МІНІСТЕРСТВО ОСВІТИ, НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

АСИМЕТРИЧНІ КРИПТОСИСТЕМИ ТА ПРОТОКОЛИ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Підготували:

студенти 4 курсу

групи ФІ-84

Ковальчук О.М.

Коломієць А.Ю.

Київ – 2021

АСИМЕТРИЧНІ КРИПТОСИСТЕМИ ТА ПРОТОКОЛИ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Вивчення криптосистеми RSA та алгоритму електронного підпису

Ознайомлення з методами генерації параметрів для асиметричних криптосистем

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

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 треба використовувати один з генераторів практикуму №1, що показав гарні статистичні властивості. В якості тесту перевірки на простоту рекомендовано використовувати тест Міллера-Рабіна із попередніми пробними діленнями.

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 **p*q <=p_1*q_1** ; **p** і **q** – прості числа для побудови ключів абонента **A**, **p_1** і **q_1** – абонента **B**.

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)** , **(e_1,n_1)** та секретні **d** і **d_1** .

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.

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** .

Кожна з наведених операцій повинна бути реалізована у вигляді окремої процедури, інтерфейс якої повинен приймати лише ті дані, які необхідні для її роботи;

наприклад, функція **Encrypt()**, яка шифрує повідомлення для абонента, повинна приймати на вхід повідомлення та відкритий ключ адресата (і тільки його), повертаючи в якості результату шифротекст. Відповідно, програмний код повинен містити сім високорівневих процедур:

GenerateKeyPair(), Encrypt(), Decrypt(), Sign(), Verify(), SendKey(),ReceiveKey().

Кожну операцію рекомендується перевіряти шляхом взаємодії із тестовим середовищем, розташованим за адресою:

http://asymcryptwebservice.appspot.com/?section=rsa.

Наприклад, для перевірки коректності операції шифрування необхідно:

a) зашифрувати власною реалізацією повідомлення для серверу та розшифрувати його на сервері;
b) зашифрувати на сервері повідомлення для вашої реалізації та розшифрувати його локально.

Хід роботи

*Програмна реалізація розміщується в відкритому доступі за посиланням на **GitLab**:*

https://gitlab.com/andrew.kolomiets/asymmetric-cryptography-2.git

Опис труднощів, що виникали, та шляхів їх розв'язання

Під час виконання комп'ютерного практикуму, було лише дві програмні проблеми з котрими стикнулися, та вирішили відповіно:

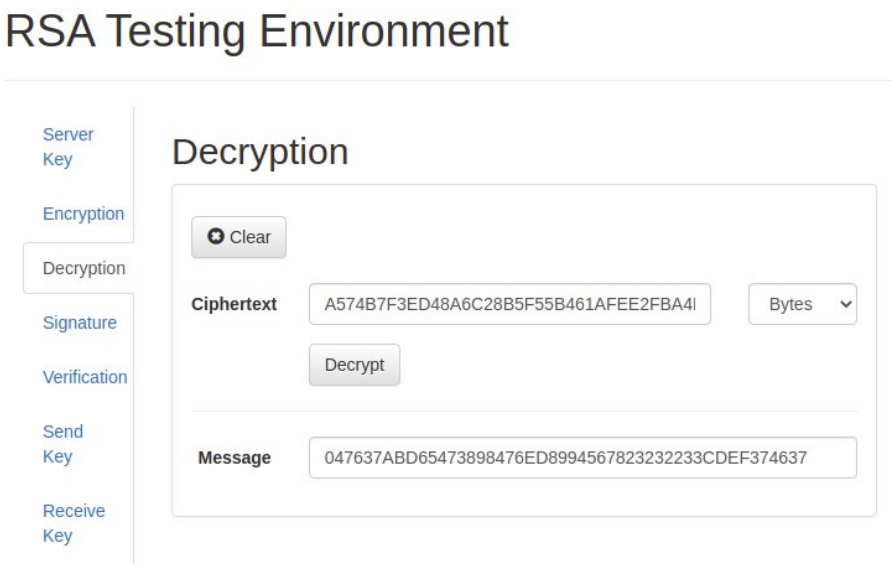
- Тест на простоту, а саме дуже багато необхідно додаткових функцій котрі працюватимуть швидко та правильно узгоджено на мові програмування **C++**, що змусило виправляти багато помилок при побудові програми.
- Організувати роботу протоколу розсилання секретних ключів. На перший обгляд проблеми не зрозуміло, як організувати програмно, а з іншого боку абстрактно. Вирішенням цієї програми полягало в створенні класів та використання інструментів **ООП**, де ми змогли обмежити видимість ключів, та за допомогою об'єктної моделі побудувати функції відправки, та отримання повідомлення. Зазначені функції при цьому приймали посилання на об'єкти **A** та **B**, таким чином функції відправки та отримання ключа могли взаємодіяти з об'єктами в зручному режимі, брати відповідні ключі, як приватні так і секретні.

Взаємодія з сайтом

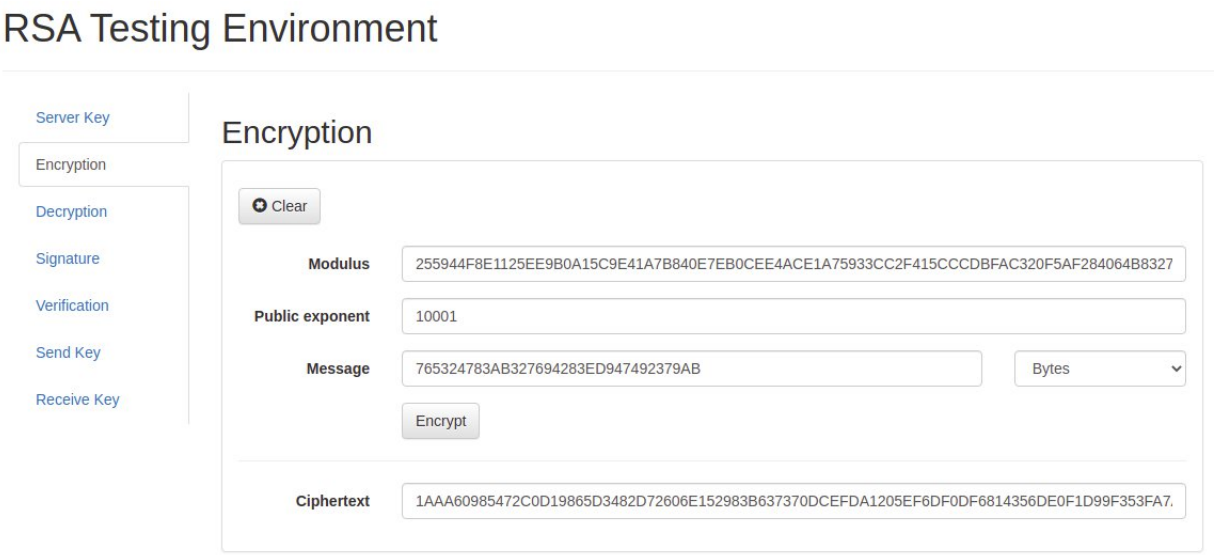
Шифрування в застосунку

```
Input other for encryption:

-moduls
B1A306ED93E01E92477CEE975A4F2C605EDA73A3186B40F9CC1DF234463F1127

-exponents
10001

-message:
47637ABD65473898476ED8994567823232233CDEF374637

- encryption message:

A574B7F3ED48A6C28B5F55B461AFEE2FBA4B5C3603C483B2360A0425530A45A7
```

Розшифрування на сайті



Шифрування на сайті



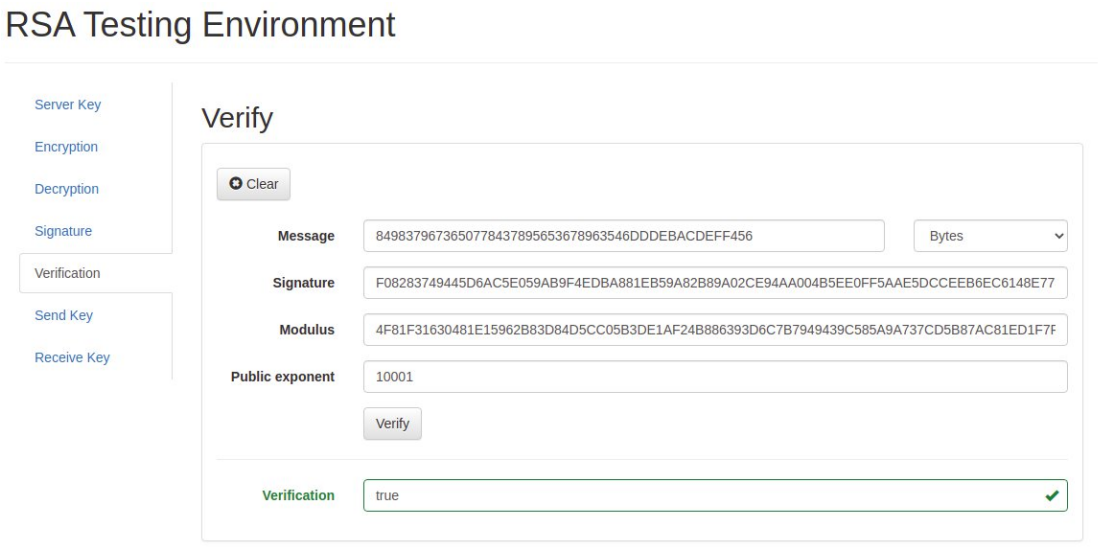
Розшифрування в застосунку

```
Input other for decryption:

-secrete keys
F6094D43F9ED7B331C50E241E761697AAA50D3AE353BE73203F092983FC41CDC4816BFBF43C6F85BC9289A226C7D9A0581C4F0CB10E6777338ADA14B27D90A1

-exponents
10001

-moduls
255944F8E1125EE9B0A15C9E41A7B840E7EB0CEE4ACE1A75933CC2F415CCCDBFAC320F5AF284064B83279DEAB7C4DC70E234E305D0171175A4B11C90DA87B0A3

-cryptogram:
1AAA60985472C0D19865D3482D72606E152983B637370DCEFDA1205EF6DF0DF6814356DE0F1D99F353FA7A35B5C55D92F2205AD7A989AF0D7420E58E03BE3B56

- decryption cryptogram:

765324783AB327694283ED947492379AB
```

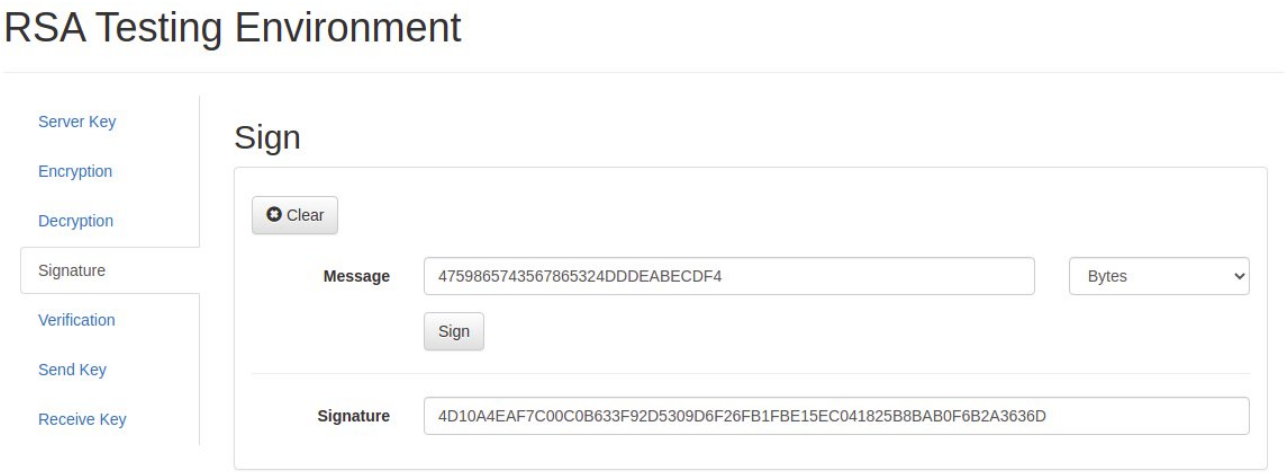
Цифровий підпис в застосунку

```
Input other for digital signature:

-secrete keys
49D9C0BB9979434875C6519EF6ACF2974DB17587BC4620A0E745017185F5912A23E1EA60BD298234148307C87E1467681621DAC42CF8978483F9627E42B5C01

-exponents
10001

-moduls
4F81F31630481E15962B83D84D5CC05B3DE1AF24B886393D6C7B7949439C585A9A737CD5B87AC81ED1F7F0FD5AE529DD8B5AB94593E0EC60F78819BFE65A6B9

-message:
84983796736507784378956536789635 46DDDEBACDEFF456

- digital signature:

F08283749445D6AC5E059AB9F4EDBA881EB59A82B89A02CE94AA004B5EE0FF5AAE5DCCEEB6EC6148E7750AF000E61147C3C3297C50E86819C25DF006960D8F
```

Перевірка цифрового підпису на сайті



Цифровий підпис на сайті



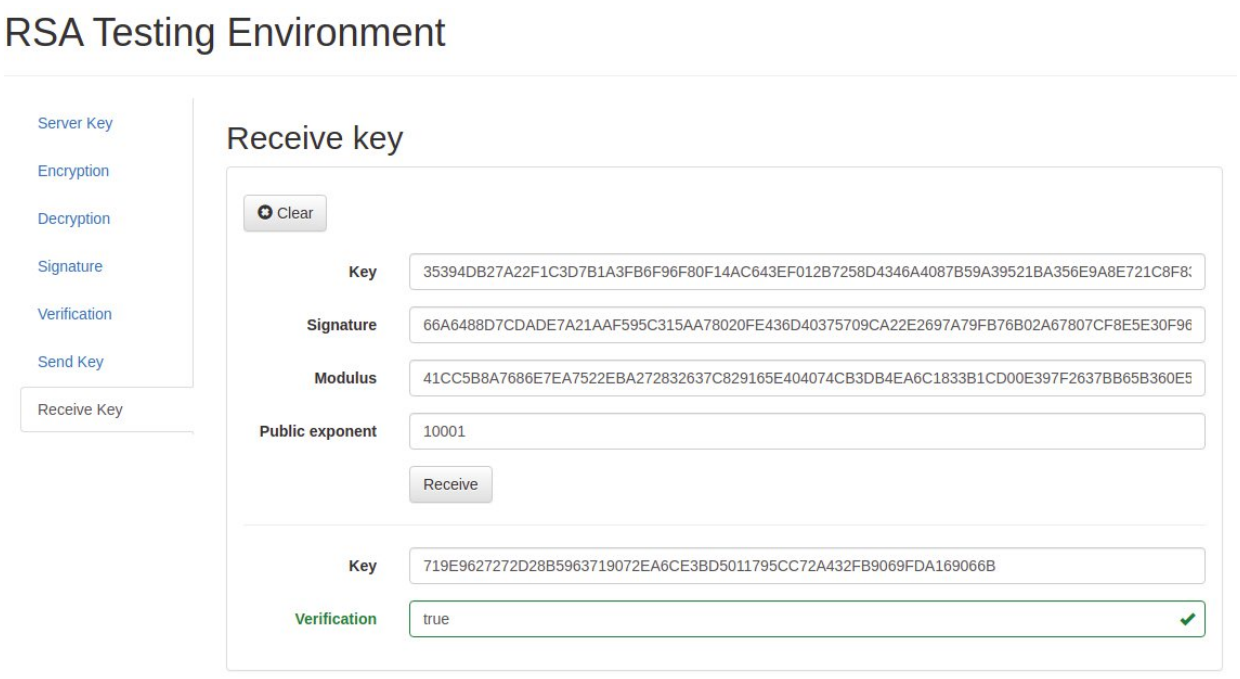
Перевірка цифрового підпису в застосунку

```
Input other for verification:

-moduls
B1A306ED93E01E92477CEE975A4F2C605EDA73A3186B40F9CC1DF234463F1127

-exponents
10001

-message:
475986574356786532 4DDDEABECDF4

-signature:
4D10A4EAF7C00C0B633F92D5309D6F26FB1FBE15EC041825B8BAB0F6B2A3636D

- verification:

Digital signature is real.

475986574356786532 4DDDEABECDF4
```

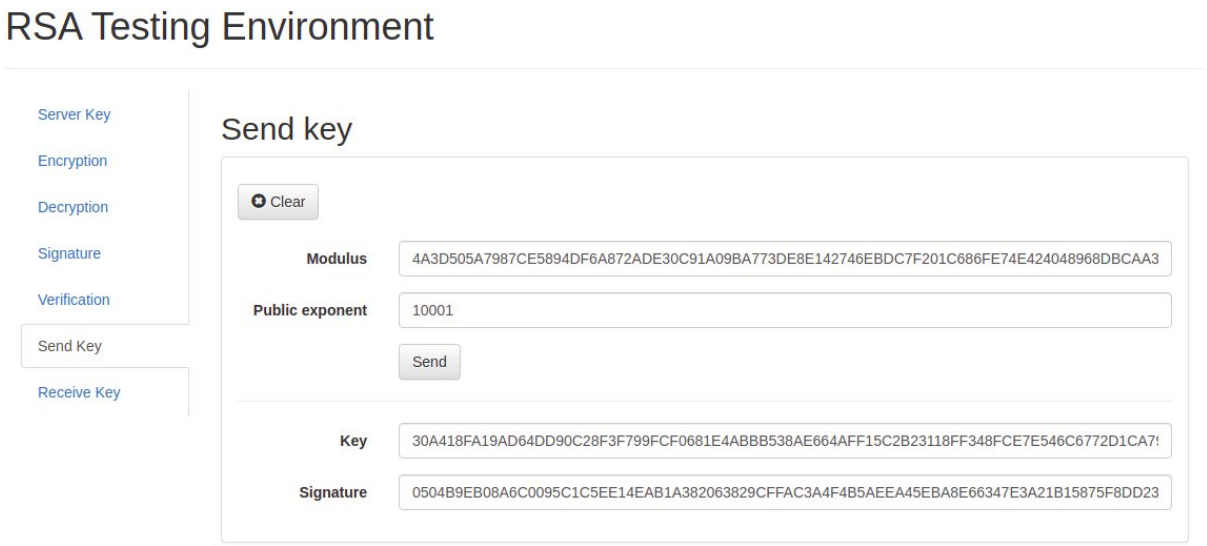
Надсилання ключа в застосунку

```
Input other for send key:

-moduls
A2DDCB579C7BC9FEEE959905EA3D665E0E8FC928B90120788C0E88FAAEF04EB3C51ED16DAEAF35C2021ADFC9F1B86EF9763F59224984C56B6BFC71FE611E645B

-exponents
10001

-key:

719E9627272D28B5963719072EA6CE3BD5011795CC72A432FB9069FDA169066B

Send keys:

-results procedure sending:

-key encrypt: 35394DB27A22F1C3D7B1A3FB6F96F80F14AC643EF012B7258D4346A4087B59A39521BA356E9A8E721C8F839FC293F34E3B39AD1787BD88937D592EDC14E0D44E

-signature encrypt: 66A6488D7CDADE7A21AAF595C315AA78020FE436D40375709CA22E2697A79FB76B02A67807CF8E5E30F96AADFDB58AEB151B66459D55F25D698EEA89567C529
```

Отримання ключа на сайті



Надсилання ключа на сайті



Отримання ключа в застосунку

```
Input other for receive key:

-moduls
B7410C4C58E89EB68B619BE67516667FC7B11EF6F8ED29303DE6C2EA07F20B0E17FAA9E8179CE7864046F3D8D2BD8275BC7015A2190F20EF7FA68CF27D7EB439

-exponents
10001

-key_encrypt:
30A418FA19AD64DD90C28F3F799FCF0681E4ABBB538AE664AFF15C2B23118FF348FCE7E546C6772D1CA79386EF356E7FEA3119CDB624ACB6715661BF1B94840C

-signature_encrypt:
0504B9EB08A6C0095C1C5EE14EAB1A382063829CFFAC3A4F4B5AEEA45EBA8E66347E3A21B15875F8DD235F302238304706E5622CF4C3060AB2593DCE51DCD9A2

Receive keys:
Digital signature is real.


-results procedure receiving:

-message decrypt: B52FE551E39013FD

-digital signature: 2249088BA9C3EDDE06CF96AF159F8C128A396909744472303AFCE87FEDECDB8C8877E3576B29F0651DBEA32C5F9095C86559D019EF2EC3F8A9A6332DC56FDCE9

-check signature with message decrypt: B52FE551E39013FD
```

Робота при виконанні протоколу розсилання секретних ключів на основній машині *з всіма параметрами та проміжними обчисленнями*

Значення вибраних чисел p, q, p_1 , q_1 із зазначенням кандидатів, що не пройшли тест перевірки простоти, і параметрів криптосистеми RSA для абонентів A і B

```
**************************************************************
Procedure of generation keys...

Generation secret keys:

-generation secret keys first pair:

        -generation prime number fixes size:
        85412926459013204123101273360117717876262904725623203823358729934817299819766
        80461577945760724108609709108760411631617709679335739674361349605326996655264
        11066305228040590244098215469993898680504138454084691766936964902847607775270 7
        96719278274248357740585171643606601650112150716545523234790678277867664596770
        59369779580528907266857744753140221478237276484373478305769459917597442715274
        64471986840970512941264758242046463037404016280003214987806331263286893739502
        57863183173634543544279497909505351987277741308891323701480482982937666675562
        41763818967914939306079918166335536198613455033859687569182256433173129342329
        49522656390837560746407899996515451062278680775322044619731554112260995158496
        25354904094699350056771529894628021533840578712574852053260481409931305335026
        37604877911359028554111073593589406014821711634676444731913533765551730649967
        29411788649010463566795720409627107034424307785675808345936028837527538744547
        30020559420083484793880227186956848114784669906147145237594296964468235822 04
        50529237160894960850207127428412522935792793028732901176849244917826231161385
        90694243268732540144305068908517691390720010416725705051168820046570911146 39
        64707195399469998995970369344023488806486997531017247640231803928982053960 03
        29274221811932712620690350709552103226164357239091663603610204692750884684283
        12616505559807469699287725867323137689102739175887039274790189560541437139887
        50077667855723603819119300323198081890957278571578657352400067348759791148594
        71650534178553877743019559760522282815332662817553283544899782280714426090056
        72073766723964981715108736185978484467231056121925487334614060819014514277139
```

88814805553414268787226957664537333509775397788991524881778996745463973532081

22539929385336448273176398281380731985416537940155279506717449067001244602 36

10642410047268192102419841619269769984647534924694841313357662348505274144 1753

57035183167500307072830706062270169770764948910548232759720454121368591567859

61257800107742532728025131547105867094171544879249776897142346828913202860224

62577863700154558872932437379683689945892708463257176624928234836687005411803

31653316292022653187772662956142806518310489959243782901000742276696753335534

88636377476589117344199950462418584643729896426026429053463597611602314988848

10647115352028937429565694233505889829312603956761155868834282106567364563834 3

88901850536097907582137524601974427903619590055095981048700367169897998338482

65602399473656979650504273008891067425868697639608537384945022252159591253917

14332222354579514442454043097137686178559894413561496840103397257632993360160

58963561914146884222946623899176779429501440731580073961142544162928724798331

13497449068149480154098143380082681623406974541291109872485911217108743726946

46005943653924528163245004304401287416685898518091713170890324251846219143246

18834715886479128594508292989783965150693028473209966524504046333110137594498

44138873400537649885145951750941867222222580916913069748131627177081534251163

21234393601803689431305041629177343245468207632445384117917144572658282746632

21534918074886916374213385901501735770545374735967102861135235014247020775935

25289821740410238295891352570137468434131716148978539916266042294984835863 32

79282349187550802962325872745812279459641462591492733592810190992926847561226

47822563757903909858316182770796074530797878445926333589226784185233990127 27

28730886397743067890907288047652454118043870292063035745398903544853475064114

90534909388555165921837796563783616634071289014797865429779923218149756459366

50374466560349508753135079910953022981703353589907984459729776506499569911763

26567757647349794126723243118068211212800941763068873517122507841818358707079

92460883268458004541778305646911232074060017962116515905106089725363292137038

73089475161620725128588421714545035176141697076792810603521168521258811409960

93827786446382614116953507204762555943154396973976672097801985470600238218135

85886201191804339578839090879819252901833735010430311545004645204437776638044

83012391475979667866612773995529781557690139994154375084273230055098879608782

83187898183536297208236788086965329026018668402096315562776830167547183326125

54944269292158764072885911109983048897222327172752882215324537173042684965077

10665914847077477900077361909643587277215516405946740275506103402604754410508 2

68243410165349803440229448060135923013722274696504056558487875500637741188257

40740740994831446703233216888352044664879231638008740328139138421874415454668

10320865981950071730506679137456130200925831651536155652477148729632230373107 3

10580315580671824949868874132172408485660702555757220222046380092930842842803 1

10103345602063825257981436602386232526575318681040292075466180645048491612701 0

30443593216745781739746082348491994376233447629174505763261181443049815421 2

76182793460674975926669416090579430373544000491903496445507714305291736453219

75300996655984761644038117098042616962454031600714838847453122338340717582488

54674823582025566865790966147665848796991165034220726681991374406473573822803

52038287004434794307694582489173401992716614936546372541164377818887009729421

22972250485364181456166845016210601781285646845636573306369535455899928192 89

80530682692697672113017065261516209666012783863529265899978441507901483198589

26032643813817770380727196524932613214976580393024890325496467885799106004325

57143254693038173347296434054752245343106375228140139668393798113243640119361

84080077554541755722788460080474668223954114524193387295383390641595217452784

63035189998165732169234102817551571044471624738354634409929208764244163482510

48503947166762162031598999632801225884399245104204827039579611842213064438305

28015944924149326939754564615263512388732653979720489420018054170651779805397

87031409924752498339620438124536390011812563707449040953162965057549483239634

53154848129618387689979923214228288491481600360470830140965749645168351208039

72175827843244575786513487307387995840098854277437052044520380970506630614094

92325191467068409694227912506640057408506787009538821582960019500545693038935

11411503508191685807371490088682968972082327254872598501081330135834263513 3

10140647409169262060497372875773710401048424918227142366271144421094996466252 4

69906548892847048319605950205988075813691334068507350989259007215990297415553

53282560931534152926992469269163895937266074032435562070874788782905697788887

44131535386188797779021068411582590372533211207134098938917536111313178679050

72176318442265740411110449405476798900482694407754384752645466416432723485753

49417349030365291193498325445630558133805988769421229354373398673815219979 47

40717389496410766666254344139040966237534257170890294433983313962042105215114

10207828667864893007041083795953401281456350655960898380982840776438868505489 7

66150318397262960275913199458406715085410780283654039840039087097640804765331

76083178755052496235663281304009066942928892281912751215390611403494525668162

46627588322541229703889381769121296309602130731995974977208157813071602170000

48116538806999634782020557835761075270949273658828114968942550834807367952504

93040683497004067900417815777522154911963879636289963819144086347839056687735

68313787574391207644970106006738289930460200359433183547205133446300915597098

71427281319034764046575696847633493509347480619052999038822248561951841439 60

741916628400064761041515804986556943346493303755401646841490623700860241535 6

841322249425525120145849968250630022819652434005762823145643147473924090634 15

109138560021915656794192510343975662625784176890230585006833164485672006923797

985000953665100458734683358943166712175142864988023925260188615103237177525

219742886538544776895166052562357121830635968066363997773427463999382865039 71

635136901769055222376317849461375646783428954309603835427191745366464229218 80

651302459485488846893784872346664934670530160143467410006780728822877277479 94

729886130781329156124123380750179365615444236180779807014047232144976845109 84

938632869164896304413924260091643068490445856684799222038921049957969170238 8

260328832613685708599034983381681470275140291197644836645031510172386673602 34

181023254617493919401833398720238435762042766286283280754500180699699362507 99

299797970838860926737486470897529044339971268982658693960425274682189993051 45

110834394942687209358032394705231050934166694872582746238287457716316709171081

887343699711069096614723247771508351417127962096724907381481644255342550385 71

791690231286814089567851557365203566701823313639814671503853856769415010337 1

700229166965099482769600027101154704417331208843194997066625721538282564702 69

720535351721323377442703010300088637989720031688962966875931076628475425547 1

103450949946108557582585312394358521397281019377308379384060205556356342403204

661175169326408958708797742494853841697387406430449690144382952306345273951 51

507522354647855078054760897235732346545765732451171751319409353737739998090 16

315348794226279619328120613489747599422083964053272554905090319539018848031 79

491441020164626547450048258524500769547886503853467103799713595934221902705 28

669190003676411256195477335068188093050061368192042863877525205301834528170 13

115011831275690072283755076896032427125254178802913674190962416552510171276582

242805644326961705333085065535492088019065637017434017910598695290527989416 17

-generation prime number fixes size:

514372685629773365754877706677947973204682858138551479847145463758203204200 77

808158702885919283859560006130740685414459545993178118318732606120761075893 28

231529357471235819164880097193979230523675815207666942918586539627391143241 62

368526513951529112685098275388030404018616910606176768030683125205129901960 20

971823483276406872252062112081916065872096388103814226314289271151659621275 14

225383366459351603830292165389057059102945630609348027475730953020045244639 29

927939478305624527837584616838202178203984436742719920898330250459020305481 23

386969970595625624637909373154161368365951460429451459697941595209094538234 06

821375235787337708137536489646801283087298307972790840717635339734344615571 06

906113244048389944015406363095299079529368028123604925450825576688496272569413930849856256246873933824786641132444736745898740650475893277501247400746199122455327764817700249767254497056696657087330824702870159675411849157565613053824719272076794538285255242993440461932408242105600731039163283432724598920879636259535671017540682635451547293734898105726669766129974005957037019181756155102223918180279486032829741736175274451610341560881703767831218555228977458306219694751148663218030144136418079334095633215681412156250382604740984137944828602702911335844940219251491792070346904183892674549644070419490469400781771587608716436336790056821624315358824450381150862738544908387764849211114148315679156404774998600638234982393482684259976823820118812111125923986966216553086813810271833328722622543238742127274879499870791228855566706031019900557643487426661135118871828901205372583400081669452514639153353505156730900842956529321043461567121114588538229766874817719330180512002880444114301210073750231043726015602946116762585038016261427191551240053244917472751478853501961261805628139695898723555311176903447984239795070545248882875652883777033577964990-generation secret keys second pair:-generation prime number fixes size:694924813579054548144365220147280943474527518293298977826363735131720516622102264984196710119751967342986725527893455595327948672463865224075284550948493549953751910714129200761155382492131921847384874915309290759964489364470307777467147336468000364111603463271147999435173707828582248739372709925026629114443787025758945756678009510766836229505026982279793614198293829854793399451546631741612553428209957203750973603986237324652926385731966667386523789576968766967736483602472069918853509355525048846007911924841237152596190396330907591375580391085786645571241838875975007558560740342260637599743859739778971852742615034387183684933938993280486180308155592478748596280939336061143878011342874020118656833443564946714941989250401731986266845491441685150831529139806277967749186677238733886113433190531932771872132719953021989724280202798901527578449523933702470478909596231571000352669371075802600619769420130223134768899404875069622088110132265661593103455174019464157797027667072215117499670152037270438261586993857052902212224382849514002518816867907251860431534995261206262735988055540238023329544773740895860806149881184047296861773476390678721005110354352242282715506505418906155875763460814479043574547089180-generation prime number fixes size:

100266316679787234887528874184072955411515153075998932569307620970859543828573

110153594432629613654324687353549888566419604485050232239597545943139757820433

108380723494273581031395794876164808079510351847825763719740910360219855604626

111619203509638538004421762662020662713167607974879233148334374952604011694137

301799008303290456956129469390629220349340538020370781083964039396239420657 30

842347246510882852568034577669858350071524236034257860859153968671525394310 60

287294496525988750263044861743765121029818040382964693663701330608891001688 92

554616353998173608773091250029837343025374686185918042236905902769165629509 75

372636908323946542591506516373465267658879482072529346089659685061759186043 66

766395056710392803238434803403591857604998970358916816421948881089238124010 02

551101655279811103887904298115539956770087104162268974412276385523114709644

176972455465110316437700876623947217031513272740552204820248307169680463671 15

898357864804814803994037510448172569094706245485399802081282373728714428008 54

664250167039837673271448671149566267319009073579406554612279446187953555551 72

879797300629944097488547731205224463936144757304592004521688720131833733154 32

269142275475818824719003900292402995914234727636600473601952269107820291714 47

665300869441206326100374481301660341805431440361240384675366948452967755876 96

198649587968883142338221337001509155449019402519668752044828342964656733528 12

975126334491239410276131214343140848715327213885212041402433987753855076175 44

730280856516031652658742389941936434392704364860033526466757845004866547134 88

786440138115435130298150274733965623644655261744655957166204342846664508917 66

147353492790961013421012037542314738969988991673612507886840349992616853934 75

570394930111054433148727962512094160515632304392275482156426853476346304561 61

323226215619072908695601658788204492238871284841288445617575580192465831391 7

239646491638482518731525679553105624814708168903468802651281239653061205376 8

694008324957936451216025768867959234184455277190584273717600655238682352166 25

355203889251035530579906667131825366543409710706467649822544749145741957978 37

694342702714538853407325187161799341046270349570542722584017359688653072734 81

799909443105494782169024401411043194576944957260475449909088539487264844470 31

318135943812483982875241403025548170970796997890871358136740403539653961732 69

209602413304124743581854772808290170992470067513597231700395170535065859346 09

532786346622816052843735861259074404905418247014575683906186777792171940229 05

896093552836630373281350919721526354242370408073206036232517068095993347849 21

578754343800409623995976045960344585677500346356003602356589719274970911214 95

868204269321858390669705873879668490632773662746749461649235219576358898864 0

953730696290127276781649475522893156265657110979179224778682061747476529049 31

463058935523717073192835843913000375988142889033299368759859198035915219027 2

641307967791486224554556214852789958264502090206239223231515506780766490511 46

883316562610344837024035860601385978745018084076451515098520236678001137166 1

367671253039938018187512461098771998127997800515941876018371101649244295265 58

900789755027838658827800247514386528538515655631062415330349492033768724244 39

865015321607570267639336508236886668249767402514952427755624251743193521248 56

825454189751210996992423783810736918310978721506224792354934959716964626234 71

102455408600096362428203212369333421648032265546007019699831044457584667658 142

710680902168089307879214138450723561845210020854182540573465652810683382878 44

801855800124631115629682473951684693239291724579227867201705358741322198036 19

104427930266535547677182607249681624869031749432985599953550514049609704705 429

192388230275455730414201148934833031627201550287276308415450982187455164598 90

831546965292138919520639504251719394400289172341866244801872027045164414328 66

669051237943705592149905338210716952861615291613098292080129422062097377284 28

298235944107806641449383393311301818976188191463286633902465772732993992965 27

229222507041818126779889990528336251457926043735392535034572362759619753064 83

461610194032531491547795041855150440655446043324261497147600346287074882676 36

372941089673229266280991147502818339319249128258234707046758095770440164569 98

496894017503598777066308903974336402826998341216018863992935561320734628850 33

300557981246238484522366494771357987425928791230931065892658076571101355507 5

725503313602261555029891134473668406452962083252751094648601626374952261365 53

692401348320328547483166691719513650385080886241053474897541037347816486170 31

454858197971877792095076508998076389695083040610325407567585621174451576098 27

827023840775881090161319901306860696412144747113069233761032009287782192479 76

105478145167993514486637405693308716164951255083636372796317737617472969307 156

772224710378187985724064440882180553318064880915472698151768662739534397467 25

976398708840723007494395800442501785569188255134753021679708233480470400826 39

948709708032421897508133228545679039000236267862613947396203524851724093430 2

775827237576119729586627205757248950153886961402093424585413191239381275381 58

232761011304193830305225778481246253287086797902283059015197015449275365827 90

618812921092584342707989640775911072676255331043925538137134025781688180092 88

209436308986829146697611431538471949002744375301294734789845394233267132723 03

878086440805170017888152336692089705032562018780049226221524667885234785502 86

303212941304959137986624426708860508141794680044195409817721416344958307657 74

487030842945183554970996418225936973300679500708102133719932599295951074686 66

102402562446991664393461901322157800385223625081025393283737669489904151443 278

875949807930732065126322809617965689062604272127773537357406454483453508784 94

948793275344497027676670790458517028552287719435215418842411396053716236032 97

675189974917288643806717657018209860292453405542892381842440490405839501809 72

416496472367713710579333119022915130569475580189001136218626191057562707142 4

659287840830149460664964692938820201632137195610182353619752741053384344886 2

197649332254311951238312397787011174393036688683789356919773403357206103598 52

151182879007791670473379479814527686125235120802105972242640263328464380397 80

147302231363513373011215192230902480553773709444845011831311122416645528082 32

895482643551826973932508080894823367639706160960399143391314434617701235391 49

113234912419888958829833220627080919846394112934587628411457800933582738300 694

232439610750946572479530358148951741548891985080383389860498397799092382346 81

439161186355134832662461491627121635617836921056995774163884260172607044133 02

656133793614828364853748983605504365445120254904576851329218456724963093103 87

967810698823280732579656278690305563467781923416107510433388729847703103716 96

450256439485611642724165846573807700266775744255607571162043795497731720181 00

663686608460326723393839496762778660119507980191852280599354079952123394787 71

565791666447570954987645070122900472426591463350714931284478229815965376912 11

435790711945206960006731963562252399714715500138649987638624272269060051666 15

111650527538205287549361223915599027603403976462989582749267734452320750109 170

345243958291471815921390881634412948918244773551467485668456382325928330133 616

707334227602816901026691833472119005887716915032596910705069933085986153887 32

320701399056401135245499852155412610404063413735048689663137964419692871670 70

107823477261353622643160311083371813443090450990910784230364918652570225073 063

914099861054569756771901572605094585214983014297348087387333135778632174322 12

711113798881593710295363923023241840428095903180850322016426775997836593966 18

623189629100569646556174027599307983877599120438531997844776250079485391506 71

323246184333335052268444813280196354753403029623873474983954210244848432167 74

835000954389952902826137353478955590961507355706230053003499802144763393735 95

195761948153073019329278572427502788635869523409027879252274906487932246692 00

116681978777197179839611358356212256620953967093145772746619532744763231485

692043041929402019230895963283466096258235284448964871865200633252465522256 83

575292089905355633660495085279343587331806780276162923369271897708018961242 68

100727533567737149685446222082973843593872689884193540574179809143468228042 595

478930655410870971949342056182873583837553931853057275150112397081580596869 19

109342298450823194974711494600662466681861420143312475705365058125494931754 766

254856601175216949056577076709771131001148036333616299458351114030121371355 9

1108810339671874193875239088242120996752199567591920296948391560225355903087957232481696442377794038887140221870845535913549010135191232903457743023348499668310404710299604282058283313897935520455908609017209008183114383025371554981113378974263869695835357222474668423670233582477115880394383453924844617582134243904235490257374640182066931255687899904061452016118085162338585862149348957373464018206693125568789990406145201611808516233858586214934892737464018206693125568789990406145201611808516233858586214934891-generation prime number fixes size:2144854706531791782826966690688301534300857285257185733090487140799232987137139410967689764579222040243579808968561696762988205125959532072425130395634661934962372644964599837783182896965745612497480198814919329106547852402246501548508372621346865626469325570533645877442625582524403031532586137142382047246785148324504508948303599451882960452901065083371196480525958535015724301483481918968018324465067846005225468965936697615787681723645628129407821099644785157435880094719763755094989191199022875220442266632453928605662166716044125793566630634328770319411987729303987697217217516871772774660006748340980216567453087624134022621003374720403755169199019054089771879401603182355664916512449635172190241751757729054330663541856413690762874728322482701870265933761136242841963306521084948193078469421931385081717566320468006829738220950049268442235602138672154358082799654733023725976670612052320728663653034100216310314943532691768700439580955824804765781340989342900210605726544085838315254967519284452491446471059793524766401576826724427780829699051733039139588111539542831841770741585523526164675214440884829502363983292717388705139508381390908429542638838811543798563841227181754718513754223839592896235327820198702985751002300415266139026046155406300484844818211309439706439112926127476452694679467159227913238218587827837605683148241690471955312346981264536359554259047446683419119245947054941950928420848739404513889251623300345188820453694625129874635092925178690990921960530829935959690026098593669849360862735502742182260123317444654751972878423540725978391475161997405495497088875461161022039903827964250466427105851304854432111356531684525507770879278842900520444704631186544441777646228760308585656446984703353393326216178835701452655487679127834525025007073391517116914009590818868251519132078369477331442501033232670960752251548786039591158760306794474168032978968733433826504058558360165068692420098619212513234745688728458342611809405127469202936793505128585660190429518961129413012595467391-prime number fixes size:

14671073820566805021251090720900993241974004286097457892797079377396216461988

46790308612253289199919074644456051031933119723882047689425001558942923003610

11963322405466161993343890362614732694585854516463450328245810060801734140197

10235390016760988333893644139724331151520748272413066943378338610443400476524 3

55658159670014184204057417658181309778791409602997590146100702451681845128892

74831810764277843625887686544984787195012894842707921276499070808415615735 14

74316241759145496268376620827165504885730801232138399021041785523307170545694

80518231631899555819938350478693230032730774092213279835036080000926598124 76

11895560320710027905796107577841381967870709806621527800497236631934689076929

29581202542184594944054813853998705837903263236752079132690036558402711834883

65779198313876329637361328704614440168582710642894207945032321658230173792241

62669018607378771668533822656727301970058962997070088651280372344316976010168

76020480111258490567928726089461832677909715190046975534106923257298380839807

10504918971619854862080067791085271489369975805217673834163949691135083782998 7

44479955424691619043400412971550880614859149599150548233917184628246336135058

56490897305630113586982932874603415373295385406676526610220933739908737427357

11321031439566391721435954702721197645488089562117762791937547932604701637176 8

57932307300907325417237410323682951690511568764093880599971299046055060002 53

55449319156311007019744841371498876213796829150438219725429533593452639552403

94296032018451436918501816845443618122521510579102700315962836424512279795745

94900668331505572582399729421509917433282771058548944346500190762011302752899

37841003076741702652037412604335188688945069596159859834604144001448611257859

17499422903058049343606498753861504803111820595324822980872630084307079377491

31830783085310663322543151528778602750772705361572832449426541316360848551714

10281484617129482802597548470559309065161569504435613321521152189215442218865 9

10303066303779632175114024000129033630313628231222734194193046405335347123645 3

89794894950988641718187889756707019876431361015345907445099634157041421475698

23575274245466251302490127784100551386917527578388140924837077878507275898517

96450383424409066524497389061860331590475083008751848882512210523914467160565

10975328515876598030182787725511251730882153734295604057784309161323797530696 7

95175368031987115917180455152187031247142768096198609098243024147481589215081

72472868025050969252756185553470480933270077016518379164766958155268184034568

32347678140864247472499457275839432198903424452291098945929400575171267542981

76580802698804563194070540708475043614930567266686594807640245084583967958061

10228200632595478339764002549040887947643842816830660032148951466652116108700 4

36129036030511402207942434230054063595853766170792948712396906511225547320232

343034822366226697347262099731613374753771156875068012790476200247229515321 78

103562322844008844204092251018092183455714617496448708816545388392859368292847

436430159136302082418195390380136277472743754632699886144746867885231187291 39

338982250580771238486237565027413613382431996312063273579923153707701811566 47

530366568061972634319420340983022141150579053157729052618810299408879183610 16

624936688368945746107072525421503532310531956517100873286911601858596236099 12

967488834141178360779092895589706510509218517264470590472865386274157017303 72

123047508117462551027970482171546939867961991446048689961634461039564671212 16

657608027558169105059648297903065223777837745850460953166767198884905174954 16

111964364600221065776307819498474921030032465970400809988912603427119842312934

157536363934851821821524641825048542450368644635878498348231835541244671665 34

241094038782575137354328018637403238918748361472619624306292690866123130202 48

310722668662538028601326734297885503652516103905098372238030895774038595642 35

766595280639725216491881424509398685524021220440695348276426294037468938998 9

108555279526815991225515739053540591299402540142899599596484127016370606248054

335693174638042677345058539960297206405605390899298882666208877243314894487 4

107328665087996719824045994475474319930599316418711412024846798177353117342531

-also inverted secret element:

805373028938027070296809376629884312344079075470162086022520062728849421118260528601186194305587 8
692004463417112394965906345534994553048211324581632779 85

449459838265349481832674335074906847580924586947719304092412272667637632321753256363855565805686 0
435255603131056148284579638823208111085073608693500781153

Generation public keys:

-generation public key first:

65537

195611059546794204150917229797252819101263426487373578296178695293557441766409477270190002966684 8
821234504128107566948519721051030834001211813212467998883

-generation public key second:

65537

455492576356464596497053888227808843030061616149819543093358844482193439042999144800526754730223 7
078586402459023074271175474672705587151397008833999280659

****

****

In hex representation all generated keys, which we will be using:

- first user:

  - secrete keys:

    35AE4FFD5BF3CB6C650D9F91A94E0C7EF6D007A70AF676FC74791169476279B1

    B21CEFD2ED48D6D31FE1F090C8297C5488DC4D6DAA117749C51D522C26DCD093

F6094D43F9ED7B331C50E241E761697AAA50D3AE353BE73203F092983FC41CDC4816BFBF43C6F85BC9289A226C7D9A0581C4F0CB10E6777338ADA14B27D90A1

  - public keys:

    10001

255944F8E1125EE9B0A15C9E41A7B840E7EB0CEE4ACE1A75933CC2F415CCCDBFAC320F5AF284064B83279DEAB7C4DC70E234E305D0171175A4B11C90DA87B0A3

- second user:

  - secrete keys:

    5DD3A5915225982A549FE8E67031C8B468E480D2EB4BA2327F040577B00ED0F1

    ED49DF26E50994AAC276FF4BE84BB0C29D0B80126FBC8D7989765A2EDFCA1B43

55D123A6A5CCF9D451430CB01DB250B9D1E74ECCCD84C64BD854EEAD9E88ADA53AD72D7AE59AB975C083F151D08B5EB69B87D921E40682B906F05733C012A261

  - public keys:

    10001

56F8036B5E133AC147AD1D3D309E15D0021838BC41E4BD7E61A57A7037416EC96343B66484CFB28A661B359A4144011650A88474A67D23815DA326E571141A13

****

Чисельні значення прикладів ВТ, ШТ, цифрового підпису для A і B

Input message:

9435647D4CC5F8303A0B94F65FDBB2BEB6C72A34300DE4DCECF355AE5DD241B5

- encryption message:

**24C9B91E1D6F9CD9BBE12CE0CCEBE510908D11455AE06FA32A0C8D3BEF52F538FAE11E26096772E8870BCF061A90C4E10
36584C2CBCAE0FCCCB1581E1B846A08**

- decryption cryptogram:

9435647D4CC5F8303A0B94F65FDBB2BEB6C72A34300DE4DCECF355AE5DD241B5

- digital signature of message:

**201DB0B6459B9E965A2FD562CF341BDC76FB52548462509DC3108EECBD7EF90DA3B50CB87E0EC8DB60A980489FAD6BEA1
FF072A8BF01C498982B5481A0E438**

- check digital signature of message:

Digital signature is real.

9435647D4CC5F8303A0B94F65FDBB2BEB6C72A34300DE4DCECF355AE5DD241B5

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

Input secret keys which we want to send using protocol sending:

9435647D4CC5F8303A0B94F65FDBB2BEB6C72A34300DE4DCECF355AE5DD241B5

Send keys:

-encryption key parameters:

9435647D4CC5F8303A0B94F65FDBB2BEB6C72A34300DE4DCECF355AE5DD241B5

10001

56F8036B5E133AC147AD1D3D309E15D0021838BC41E4BD7E61A57A7037416EC96343B66484CFB28A661B359A4144011650A88474A67D23815DA326E571141A13

-digital signature parameters:

9435647D4CC5F8303A0B94F65FDBB2BEB6C72A34300DE4DCECF355AE5DD241B5

10001

255944F8E1125EE9B0A15C9E41A7B840E7EB0CEE4ACE1A75933CC2F415CCCDBFAC320F5AF284064B83279DEAB7C4DC70E234E305D0171175A4B11C90DA87B0A3

-encryption digital signature parameters:

201DB0B6459B9E965A2FD562CF341BDC76FB52548462509DC3108EECBD7EF90DA3B50CB87E0EC8DB60A980489FAD6BEA1FF072A8BF01C498982B5481A0E438

10001

56F8036B5E133AC147AD1D3D309E15D0021838BC41E4BD7E61A57A7037416EC96343B66484CFB28A661B359A4144011650A88474A67D23815DA326E571141A13

-results procedure sending:

-message encrypt:
**207FD3A9EA55FEF6CE59A3C3D136504C98FB422AB301AC7DD4D6D9C501D2CDB9DFB9955DBC53F05FC5794CBF2B72E46E3
5763C187A91F4AF07E7C45CD19B3079**

-digital signature:
**201DB0B6459B9E965A2FD562CF341BDC76FB52548462509DC3108EECBD7EF90DA3B50CB87E0EC8DB60A980489FAD6BEA1
FF072A8BF01C498982B5481A0E438**

-signature encrypt:
**2E72180D975F0CEDD5F0D6455FBF799D95B59647806B48567F47BA2008B638CBE2BBA54D7B92BCF35F5DF3F38C613EA20
D22E6C47D8FF5644666126BBD0EB42**

Receive keys:

-decryption key parameters:

**207FD3A9EA55FEF6CE59A3C3D136504C98FB422AB301AC7DD4D6D9C501D2CDB9DFB9955DBC53F05FC5794CBF2B72E46E3
5763C187A91F4AF07E7C45CD19B3079**

**55D123A6A5CCF9D451430CB01DB250B9D1E74ECCCD84C64BD854EEAD9E88ADA53AD72D7AE59AB975C083F151D08B5EB69
B87D921E40682B906F05733C012A261**

**56F8036B5E133AC147AD1D3D309E15D0021838BC41E4BD7E61A57A7037416EC96343B66484CFB28A661B359A414401165
0A88474A67D23815DA326E571141A13**

-decryption digital signature parameters:

**2E72180D975F0CEDD5F0D6455FBF799D95B59647806B48567F47BA2008B638CBE2BBA54D7B92BCF35F5DF3F38C613EA20
D22E6C47D8FF5644666126BBD0EB42**

**55D123A6A5CCF9D451430CB01DB250B9D1E74ECCCD84C64BD854EEAD9E88ADA53AD72D7AE59AB975C083F151D08B5EB69
B87D921E40682B906F05733C012A261**

**56F8036B5E133AC147AD1D3D309E15D0021838BC41E4BD7E61A57A7037416EC96343B66484CFB28A661B359A414401165
0A88474A67D23815DA326E571141A13**

-check digital signature parameters:

Digital signature is real.

201DB0B6459B9E965A2FD562CF341BDC76FB52548462509DC3108EECBD7EF90DA3B50CB87E0EC8DB60A980489FAD6BEA1FF072A8BF01C498982B5481A0E438

10001

255944F8E1125EE9B0A15C9E41A7B840E7EB0CEE4ACE1A75933CC2F415CCCDBFAC320F5AF284064B83279DEAB7C4DC70E234E305D0171175A4B11C90DA87B0A3

9435647D4CC5F8303A0B94F65FDBB2BEB6C72A34300DE4DCECF355AE5DD241B5

-results procedure receiving:

-message decrypt: 9435647D4CC5F8303A0B94F65FDBB2BEB6C72A34300DE4DCECF355AE5DD241B5

-digital signature:
201DB0B6459B9E965A2FD562CF341BDC76FB52548462509DC3108EECBD7EF90DA3B50CB87E0EC8DB60A980489FAD6BEA1FF072A8BF01C498982B5481A0E438

-check signature with message decrypt:
9435647D4CC5F8303A0B94F65FDBB2BEB6C72A34300DE4DCECF355AE5DD241B5

Висновки

Під час виконання комп’ютерного практикому, було прийнято рішення використовувати генератор випадкових чисел та тест Міллера-Рабіна для пошуку простих чисел, що видавав генератор випадкових чисел. Найкращим генератором для пошуку простоти виявився **l20_generator**, він має статистичні властивості, котрі є прийнятними на практиці, та виявився досить швидким, тому всі процедури відбуваються миттєво. Сама реалізація криптосистеми **RSA** має багато винятків, що враховані при програмній реалізації. Але слід зазначити, що тут не повний стандарт **RSA,** бо ми не використовували попереднього шифрування повідомлення, та геш-функції. Найскладніший процес в реалізації-це протокол узгодженого надсилання секретних ключів, що виник в даній роботі.