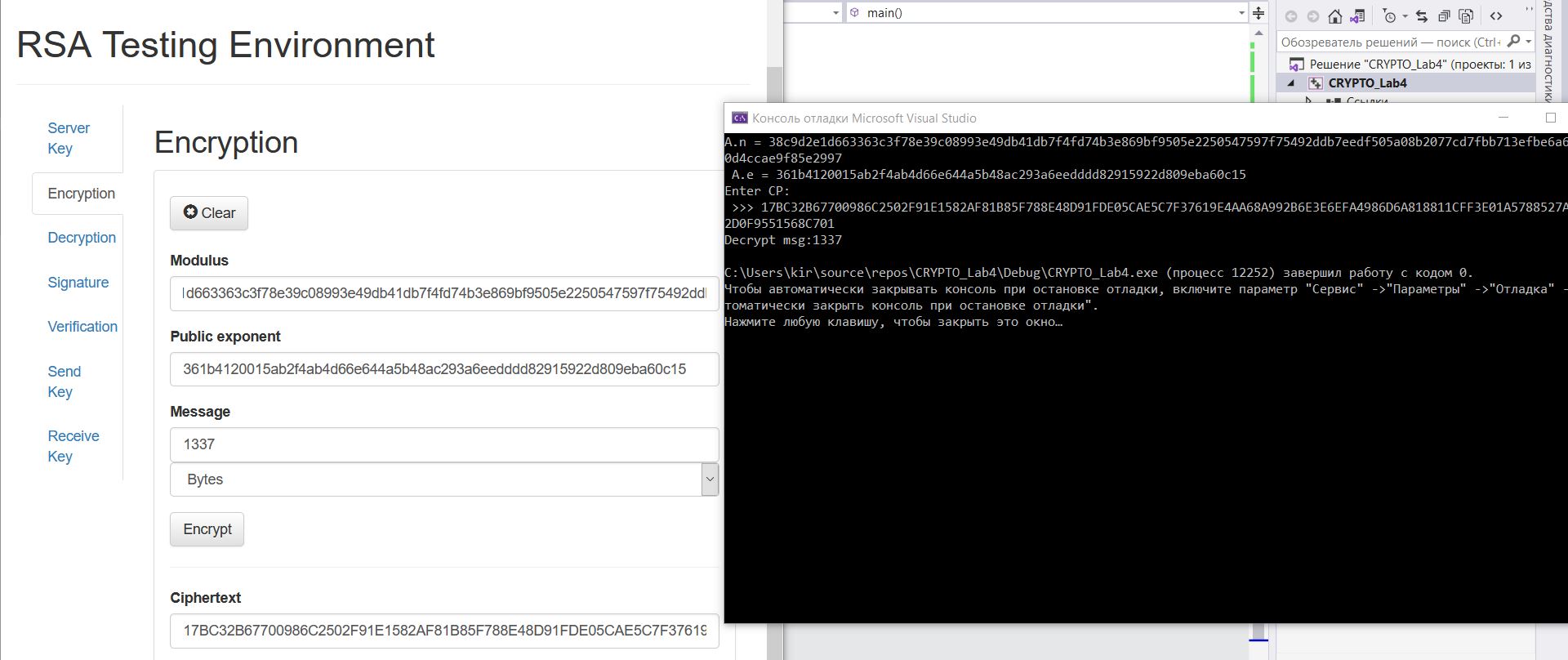
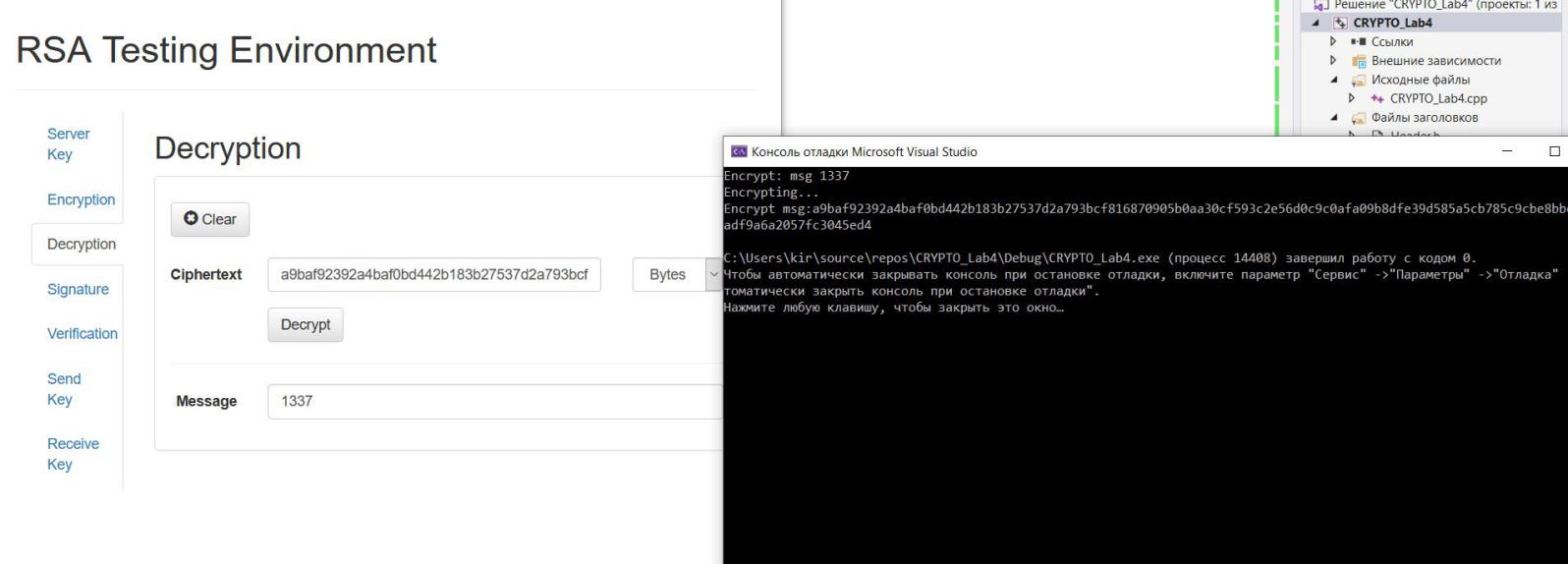
Абонент В за допомогою свого секретного ключа d1 знаходить (конфіденційність):

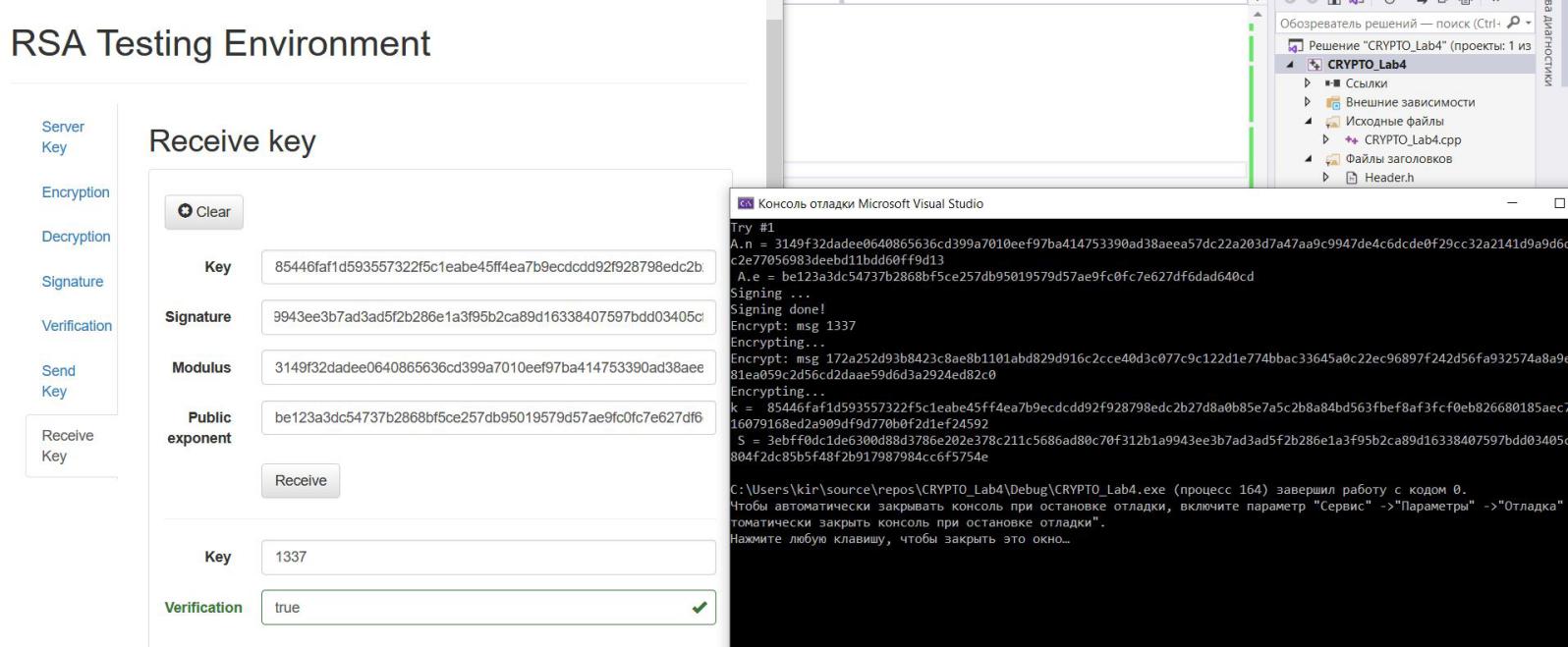
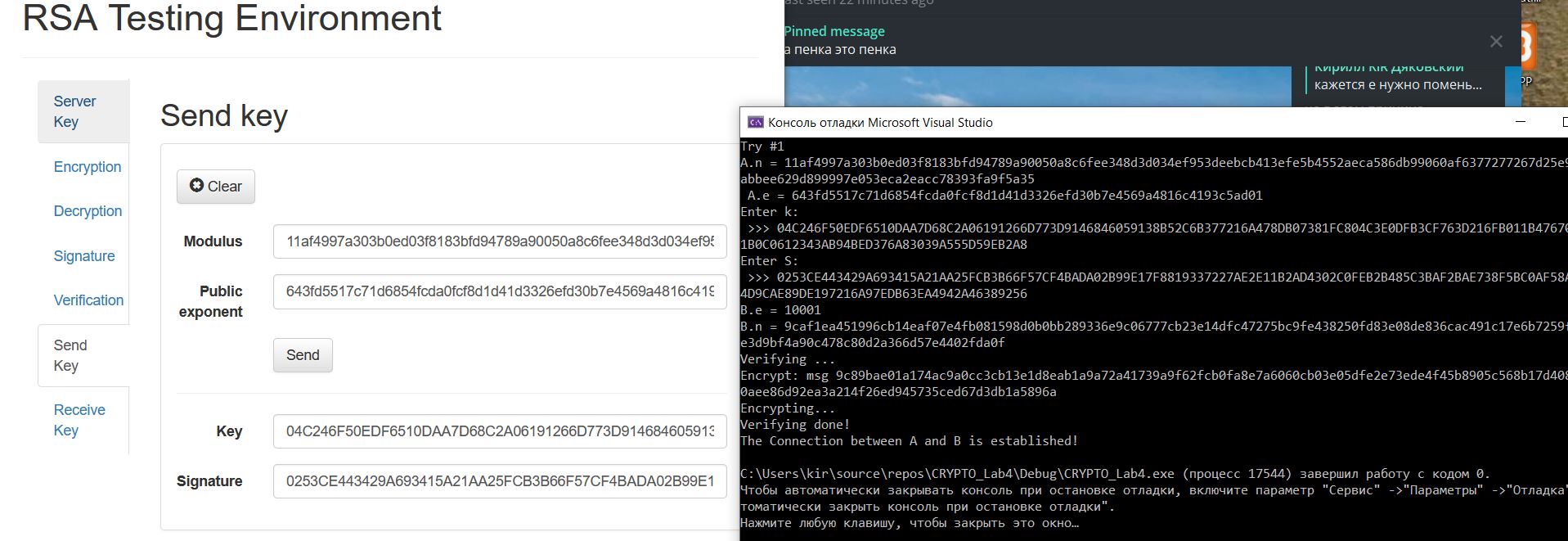
k = k1^d1 mod n1

S = S1^d1 mod n1

І за допомогою відкритого ключа е абонента А перевіряє підпис А (автентифікація):

k = S^e mod n





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..