



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

АСИМЕТРИЧНІ КРИПТОСИСТЕМИ ТА ПРОТОКОЛИ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

Підготували:
студенти 4 курсу
групи ФІ-84
Ковальчук О.М.
Коломієць А.Ю.

Криптосистема Рабіна

Атака на протокол доведення знання без розголошення

Мета лабораторної роботи

Ознайомлення із **криптосистемою Рабіна** та особливостям її реалізації.
Ознайомлення з криптографічними протоколами взагалі та протоколами доведення знання без розголошення зокрема. Ознайомлення із перевагами, недоліками та особливостями реалізації різних криптографічних протоколів. Аналіз наведеного протоколу; реалізація атаки на цей протокол.

Постановка задачі

Комп'ютерний практикум включає в себе два завдання: реалізацію розширеної криптосистеми Рабіна та реалізацію атаки на описаний протокол доведення із нульовим розголошенням.

Реалізація криптосистеми Рабіна виконується таким саме чином, як і реалізації криптосистеми **RSA** у комп'ютерному практикумі №2. Основні операції (генерування ключів, шифрування/розшифрування, постановка/перевірка підпису) необхідно оформлювати високорівневими процедурами **GenerateKeyPair()**, **Encrypt()**, **Decrypt()**, **Sign()**, **Verify()**.

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

<https://asym-crypt-study.herokuapp.com/?section=rabin>

Наприклад, для перевірки коректності операції шифрування необхідно:

- а) зашифрувати власною реалізацією повідомлення для серверу та розшифрувати його на сервері;
- б) зашифрувати на сервері повідомлення для вашої реалізації та розшифрувати його локально.

Для проведення атаки на протокол доведення із нульовим розголошенням також необхідно користуватись тестовим середовищем.

За адресою:

<http://asymcryptwebservice.appspot.com/?section=znp>

проживає сервер, який генерує ключі **RSA** довжиною **2048 біт** та користується описаним протоколом, щоб довести будь-кому своє знання розкладу модуля на прості множники.

Кроки взаємодії з сайтом під час проведення атаки:

1. Реалізуйте допоміжне програмне забезпечення для проведення сценарію атаки.
2. Згенеруйте на сервері ключі для аналізу. Сервер поверне вам значення модуля n (це значення буде існувати доти, доки ви не завершите сесію зв'язку).
3. Користуючись формою введення, надсилайте серверу випадкові t , поки атака не завершиться успіхом. Зафіксуйте, з якої спроби вам вдалось зламати ключ.
4. Продемонструйте викладачеві вашу перемогу над бездушною машинерією.

Хід роботи

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

Під час виконання лабораторної роботи, були труднощі в реалізації форматування повідомлення, не досить зрозуміло, як форматується і розформатовується повідомлення. Вирішенням цього було накладання маски, та зняття з повідомлення. Також були помилки при написанні коду в алгоритмі розшифрування, що пов'язано з обчисленням символу Якобі, для цього тестувалася функція на тридцять значень згенеровані довільним чином, та знаходилися місця в коді де символ Якобі обчислювався не досить коректно. Помилки котрі були в методичних рекомендаціях відшукувалися в іноземних джерелах.

Значення модуля n , згенероване сервером

Rabin Testing Environment

The screenshot shows a web interface for a Rabin Testing Environment. On the left is a sidebar with navigation links: 'Server Key' (selected), 'Encryption', 'Decryption', 'Signature', and 'Verification'. The main content area is titled 'Get server key' and contains a 'Clear' button, a 'Key size' input field set to '512', and a 'Get key' button. Below these, the 'Modulus' is displayed as a long hexadecimal string: '85920944EAB0065197FDA61DD2C31C2CB48A2066ED4D8119F76F0BA6022B59626A57714E71C198C16E2CA'. The 'B' value is also shown as a hexadecimal string: '1A2C6AE536255B38B1D2B418B87D92EE6D0FDD0FB1DC02A78648F81773AA01A85CD66EAF1F594585D168'.

Чисельні значення прикладів відкритого тексту, шифротексту, цифрового підпису у схемі Рабіна для A і B

Шифрування

- input other for encryption:

-moduls:

85920944EAB0065197FDA61DD2C31C2CB48A2066ED4D8119F76F0BA6022B59626A57714E71C198C16E2CACB902
776DE285BF613B9C0C4F4740AD10F3C8AC9B41

-constant:

1A2C6AE536255B38B1D2B418B87D92EE6D0FDD0FB1DC02A78648F81773AA01A85CD66EAF1F594585D1684F7F2F
EB384BEB2825F566A1BBDCBBC4A7EB86992631

-message:

472424242662534598245792456245264562164126185246342365481354294523846184527642342

- encryption message:

- ciphertext:

5A36D5DDBB14A6D4DF4502362DB8E2E4E69552DA6028BB1AE5DB768415794E8B031BCA351FA01F6D6FE574596F
C2ECC8B78A7028EF3F50508F4F6CB3AA6ACA7E

- parity:

1

- jacoby symbol:

1

Взаємодія із сайтом

Rabin Testing Environment

Server Key

Encryption

Decryption

Signature

Verification

Decryption

Clear

Ciphertext

5A36D5DDBB14A6D4DF4502362DB8E2E4E69552DA6028BB1AE5DB768415794

Bytes

Parity

1

Jacobi Symbol

1

Decrypt

Message

0472424242662534598245792456245264562164126185246342365481354294523846184527642342

Розшифрування

- input other for decryption:

- public constant:

3426599029FDA5D8ECD7ADCC7146805D0F19A5B9BCFDB

- public moduls:

A5182F88ED60FBA408807AEE4C3813E01F3BDA4BD6D75D613D85478205F9CA3D1D77C82EC6F4EE6D348831BC3A
891B27E696C394DE92FF4A66CB55FE16C81779

- ciphertext:

131A23087F8AE6BF10621449DEFAB259AA56BF5E6463D78A3896E3178AD06EB661389A891EC4ACD24BA95862C9
CB0F948995EA2419CEBF1659E4572D5D712219

- parity:

0

- jacoby symbol:

1

- decryption cryptogram:

990323932BEDADDDEBFF224905824

Взаємодія із сайтом

Rabin Testing Environment

[Server Key](#)
[Encryption](#)
[Decryption](#)
[Signature](#)
[Verification](#)

Encryption

✖ Clear

Modulus

A5182F88ED60FBA408807AEE4C3813E01F3BDA4BD6D75D613D85478205F9CA3D1D77C82EC6F4EE6D3488

B

3426599029FDA5D8ECD7ADCC7146805D0F19A5B9BCFDB

Message

990323932BEDADDDEBFF224905824

Bytes ▼

Encrypt

Ciphertext

131A23087F8AE6BF10621449DEFAB259AA56BF5E6463D78A3896E3178AD06EB661389A891EC4ACD24BA95

Parity

0

Jacobi Symbol

1

Цифровий підпис

-input other for digital signature:

- public constant:

3426599029FDA5D8ECD7ADCC7146805D0F19A5B9BCFDB

- public moduls:

A5182F88ED60FBA408807AEE4C3813E01F3BDA4BD6D75D613D85478205F9CA3D1D77C82EC6F4EE6D348831BC3A891B27E696C394DE92FF4A66CB55FE16C81779

-message:

DEBADEFAA73829374628236454646374411

- digital signature:

1192C633CA0DD73A019B3B2B3F59F81C62F8837956D8089494776DE8FB9E760D853B7140386BAF60B9BF09BD890F68EF9DEADCC3163955B5A733E20F5AAEC02F

Взаємодія із сайтом

Rabin Testing Environment

Server Key

Encryption

Decryption

Signature

Verification

Verify

Clear

Message

DEBADEFAA73829374628236454646374411

Bytes

Signature

1192C633CA0DD73A019B3B2B3F59F81C62F8837956D8089494776DE8FB9E760D853B7140386BAF60B9BF0E

Modulus

A5182F88ED60FBA408807AEE4C3813E01F3BDA4BD6D75D613D85478205F9CA3D1D77C82EC6F4EE6D348E

Verify

Verification

true

✓

Перевірка цифрового підпису

-input other for verification:

-moduls

85920944EAB0065197FDA61DD2C31C2CB48A2066ED4D8119F76F0BA6022B59626A57714E71C198C16E2CACB902
776DE285BF613B9C0C4F4740AD10F3C8AC9B41

-message:

624168EDDDAAAFF8392634

-signature:

293756D7B9516B215AEB62604E684479DADD0B29701A0479DC9D65F8F7B199C5D51722F6D05CA3FA2A607A03E
427FBFA83ADF320050478E4C1975435ED4C4A7

- verification:

-digital signature pass examination:

624168EDDDAAAFF8392634

Взаємодія із сайтом

Rabin Testing Environment

Server Key

Encryption

Decryption

Signature

Verification

Sign

✖ Clear

Message

624168EDDDAAAFF8392634

Bytes ▼

Sign

Signature

293756D7B9516B215AEB62604E684479DADD0B29701A0479DC9D65F8F7B199C5D51722F6D05CA3FA2A6C

Zero knowledge protocol

-zero knowledge protocol:

- input moduls:

ABDABD1183B31FC6EA4D3A1F32231DEC2E1A9FD46F4A279C56364439DD13D29CC9112D907E62FBBABAE23C9A6EF48BF186573ACA9609391A44B2D5D5BBF6A45DC7E5FBEC33B83FB90FAE8846D3DEC035E4E804C8A9CB3350BC19BD3518A319C7902C2F64D6FFA8AD3D3031B8E8C6B042968BD1F9555A8670B2582134E0388B8D0A3F072252F1F9563B05E6FC7EFFE0134652992C04F99E35FE309409300533D6C1D0253921B6D361B4B6CEA595EACCB766F3699A44A56FDF5B072280EDB4DEBB1D5D6EDB36CC9EA38A0CEBA7736577A5F32BC2C20474176AC637175D45EFC379CACEB99F583FBE2F19E5A2E653BD2AF2F7FBE980BDDDB76FC4D34B4905FC39F5

- send number:

78AADF66A5986E1BBE2F1CA9427553B93293411F58C9AB6F36D262C87CEA4FAA59373FE916291EC0718E86C063147B538ECE15AFE55FEFE139BC073769943061A5EBA151AF98C5902C933A17CF21A30CE0860F091736DFE89D835C167E4D6E1432510A1D12C1B168C8B1C079C24F4DDEB96DFD9CB4DCA758B4343E1A25100

- root number:

2BF082FBB6ADD038BB13C88E6CE8286081051B719B701599EDDAD0057D72A76AAD45C1A62D2EA65D1D0425A1B8A5D2AFB6EF6D2A58E676101F65846D8809090

Good proof.

Відомості з сайту

Zero Knowledge Protocol

Server Key

Challenge

Get server key

Clear

Get key

Modulus

ABDABD1183B31FC6EA4D3A1F32231DEC2E1A9FD46F4A279C56364439DD13D29CC9112D907E62FBBABAE

Zero Knowledge Protocol

Server Key

Challenge

Challenge

Clear

Y

78AADF66A5986E1BBE2F1CA9427553B93293411F58C9AB6F36D262C87CEA4FAA59373FE916291EC0718E8

Challenge

Root

2BF082FBB6ADD038BB13C88E6CE8286081051B719B701599EDDAD0057D72A76AAD45C1A62D2EA65D1D0425A1B8A5D2AFB6EF6D2A58E676101F65846D8809090

***Покрокову реалізацію сценарію атаки на протокол, із зазначенням усіх проміжних значень
(для спрощення значення генеруються локально в нашій програмі)***

- attack on crypto system:

- public key Client:

- public constant:

3426599029FDA5D8ECD7ADCC7146805D0F19A5B9BCFDB

- public moduls:

A5182F88ED60FBA408807AEE4C3813E01F3BDA4BD6D75D613D85478205F9CA3D1D77C82EC6F4EE6D348831BC3A
891B27E696C394DE92FF4A66CB55FE16C81779

- public key Server:

- public constant:

D3B3C29D3CC8ED7E01E4A3305BB5C81C3587C641781BB1

- public moduls:

4B7663D049D35D6738D88084B6092420DDFDF73A7AA6FD7EDBFF9927BFD778FB7813A41A954B154C00FDE2432B
23737CE161AAE1FE06B2745DD865125E6F7F35

- input moduls for attack:

4B7663D049D35D6738D88084B6092420DDFDF73A7AA6FD7EDBFF9927BFD778FB7813A41A954B154C00FDE2432B23737CE
161AAE1FE06B2745DD865125E6F7F35

- attack get key:

7E776A493C52657245E6221C0DF641C8DD3C7FEE96D84EE1C25760811DD22C2F

- number of iteration for cracking system:

2

Перевірка, що ви дійсно знайшли розклад n на прості множники

- compare with secrete parametre Server:

- public constant:

D3B3C29D3CC8ED7E01E4A3305BB5C81C3587C641781BB1

- secrete p:

7E776A493C52657245E6221C0DF641C8DD3C7FEE96D84EE1C25760811DD22C2F

- secrete q:

98C14A3F119534B09C6B04FCBC7DADC7F9D4A4607720834196988101250BBDDDB

Приклад генерування випадкових простих чисел Блюма

-generation bloom prime number fixes size:

85412926459013204123101273360117717876262904725623203823358729934817299819766
80461577945760724108609709108760411631617709679335739674361349605326996655264
110663052280405902440982154699938986805041384540846917669369649028476077752707
96719278274248357740585171643606601650112150716545523234790678277867664596770
59369779580528907266857744753140221478237276484373478305769459917597442715274
64471986840970512941264758242046463037404016280003214987806331263286893739502
57863183173634543544279497909505351987277741308891323701480482982937666675562
41763818967914939306079918166335536198613455033859687569182256433173129342329
49522656390837560746407899996515451062278680775322044619731554112260995158496
25354904094699350056771529894628021533840578712574852053260481409931305335026
3760487791135902855411107359358940601482171163467644473191353376551730649967
29411788649010463566795720409627107034424307785675808345936028837527538744547
3002055942008348479388022718695684811478466990614714523759429696446823582204
50529237160894960850207127428412522935792793028732901176849244917826231161385
9069424326873254014430506890851769139072001041672570505116882004657091114639
6470719539946999899597036934402348880648699753101724764023180392898205396003
29274221811932712620690350709552103226164357239091663603610204692750884684283
12616505559807469699287725867323137689102739175887039274790189560541437139887
50077667855723603819119300323198081890957278571578657352400067348759791148594
71650534178553877743019559760522282815332662817553283544899782280714426090056
72073766723964981715108736185978484467231056121925487334614060819014514277139
88814805553414268787226957664537333509775397788991524881778996745463973532081
2253992938533644827317639828138073198541653794015527950671744906700124460236
106424100472681921024198416192697699846475349246948413133576623485052741441753
57035183167500307072830706062270169770764948910548232759720454121368591567859
61257800107742532728025131547105867094171544879249776897142346828913202860224
62577863700154558872932437379683689945892708463257176624928234836687005411803
31653316292022653187772662956142806518310489959243782901000742276696753335534
88636377476589117344199950462418584643729896426026429053463597611602314988848
106471153520289374295656942335058898293126039567611558688342821065673645638343
88901850536097907582137524601974427903619590055095981048700367169897998338482
65602399473656979650504273008891067425868697639608537384945022252159591253917
14332222354579514442454043097137686178559894413561496840103397257632993360160
58963561914146884222946623899176779429501440731580073961142544162928724798331

13497449068149480154098143380082681623406974541291109872485911217108743726946
46005943653924528163245004304401287416685898518091713170890324251846219143246
18834715886479128594508292989783965150693028473209966524504046333110137594498
4413887340053764988514595175094186722222580916913069748131627177081534251163
21234393601803689431305041629177343245468207632445384117917144572658282746632
21534918074886916374213385901501735770545374735967102861135235014247020775935
2528982174041023829589135257013746843413171614897853991626604229498483586332
79282349187550802962325872745812279459641462591492733592810190992926847561226
47822563757903909858316182770796074530797878445926333358922678418523399012727
28730886397743067890907288047652454118043870292063035745398903544853475064114
90534909388555165921837796563783616634071289014797865429779923218149756459366
50374466560349508753135079910953022981703353589907984459729776506499569911763
26567757647349794126723243118068211212800941763068873517122507841818358707079
92460883268458004541778305646911232074060017962116515905106089725363292137038
73089475161620725128588421714545035176141697076792810603521168521258811409960
93827786446382614116953507204762555943154396973976672097801985470600238218135
85886201191804339578839090879819252901833735010430311545004645204437776638044
83012391475979667866612773995529781557690139994154375084273230055098879608782
83187898183536297208236788086965329026018668402096315562776830167547183326125
54944269292158764072885911109983048897222327172752882215324537173042684965077
106659148470774779000773619096435872772155164059467402755061034026047544105082
68243410165349803440229448060135923013722274696504056558487875500637741188257
40740740994831446703233216888352044664879231638008740328139138421874415454668
103208659819500717305066791374561302009258316515361556524771487296322303731073
105803155806718249498688741321724084856607025557572202220463800929308428428031
101033456020638252579814366023862325265753186810402920754661806450484916127010
304435932167457817397460823484919943762334476291745057632611814430498154212
76182793460674975926669416090579430373544000491903496445507714305291736453219
75300996655984761644038117098042616962454031600714838847453122338340717582488
54674823582025566865790966147665848796991165034220726681991374406473573822803
52038287004434794307694582489173401992716614936546372541164377818887009729421
2297225048536418145616684501621060178128564684563657330636953545589992819289
80530682692697672113017065261516209666012783863529265899978441507901483198589
26032643813817770380727196524932613214976580393024890325496467885799106004325
57143254693038173347296434054752245343106375228140139668393798113243640119361
84080077554541755722788460080474668223954114524193387295383390641595217452784
63035189998165732169234102817551571044471624738354634409929208764244163482510

48503947166762162031598999632801225884399245104204827039579611842213064438305
28015944924149326939754564615263512388732653979720489420018054170651779805397
87031409924752498339620438124536390011812563707449040953162965057549483239634
53154848129618387689979923214228288491481600360470830140965749645168351208039
72175827843244575786513487307387995840098854277437052044520380970506630614094
92325191467068409694227912506640057408506787009538821582960019500545693038935
114115035081916858073714900886829689720823272548725985010813301358342635133
101406474091692620604973728757737104010484249182271423662711444210949964662524
69906548892847048319605950205988075813691334068507350989259007215990297415553
53282560931534152926992469269163895937266074032435562070874788782905697788887
44131535386188797779021068411582590372533211207134098938917536111313178679050
72176318442265740411110449405476798900482694407754384752645466416432723485753
4941734903036529119349832544563055813380598876942122935437339867381521997947
40717389496410766666254344139040966237534257170890294433983313962042105215114
102078286678648930070410837959534012814563506559608983809828407764388685054897
66150318397262960275913199458406715085410780283654039840039087097640804765331
76083178755052496235663281304009066942928892281912751215390611403494525668162
46627588322541229703889381769121296309602130731995974977208157813071602170000
48116538806999634782020557835761075270949273658828114968942550834807367952504
93040683497004067900417815777522154911963879636289963819144086347839056687735
68313787574391207644970106006738289930460200359433183547205133446300915597098
7142728131903476404657569684763349350934748061905299903882224856195184143960
7419166284000647610415158049865569433464933037554016468414906237008602415356
84132224942552512014584996825063002281965243400576282314564314747392409063415
109138560021915656794192510343975662625784176890230585006833164485672006923797
9850009536651004858734683358943166712175142864988023925260188615103237177525
21974288653854477689516605256235712183063596806636399777342746399938286503971
6351369017690552237631784946137564678342895430960383542719174536646422921880
6513024594854888468937848723466649346705301601434674100067807288228727747994
72988613078132915612412338075017936561544423618077980701404723214497684510984
93863286916489630441392426009164306849044585668479922220389210499579691702388
26032883261368570859903498338168147027514029119764483664503151017238667360234
18102325461749391940183339872023843576204276628628328075450018069969936250799
29979797083886092673748647089752904433997126898265869396042527468218999305145
110834394942687209358032394705231050934166694872582746238287457716316709171081
88734369971106909661472324777150835141712796209672490738148164425534255038571
7916902312868140895678515573652035667018233136398146715038538567694150103371

70022916696509948276960002710115470441733120884319499706662572153828256470269
7205353517213233774427030103000886379897200316889629668759310766284754255471
103450949946108557582585312394358521397281019377308379384060205556356342403204
66117516932640895870879774249485384169738740643044969014438295230634527395151
50752235464785507805476089723573234654576573245117175131940935373773999809016
31534879422627961932812061348974759942208396405327255490509031953901884803179
49144102016462654745004825852450076954788650385346710379971359593422190270528
66919000367641125619547733506818809305006136819204286387752520530183452817013
115011831275690072283755076896032427125254178802913674190962416552510171276582
24280564432696170533308506553549208801906563701743401791059869529052798941617
51437268562977336575487770667794797320468285813855147984714546375820320420077
80815870288591928385956000613074068541445954599317811831873260612076107589328
23152935747123581916488009719397923052367581520766694291858653962739114324162
36852651395152911268509827538803040401861691060617676803068312520512990196020
97182348327640687225206211208191606587209638810381422631428927115165962127514
22538336645935160383029216538905705910294563060934802747573095302004524463929
92793947830562452783758461683820217820398443674271992089833025045902030548123
38696997059562562463790937315416136836595146042945145969794159520909453823406
82137523578733770813753648964680128308729830797279084071763533973434461557106
90611324404838994401540636309529907952936802812360492545082557668849627256941
39308498562562468739338247866411324447367458987406504758932775012474007461991
22455327764817700249767254497056696657087330824702870159675411849157565613053
82471927207679453828525524299344046193240824210560073103916328343272459892087
96362595356710175406826354515472937348981057266697661299740059570370191817561
55102223918180279486032829741736175274451610341560881703767831218555228977458
30621969475114866321803014413641807933409563321568141215625038260474098413794
48286027029113358449402192514917920703469041838926745496440704194904694007817
71587608716436336790056821624315358824450381150862738544908387764849211114148
31567915640477499860063823498239348268425997682382011881211112592398696621655
3086813810271833328722622543238742127274879499870791228855566706031019900557
64348742666113511887182890120537258340008166945251463915335350515673090084295
65293210434615671211145885382297668748177193301805120028804441143012100737502
31043726015602946116762585038016261427191551240053244917472751478853501961261
80562813969589872355531117690344798423979507054524888287565288377703357796499

-generation bloom prime number fixes size:

69492481357905454814436522014728094347452751829329897782636373513172051662210
22649841967101197519673429867255278934555953279486724638652240752845509484935
49953751910714129200761155382492131921847384874915309290759964489364470307777
46714733646800036411160346327114799943517370782858224873937270992502662911444
37870257589457566780095107668362295050269822797936141982938298547933994515466
31746125534282099572037509736039862373246529263857319666673865237895769687669
67736483602472069918853509355525048846007911924841237152596190396330907591375
58039108578664557124183887597500755856074034226063759974385973977897185274261
50343871836849339389932804861803081555924787485962809393360611438780113428740
20118656833443564946714941989250401731986266845491441685150831529139806277967
7491866772387338861134331905319327718721327199530219897242802027989015275784
92358802599437195389496742380303771183734293582045170089559926729370091863760
41271495731355178445239337024704789095962315710003526693710758026006197694201
3022313476889940487506962208811013226566159310345517401946415779702766707221
51174996701520372704382615869938570529022122243828495140025188168679072518604
31534995261206262735988055540238023329544773740895860806149881184047296861773
47639067872100511035435224228271550650541890615587576346081447904357454708918
100266316679787234887528874184072955411515153075998932569307620970859543828573
110153594432629613654324687353549888566419604485050232239597545943139757820433
108380723494273581031395794876164808079510351847825763719740910360219855604626
111619203509638538004421762662020662713167607974879233148334374952604011694137
30179900830329045695612946939062922034934053802037078108396403939623942065730
84234724651088285256803457766985835007152423603425786085915396867152539431060
28729449652598875026304486174376512102981804038296469366370133060889100168892
55461635399817360877309125002983734302537468618591804223690590276916562950975
37263690832394654259150651637346526765887948207252934608965968506175918604366
76639505671039280323843480340359185760499897035891681642194888108923812401002
551101655279811103887904298115539956770087104162268974412276385523114709644
17697245546511031643770087662394721703151327274055220482024830716968046367115
89835786480481480399403751044817256909470624548539980208128237372871442800854
6642501670398376732714486711495662673190090735794065546122794461879535555172
87979730062994409748854773120522446393614475730459200452168872013183373315432
26914227547581882471900390029240299591423472763660047360195226910782029171447
66530086944120632610037448130166034180543144036124038467536694845296775587696
19864958796888314233822133700150915544901940251966875204482834296465673352812

97512633449123941027613121434314084871532721388521204140243398775385507617544
73028085651603165265874238994193643439270436486003352646675784500486654713488
78644013811543513029815027473396562364465526174465595716620434284666450891766
14735349279096101342101203754231473896998899167361250788684034999261685393475
57039493011105443314872796251209416051563230439227548215642685347634630456161
3232262156190729086956016587882044922388712848412884456175755801924658313917
23964649163848251873152567955310562481470816890346888026512812396530612053768
69400832495793645121602576886795923418445527719058427371760065523868235216625
35520388925103553057990666713182536654340971070646764982254474914574195797837
69434270271453885340732518716179934104627034957054272258401735968865307273481
79990944310549478216902440141104319457694495726047544990908853948726484447031
31813594381248398287524140302554817097079699789087135813674040353965396173269
20960241330412474358185477280829017099247006751359723170039517053506585934609
53278634662281605284373586125907440490541824701457568390618677779217194022905
89609355283663037328135091972152635424237040807320603623251706809599334784921
57875434380040962399597604596034458567750034635600360235658971927497091121495
8682042693218583906697058738796684906327736627467494616492352195763588988640
95373069629012727678164947552289315626565711097917922477868206174747652904931
4630589355237170731928358439130003759881428890332993687598591980359152190272
64130796779148622455455621485278995826450209020623922323151550678076649051146
8833165626103448370240358606013859787450180840764515150985202366780011371661
36767125303993801818751246109877199812799780051594187601837110164924429526558
90078975502783865882780024751438652853851565563106241533034949203376872424439
86501532160757026763933650823688666824976740251495242775562425174319352124856
82545418975121099699242378381073691831097872150622479235493495971696462623471
102455408600096362428203212369333421648032265546007019699831044457584667658142
71068090216808930787921413845072356184521002085418254057346565281068338287844
80185580012463111562968247395168469323929172457922786720170535874132219803619
104427930266535547677182607249681624869031749432985599953550514049609704705429
19238823027545573041420114893483303162720155028727630841545098218745516459890
83154696529213891952063950425171939440028917234186624480187202704516441432866
66905123794370559214990533821071695286161529161309829208012942206209737728428
29823594410780664144938339331130181897618819146328663390246577273299399296527
22922250704181812677988999052833625145792604373539253503457236275961975306483
46161019403253149154779504185515044065544604332426149714760034628707488267636
37294108967322926628099114750281833931924912825823470704675809577044016456998
49689401750359877706630890397433640282699834121601886399293556132073462885033

3005579812462384845223664947713579874259287912309310658926580765711013555075
72550331360226155502989113447366840645296208325275109464860162637495226136553
69240134832032854748316669171951365038508088624105347489754103734781648617031
45485819797187779209507650899807638969508304061032540756758562117445157609827
82702384077588109016131990130686069641214474711306923376103200928778219247976
105478145167993514486637405693308716164951255083636372796317737617472969307156
77222471037818798572406444088218055331806488091547269815176866273953439746725
97639870884072300749439580044250178556918825513475302167970823348047040082639
9487097080324218975081332285456790390002362678626139473962035248517240934302
77582723757611972958662720575724895015388696140209342458541319123938127538158
23276101130419383030522577848124625328708679790228305901519701544927536582790
61881292109258434270798964077591107267625533104392553813713402578168818009288
20943630898682914669761143153847194900274437530129473478984539423326713272303
87808644080517001788815233669208970503256201878004922622152466788523478550286
30321294130495913798662442670886050814179468004419540981772141634495830765774
48703084294518355497099641822593697330067950070810213371993259929595107468666
102402562446991664393461901322157800385223625081025393283737669489904151443278
87594980793073206512632280961796568906260427212777353735740645448345350878494
94879327534449702767667079045851702855228771943521541884241139605371623603297
67518997491728864380671765701820986029245340554289238184244049040583950180972
4164964723677137105793331190229151305694755801890011362186261910575627071424
6592878408301494606649646929388202016321371956101823536197527410533843448862
19764933225431195123831239778701117439303668868378935691977340335720610359852
15118287900779167047337947981452768612523512080210597224264026332846438039780
14730223136351337301121519223090248055377370944484501183131112241664552808232
89548264355182697393250808089482336763970616096039914339131443461770123539149
113234912419888958829833220627080919846394112934587628411457800933582738300694
23243961075094657247953035814895174154889198508038338986049839779909238234681
43916118635513483266246149162712163561783692105699577416388426017260704413302
65613379361482836485374898360550436544512025490457685132921845672496309310387
96781069882328073257965627869030556346778192341610751043338872984770310371696
45025643948561164272416584657380770026677574425560757116204379549773172018100
66368660846032672339383949676277866011950798019185228059935407995212339478771
56579166644757095498764507012290047242659146335071493128447822981596537691211
43579071194520696000673196356225239971471550013864998763862427226906005166615
111650527538205287549361223915599027603403976462989582749267734452320750109170
34524395829147181592139088163441294891824477355146748566845638325928330133616

70733422760281690102669183347211900588771691503259691070506993308598615388732
32070139905640113524549985215541261040406341373504868966313796441969287167070
107823477261353622643160311083371813443090450990910784230364918652570225073063
91409986105456975677190157260509458521498301429734808738733313577863217432212
71111379888159371029536392302324184042809590318085032201642677599783659396618
62318962910056964655617402759930798387759912043853199784477625007948539150671
32324618433333505226844481328019635475340302962387347498395421024484843216774
83500095438995290282613735347895559096150735570623005300349980214476339373595
19576194815307301932927857242750278863586952340902787925227490648793224669200
1166819787771971798396113583562122566209539670931457727466195327446763231485
69204304192940201923089596328346609625823528444896487186520063325246552225683
57529208990535563366049508527934358733180678027616292336927189770801896124268
100727533567737149685446222082973843593872689884193540574179809143468228042595
47893065541087097194934205618287358383755393185305727515011239708158059686919
109342298450823194974711494600662466681861420143312475705365058125494931754766
2548566011752169490565770767097711310011480363336162994583511140301213713559
110881033967187419387523908824212099675219956759192029694839156022535590308795
72324816964423777940388871402218708455359135490101351912329034577430233484996
6831040471029960428205828331389793552045590860901720900818311438302537155498
111337897426386969583535722247466842367023358247711588039438345392484461758213
42439042354902573746401820669312556878999040614520161180851623385858621493489
21448547065317917828269666906883015343008572852571857330904871407992329871371
39410967689764579222040243579808968561696762988205125959532072425130395634661
93496237264496459983778318289696574561249748019881491932910654785240224650154
85083726213468656264693255705336458774426255825244030315325861371423820472467
69873379609715329056276865126956786166513511675470705137218164857252884303908
56510736741407806419493129751676557438043608593295245436396043001571955301518
55160953981923469869594650767459597571797569262423619548587809759766645327289
32470450894830359945188296045290106508337119648052595853501572430148348191896
80183244650678460052254689659366976157876817236456281294078210996447851574358
80094719763755094989191199022875220442266632453928605662166716044125793566630
63432877031941198772930398769721721751687177277466000674834098021656745308762
41340226210033747204037551691990190540897718794016031823556649165124496351721
90241751757729054330663541856413690762874728322482701870265933761136242841963
30652108494819307846942193138508171756632046800682973822095004926844223560213
86721543580827996547330237259766706120523207286636530341002163103149435326917
68700439580955824804765781340989342900210605726544085838315254967519284452491

44647105979352476640157682672442778082969905173303913958811153954283184177074
15855235261646752144408848295023639832927173887051395083813909084295426388562
11543798563841227181754718513754223839592896235327820198702985751002300415266
13902604615540630048484481821130943970643911292612747645269467946715922791323
82185878278376056831482416904719553123469812645363595542590474466834191192459
47054941950928420848739404513889251623300345188820453694625129874635092925178
6909909219605308299359596900260985936698493608627355027421822601233174446547
51972878423540725978391475161997405495497088875461161022039903827964250466427
105851304854432111356531684525507770879278842900520444704631186544441777646228
76030858565644698470335339332621617883570145265548767912783452502500707339151
71169140095908188682515191320783694773314425010332326709607522515487860395911
57603067944741680329789687334338265040585583601650686924200986192125132347456
8872845834261180940512746920293679350512858566019042951896112941301259546739
14671073820566805021251090720900993241974004286097457892797079377396216461988
46790308612253289199919074644456051031933119723882047689425001558942923003610
11963322405466161993343890362614732694585854516463450328245810060801734140197
102353900167609883338936441397243311515207482724130669433783386104434004765243
55658159670014184204057417658181309778791409602997590146100702451681845128892
7483181076427784362588768654498478719501289484270792127649907080841561573514
74316241759145496268376620827165504885730801232138399021041785523307170545694
8051823163189955581993835047869323003273077409221327983503608000092659812476
11895560320710027905796107577841381967870709806621527800497236631934689076929
29581202542184594944054813853998705837903263236752079132690036558402711834883
65779198313876329637361328704614440168582710642894207945032321658230173792241
62669018607378771668533822656727301970058962997070088651280372344316976010168
76020480111258490567928726089461832677909715190046975534106923257298380839807
105049189716198548620800677910852714893699758052176738341639496911350837829987
44479955424691619043400412971550880614859149599150548233917184628246336135058
56490897305630113586982932874603415373295385406676526610220933739908737427357
113210314395663917214359547027211976454880895621177627919375479326047016371768
5793230730090732541723741032368295169051156876409388059997129904605506000253
55449319156311007019744841371498876213796829150438219725429533593452639552403
94296032018451436918501816845443618122521510579102700315962836424512279795745
94900668331505572582399729421509917433282771058548944346500190762011302752899
37841003076741702652037412604335188688945069596159859834604144001448611257859
17499422903058049343606498753861504803111820595324822980872630084307079377491
31830783085310663322543151528778602750772705361572832449426541316360848551714

102814846171294828025975484705593090651615695044356133215211521892154422188659
103030663037796321751140240001290336303136282312227341941930464053353471236453
89794894950988641718187889756707019876431361015345907445099634157041421475698
23575274245466251302490127784100551386917527578388140924837077878507275898517
96450383424409066524497389061860331590475083008751848882512210523914467160565
109753285158765980301827877255112517308821537342956040577843091613237975306967
95175368031987115917180455152187031247142768096198609098243024147481589215081
72472868025050969252756185553470480933270077016518379164766958155268184034568
32347678140864247472499457275839432198903424452291098945929400575171267542981
76580802698804563194070540708475043614930567266686594807640245084583967958061
102282006325954783397640025490408879476438428168306600321489514666521161087004
36129036030511402207942434230054063595853766170792948712396906511225547320232
34303482236622669734726209973161337475377115687506801279047620024722951532178
103562322844008844204092251018092183455714617496448708816545388392859368292847
43643015913630208241819539038013627747274375463269988614474686788523118729139
33898225058077123848623756502741361338243199631206327357992315370770181156647
53036656806197263431942034098302214115057905315772905261881029940887918361016
62493668836894574610707252542150353231053195651710087328691160185859623609912
96748883414117836077909289558970651050921851726447059047286538627415701730372
12304750811746255102797048217154693986796199144604868996163446103956467121216
65760802755816910505964829790306522377783774585046095316676719888490517495416
111964364600221065776307819498474921030032465970400809988912603427119842312934
15753636393485182182152464182504854245036864463587849834823183554124467166534
24109403878257513735432801863740323891874836147261962430629269086612313020248
31072266866253802860132673429788550365251610390509837223803089577403859564235
7665952806397252164918814245093986855240212204406953482764262940374689389989
108555279526815991225515739053540591299402540142899599596484127016370606248054
3356931746380426773450585399602972064056053908992988826662088772433148944874
107328665087996719824045994475474319930599316418711412024846798177353117342531

- public moduls:

A5182F88ED60FBA408807AEE4C3813E01F3BDA4BD6D75D613D85478205F9CA3D1D77C82EC6F4EE6D348831BC3
A891B27E696C394DE92FF4A66CB55FE16C81779

Висновки

Під час виконання комп'ютерного практикуму ми навчилися реалізовувати розширену модель, криптосистеми Рабіна та використовувати апарат абстрактної алгебри та теорії чисел на практиці. Багато алгоритмів було тяжко реалізовувати через абстрактність їх опису.

Посилання на програмну реалізацію:

<https://gitlab.com/andrew.kolomiets/asymmetric-cryptography-3.git>