

Криптографія
Комп'ютерний практикум №3
ФБ-05 Чирков Андрій,
ФБ-05 Семенов Олексій
варіант 10

Мета 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.

Хід роботи:

Спочатку була написана функція пошуку випадкового числа, та перевірка цих чисел на простоту через тест Міллера-Рабіна.

Після генеруємо пари $p, q, p-1, q-1$.

Генеруємо пари ключів, для користувачів А і В, де (d, p, q) - секретні ключі, а (n, e) відкриті.

Варіанти p які не підходять:

105282585700526347273360582147371322851336859425932117795129839337444071467496
79808921879917912312805597120317352545219269051276978031316770935128467017856
106348068542057345921296083702624328781979875717083356457608649627377423163163
76023505646271033009428187436826317299709207769723849617524141369859561093335
93977924492872190841112600006938968944089325497138835478990113678228671064524
89972954841772934163546602968673411047631687087765528371955268467469597532637
87426917740949823729911572011833046789131289016788827997168525999870308766572
79435812574643747718548602323186024981615416666230510676021795679229579153108
61332624657535893808366832886397851230169719573678652743688833637892789451519
108464404595324015333400472791397795143032478765980578264562266345739251003789
76807383638870283136289783472531762455319696114716454928955768047951631484891
102561081379337402450791392609593397102749313238175924766983056969997665698893
63789527449358916222471346982878789938685696144982977347232125793614628875613
97919671290078235262123449541532979096546842113756388876038600953651203232724
58387103291607646622444098397673789138271964865979999132147983536885663251949
83762416738446021228170325818945123136195916620574959335346471851754422769830
109037075072271328693824324555556752112375981900312641435754406284709886169967
80724843572388660407288901608582236439631919144827155328738864619018867742789
78404925029119962844685213880983529738231201546826232237702996468948302568204
84902608814455752830570528726038945004583108604525955217438221108630394573042
58097325238633287633895838796688500703364907428554970831420180561045967412459
75074287869110272020926180200816036442734230243159896662217301176682642390499

Варіанти q які не підходять:

60478384291040889942378829472892855159989624801198059347575467202480552860252
60368403141870495860511940089658869786487286091952516099743965699550949271860
97856184293896474164376620599208342500776316171579231332570855168721385183217
62031495013776561318862955013022505137895414383316974120618621586427580347592
62094199435034630875778162857917016098084504189739103553168663982943206140075
96415315991012716946307647560032654341635619982276694870977086181425547803958
108414352539993866523188113501618529373665851670487845567736474611732876430244
64033504875905916444000576138931126576044347965712034308956718337381403016478
111514326880082042371785314513954871265844613310356903064602183384388800046250
77026756602259815480308698760803088748503382279014310023680435900410552694689
106355532173969470165223272012264960425538340504834803706129214903072338491205
58662156546625709334229556590131977487618882408303080060349344144743203527330

103947215457868747533943923855796697653567296231568100708213764817147808608388
85897871731491222049109790306410588644579514966632014934122216214287293248820
110197166163530207254357902276042226764437418460061896384400786001754592013927
91600677539384878489834818929509346166516166520234420785853189546690244039701
98468023829906164908637202797311304959447911371580019687821034162440145087073
77665723547888096539006097117426600401141838496782928108022146842403066456147
113994240619027736301177455485746267998938486718862334536978721988827266333352
115501245767804505072962180470585997893366322437120733929012956976806237297783
82643732947129520834019861876570977408462522115027627479240969040718515977555
106697271045681959669550149740869762706514127069161039385176285860861402247655
79833879945807248999890653458419676998458445723397610565203245006807557448788
85687547676529979372009847340904941393397555101081381165704164805672114503284
60170738422069567825585638463080623503933903903962578016890194755701552554430
76675812984608845556594461857066442197034068884382336139080219806611866030363
64561392162767359380467960753553177639973817639626099462181981008451280799534
70939365080073550481513719810954911443608388739213108835053116438888452726777
66593830061031126689329631928311025313067468628830603545192329996561043737451
96397188354515968580970039687078182441128509338179880208998585007282029498895
86689002233443411842178598634959330493015408643468022278822497716059493630465
77122052497682077508463570022762485209810016056301574464672151834603238811376
85905616465285866569678053933725196812625469534383248795757977435296538804350
89511021075200589983594554216968697602290220573840573654670959436823460889489
75202232666396216116370599288098163018861032624390379664750874491687904205063
114526015707037292368803304109689038698810278825487358786325230079229568184818
92299183271250340594077486633204693752009845587845880255736943337417440126215
64167288056015438308409378079371039992972621925310251669579036077872870916209
101242625640932260043414420990939068215947051543996939744372639558658081384123
79016559159067726053146645758523829562257079928436266649275975079526910910183
99485724451237322512114864542026686650240723096897768912404316872664477467451
70161634180248711757130880413626261267543485720774224533868532841769193436313
62014873266058165151431064270059420217225794710163291876471498052664371996186
85041457537834469299539809886407542050743675080385008373072344411027478156232
84706122112633383556816805158520701448774858525668212788374174949243249327112
75045661925518609888583748677503594999486363378443832614567057745032708684680
87613141984145317240939748257995136631306327874936939788798356306710632955271
86102691225497667910982675410236143850888839135757298174553475569178775805507
82172093146938987298884668286215915458876177668273244361640847108958811606689
106808025134915338023893432735455876094328116944128668437897570150391595767349
113743136440166315276822808860736756914992401467271472558315470723429624043229
88950433666532429040361883053357884539650749969892855741094840993396399881698
9266773448535416115806952027849325910029895988860794096587123622670679076143
93211256181310586547561568197457933258199900183486018013707660212375851878412
84518916712992449027038496483193917514404125737668450388178284919085097843706
114278684355739035280000940375399617809416542703992040811455070854497631820840
96657304841663833885485342882881561453442241712876769748256903123979325721654
92434265856920508567586905599378604617924707876051906865234410230634663592519
91832955083976883089525118132347403004160576131133926615073677565184695503840
94508541491666305885653775982665192180611173004353820941460070923725148964895
75348580685825413970065432071058990737735795019349246190154421213263179140523
87066433097184472017316606545346756208930036318739117984808365949970119482912
102700938378963861414175702152557277218927941928180987192530019357407102143117
102340698160740484491841115272676503303589133035532228240611871433456507102850
89708734609774910872131405528051157037327874041836827357736940610829623003922
82542716491495874724656900613450411743958338107130366052792598549398032574838
98185113303044799850813676915355544431126836922219400874956245608610243949552
113145593782550938141212779857502098077735494128025247504948250074738454882865
83016423682522170390014762244748190804822223021065181702517816459946267424792

78108284794544739510455169360095321387330757680929957265718409699113269043482
97304000036538763979593522510461069062596817436278489084589803963543855900236
86557212017884917452645638790238302231012227577145709774671011114262007596842
87692102120755914806521475664026460668755134352986562391851545116450377241884
67344458668693072385660563205137498310864191622426842241899746193403452095688
84038252053089330499904266223709374530433877528993384101834315019079464720926
76038545164046285901195503680776492223810580738327558296676564175601482909582
75976366288411903321771221052550185172157428258842018420545477833107999337150
106921457602020319976299678864248376456291034473339414646900911486443898024611
7624095555559588641570071385490690660290879809693251720131348839387822947432
110986838477725408202117212390468228863852510995402168000004281972098651765667
95032512762774603313477388876895167257687297992692573349263195084225806939233
9551658888669425558220766178705111209174818586070760302805307691823915733225
88391369901483195581053719066017934458541968211411919017915878185140658629086
58924282985467962821364752431394249435873195962625788239602484469862735250870
60513889742007699804915531579603679458840713212360687235755758432453840715748
88662116285627395580992525677769418890872531732591384587368678636168757689544
106333486317843058198314405750161040646183166582001868170048381058288833525572
110586960047709016495608115002040217005592852353594257112875869144578809354866
66668845144626745763835681680304719919141438420285381527926119568614399491342
105275023476806812265407993103883101520020852490672561189358962208902405751171
59470270768022861829848593846734352534812391876862254302206893270795102649424
115063339306430032573940772358687184431367522490771131579040078963981613410904
112382247192625129926567974195903529413017554818531657492396568915154619397389
104042570659443912077183400543129746400032034423820263918347822617427456131473
114365511200568180540617038034153398330594365164028824616713850787140335476963
77661661797298339722298869910005755915037304084622450716815093741917044142471
87789315446485259147224296656818287638357958073708636482624159214185653148423
75813587771372727752651443584646062144894291230645694569461927213322030003705
89232087128389774077303028367659183911474808796884948165728355571474001877810
79816457163024498753216174965243425138257003047375401716336647728862921597779
76076109661929530323134455769368842784327603081595277366610250863504644543497
114724789500438775584839944436557234856244496783466298401134257777046150439448
85004077080871682219167892916252585633117246822616585432871620312107577296418
71198674767682431808167090488697103572357106532439190680120631932179642244953
86045167608121097709469389501111409907825283382603905461241450700950846764945
102100815326067158987807502872354124230267965895321273820539328473883888002988
72135037275135215482101152383179572705911107240877564936941324629509600168454
77931694580690208535929969177899476246579477700415713797323808932326101796686
68626946150836046844375126224723234638203710755313709470271362921910213547590
84719528035807496162722804958758703221869507856027094850046801357277425368925
107338128350618276392753132059092773038145506375939362744741591414573782053801
68208737697863630264549656302058588373091256949249249827704206215248254320551
113908002344224431544280478232742327194709244097553268848388737417765991068546
78171910413135000534860028547375721895417173930968014717155793463253787472235
84971150388054372792371366362326863628115073675231193789413436658599762331059
97217493708141897073424856888323448772873585259013568975217354559281375372279
114505102807861597688472465737369029320668042255650372166067333368150944615974
64388104717609648353750791700246309197681840410827022016062246170403854277338
104610537187823863040399341950849908313053195454999109134775624785712280111375
67330170010395405216428800516585341873096400509711868063420221065164373820127
114651285318064463134980071631276876967265294295342879406200628584722824956632
105500265930971463627790265623268730289674739291363551211181258278399946555647
69724810763987064380337154708822812386634814175192763081592988194859819127553
82967657549154942308850429626906364548482373898832373514819136835079681670374
87440597849474367989141312563843431635144604909644955076210447425668169908295
58334740961523070518990479086921798199134660290470250798589587830735833867796

84582463301435280529892074902158073740218387596002630455181241534229170470804
60878190835890823333849689563709781605716437460360407087649092949358206435391
89516846695829628959718861865029111763463603302130790768986079488363533455296
100351601964713134303592051096170641232604940818786435314299408354597488748644
93202214851242945737139482165865300734802721280258473703570950484624655286631
99379141623389588716079534289375959354076632430075899859603779804393500380482
58552758932470142155784004806389205507201966110110352746334196816198023666804
79548551339264391206343136746793099292875682929421170376995858988786241534950
81782695172067528998628351535369082985101692741939652300658384923787452188402
73906325876702552697248364436911509789992949799173640200902514335542967551413

Варіанти р_1 які не підходять:

75237148250097753699988220549626249895760393774205120521184439615598307929335
78543692349037711116347877261323193583438652566196293010360244326775539268702
101566279359412152554497206335163275387358960520863553298427986337666149089919
87389098313632236577378780028353522524862752981050483367268293329598095809377
112695897750722515257827548008732445436591211690753021689414273825406104606276
69773213479033936417273295666737586379105206157907105248446156332925445300094
97550222029864195406945654117685100162520843703784347186642380072841029155099
59284127183863950105171334532183805869201487642144895927889431792943932706512
88037905229049034848024583850548004431596853910846882778383770983293840965675
101442211389586071210529677503507977442467860330891156682354991569449487948387
63089620236007552590336009723051250526931704430485737521087837756859048083621
60014998142302228679129715523527090789372919173926861089483164255744886244566
81419568733267111834276454830576985496642061828678658507800085195722613833306
82917069449530977563642745540077899984913687421490331145884967223836519923644
58320182770194585689440218005696590181151689581926934178947518686556367237669
75682367105404636207146906268619677187855664677817655947074360399554710937426
77889477820971171892247457013682750694357399111328877666546692283210942181878
59471675170314628750037059071894775925011050938667929390060797724112004871435
72072212351801011048208396514610810794069290331722297050140873919040471716537
112379315763238831437271216002756431740698927564657158574021396094936490571790
95041829996544016190947441551857055575448489196202509051223267494107975781241
108479457460396633996562736527120526198998625692080557441185940265742416610860
83440508107811513298676303033744785021274144650808620034513065335752668135159
96488821824887324318695619948832956412567444731719781231229909546292220172548
104193432789070875243225900687439307964539513475000820053752363785810135511773
63159824855573723245196099821512504919584467976540467424706129668582025083764
58187238273331238884464009818536633623544624814520382280593379030751175726905
68783528901059825866200328511353040624035863367028019984598798324553498539294
87443416844593582031688028413977639509174480056351320973804125224090697218618
88954060142601117481518113019812858828565117438772921942039882077028022340066
108380611906762156878889845387827975390067573251421794091489503765020266665150
105950459190708766025693262949226961572867702347094282450645744342602704308142
97897993130598557108566148588633300159874139762960700577724036132823725954005
111265246419041617945867563303876045550422670314149843561126793223871533345148
82894036948735486630120112870376369887447673828802202686802256301604893144545
70676653350516193580753381280150823313693454107012434448049817320395965054197
106545463925146035711976510185472804645691275366745390048004676782345504284353
104086211235525766345801322834127024839748272048652216615954710120849815923200
90544404377634234438047757146418838817181523862515513818251170806883388608120
109172463862469817259250853714558865044834592657184843231815408913865139339161
94131429126583706145976170433100457290528870271551497698941296968216001483323
115216309116038219371894020362147442021779097927321033229475369231968138105012
95393510489436201432199040790417767277715457941290717120130895715231651293190
64174730790010688704212411695139367949904698713872543758307986171465037999110
87269844214996068956476659185054022276526485213064310891063656491810050625477

73301697249834485709227462604298923194494398719298071379244679461798858152394
89675133329214769102953392178047585239428845896083380180267013548093892818072
109994974831415093040111943425743862789273185894683713394463316027718491671911
102441055377039802410790483877884226608842838280149581792148729442116360100631
74371581029160097566111052349475494140267024781756505061504755142865025932027
82927099454905694955212003295600865440062485160998402826987850452744798538736
88265743233459200764881482923621233231602403385410190400038090114227842852288
101406553610054327611380459526447405258104174003144912055481583944655893166229
79921963674265373691503553748491454947284644076151110868078161371095314624199
99865654291511595674026569226261902134320054223584936226374450278003141338828
87974097626133803703508890018708433575737998340794658092158667496536466259478
82966274435245486040807958312177246763614466064329508746112227157340423217883
103479956016536127749977970560398823770950391769513051552052387157595992430971
103711837347931964016885537206491233933515389987764872551317888220051279455595
9578688840989116796753414194286379253399158961772116817957203604495055496462
77813134155476223241492908032741904391904229979611831711354685246604196706984
90181672385123768459828352085973165954493365096892053798312960361588447237494
59337207439384330769943036464608780067037034311552344277942663038504811914522
66511198954679145477719477269368972437822960191949977769382354595957578357697
83483509146326031177408132632453114077140103780706061584600067031326230086844
66232226795970585385052011416843368659891206053527990981166291311627102090712
113519368250954379254435438125226151695524961417358224660110610163156295791768
88118756150974380796506171034654507903965322665467664008842271445965146346685
94294103833799246381485538766969797384688301301954085190669854286877759057547
75153122399046807723435481953380440920137102057375096989855311622910247234728
62139889481505324806198413227643368307220458500445308476486661987014204816829
79339323271299021308830475895008387518342387687951986281805687123103795124609
60063014111410918789528354015438833325665103787302793963509129784544448699748
97143929439939696946056558501541725192539404506337914078816461319516008110778
70267568330179434672214585595415711831254456830379626073652883385855224769987
81492231731490083716273121906567101566821806434786046693848745799116137959188
85657924652955551050616046411568171628357159812206708097018557364142456769500
112496557028030007894404146816881190929938450099058315615960531657467068759718
77989200908196590492981321983256099861576920004539210661103371723793161195217
101338578159631617855394704998789233769259304560648424642815335083937869316089
107500819988938891083450681293451143710663603681660213924276437799588611482532
59994551168368677957862012997485083668143805231736483853815779873656545228989
104433015655145883473309354515978142082947865433634189137954373649908344317007
65240672262345954264530630977156770449242209059293935367206509625786308619010
60249405107583177611071814512426992371859227142345353600742092407888695580347
105795057765667584581826718286036706163234937747128501000805691534698181538973
84145518319798326663824895616604268473379533289347740003915777042453436049272
80004292078108085083027112907308947104351407177875225195704619959376057724361
72885866635441896638482762129811099019059434655978935028193674950098872959591
81867867781745168794212864965014374112435820612620259756620020422858605806606
103535807599082762334409561521802848028263095430719296781039015539183567493173
65387544219953792167124878347864269919684914254301835110000333609278171631192
108501690857984345531890793026014399778240757103849432368734535293717494320154
101563995691040416678055568431639509315811086432211847775829938281826782101266
60798511821968987675276817820396676617506259682114759254937109540309252492759
102525782922821576902168549077341008883575651210134796110695949281016998954941
68775991917086437761986064453497691295129342039242678536437571747228479544298
62226989878997899929157571482122064448267041893566373244787967623394650120203
73664240854581407496703823811898122064562918493435930673617900083838236816523
64579178397196827066674282186287024867732825648778462096536332811013892703799
62862421649763843719678808221922878762572445015796256142275036292009349332632
107409797952790266848887461790297725648168145104365010879733693099522760133014

59060716006034007019951015370277466772437176029690329500337528816627955128558
99104457433076604013628808265800084348146580655983349101287310332832069459269
81920281670447853321141182533912402479518893366338492041384294902617513456209
84677186011403657504686213781422267727980373439762464646390013741875888657132
99799794131864474073844290665790689519158199413221285662253782502361869365302
83996565719274554520036246037918810142604504916835585618221207768562834162090
65268070034626833937087356196169114190281720861353796101504900246956567195751
102986634747411789161055054403989184073333171340423781294281098173629861678479
98544631732154252857766112247291253803988076912640124572306255489146195876086
82690391965771631576792509597865587023912366797767260516513863841658933146115

Варіанти q_1 які не підходять:

64438541771758212375147240706220012269095931313797343439427557945456904186332
96846318634138602370129130602129284466313032634401439822117697687876929197002
59309121612235606602775013461004212734896648551524253545544551696695440169993
62273382649023990410677015091642614462081899957622540646294397985653976421262
76297980134338399919548666643146539076965910034854467397631932414486495908856
103297906212123965455465333319997952242483722080734789269286540915216306010979
84593425699435913991484767384909208785892133018195398737890585221763603717000
71562241055439949670685909950284629479151984415635030715615821493166523937134
78800038294546450169834562610668887673083615583254388003604780959002460165469
101355819541428453678207760017241861296664635742391370904073109951805616800480
96767795625954181123479812134606187038833233631910671643981091765221026722398
106277263047855212050320088540901097759650294492337816056016171816110814289065
98546697996204123640892816734467127441191037900912432125683674126261429315789
111094812003254565944872618571133114115515800009862385584368590556532374002991
110643179009363182055774170081197237446619704737955673699733774222465375923684
95459755427515624934174694848036987942110523152465609618091475438226655472847
100442055633462633943600510769045828628659477693279439458138651690758798237695
106456188737141069528212345082206092920700579582448345863293047546225917127168
110763947137693371389413943472348079355044188606539174504937140072442936648580
78176677493141219315870332535731956397104965142554089304043634419576187766010
112639132702312877189628630061654642807477124265640195974987055754162518869442
112633267006367255234509292308891084163256801582918312227190070129982159371032
106160345902104087107360558988783354566381003236203996899975756626785633172458
11360121415294234673492290282995674533622285810999323182806650167652675499777
69099004599843108968414793583629619948037191467364092751102568039578918506307
110656574355523450656832086051825769677016013981454767014910378791459013891568
92029269618473193271795474056147796411548977538934653889338363359956847692245
64823294048006524851531580960747460892068337347436472435451890560809977445117
100236966702279298814906524681978989331885625170455207850580843428257726491371
106421278191698457176200843167201122428701713546225202084555520544041274587809
99315131230202423442385414547336837748681336953625665856982728672951509208197
107421881758476281241163942154027279478812520214085857804679018225682341035526
106019210940168173518606754683610743289744406769669323118069461247286878532088
90416212846821346717124535820834669144023100751724246380854495445426996951582
68477030589118854188004896027879588941382909858200799752593052484655009431303
96844122781825039231559816285939060539846670055059654310043659068813547440551
90158789066363491655904920944024309770413749534283230344952537950180381173035
115114645400421203853851103588569584481968395518935880830106552423450239049403
91113993273685483286082352542845419004838015200871481088882318069381945091745
60658918544444609877354302609138278489784918477942509372876913645387757996857
101361360605612254128928602421283903269238966114561587387086647591616847586422
62235438945625206224925609720057856303643317980184980090171410119071855478933
112242950888124059622199552255197943334364616250989826892560184005913736182275
111353783993784885757095733305440198308610868658789574839684453538490692076349
87258359763801780436445349966930604896003118990793124038864852723268864757052

58242378551651964633682197124350574387294363505216107005507034195118146783428
60186008865239819235801143417968127042199706908938653866771235823812214233166
76092217080523813895015788781574295611713155085079344098520551318959662507237
74191090622621815847301444113041600309148077215243518730957410745344954013855
97591143698020739476389416370095174408188339110036446003636243812863683608328
77930281641587885641490458833484631706726880900693567625969996751803830595025
10046704715827950450159113413056917316238988922378340114186329468511242740856
77499034770384326092450889641322954815105598687484864262018997257497812077953
71975659046586849588173238131850111145216415584892322233474204108188697723533
85857836197012628782861713310900445589527267356623805588800102345694893750433
78699900176984796022210830053900656661230174501147893946129405344189081412363

```
A:
e: 115792731926690495505992592175973672541639217300923788562038239326483005397616902623284295944247004132702765150188645279
390055756050498895420970715935567
n: 6478035089325590447047910733535193965488076301554843961861654772959054291418677170014186573308721535621002144174974337346
228912694098021319248909353115351
d: 3264886969863771047466967531490985469090200193797048016605093079805461414131856827857578979332346250863267648826728637609
108979718790252157919309714144335
p: 91652799695418215218181745839946494019442655059428659864183627284145613525127
q: 7068016591804594656182229951614455460509321201160556021760181131856885688113

B:
e_1: 23966298142872694469895536312305905424984184602990812775426299979092698544307040501392636664407572274027345924386357703
75078159655536023859665707191078835
n_1: 824797166065329483377415060076979289607929681440494957990009596892822692335724008671005152676928976497668015189264137
27764033440723944041511371184745541
d_1: 32495809830793743588559253416610507945061281714904009594787225214054832310420837731166030610950569263826166852382144240
32435133810845456002967555826359691
p_1: 115447999078749380501892850639718821115849685043158542585431054647852126152503
q_1: 71443175511662086244931447648331059716012181100361281925026527416003429109347

Start k: 3194852635298059064100247322181926663852483701652409561388949758186706134047104293389774889083622347317481614912576
58023563484586139528983486919483208543
Message: 5292834498576892026659411350775349747309952295635249755965305617315316199493447410262571019597419769195712946729954
839321064684389656843171649144825421850

The key has been received: 3194852635298059064100247322181926663852483701652409561388949758186706134047104293389774889083622
34731748161491257658023563484586139528983486919483208543

Encrypted message: 514185321221095190816335760970731459609511250140936512252861610733059508713197630239517916489831019869515
3834132252717892459259068255907312283113624028749
Decrypted message: 52928344985768920266594113507753497473099522956352497559653056173153161994934474102625710195974197691957
12946729954839321064684389656843171649144825421850
```

Перведемо всі значення в hex для перевірки з сайтом

```
C:\Program Files (x86)\Microsoft Visual Studio\Shared\Python39_64\python.exe
A:
e: 0x171fdd63bd06fa505b1c2a6527ec3cc91e276c41118885770d41c1f8902b7b500575f2cd8cbca6c3a3fec97e76b3550e18d5c5f51a2521cea20c256
58e47a39f
n: 0x736af06c210f0c2b54095338ba0d6dce31238ee40fed2885fab96d3f7858eb9243957e4469d3a7c2082997ca375033551c4de2622ede82e5710e65d
b132f79c9
d: 0x6b5b7bba1f02f680aa6b67aa350f1e67d08860b3973032325f613ef80df0bdfdbc2356f230625486985d3dc526001f309d5479e8af891a6c46b26a2
c706419df
p: 0xaa6d54eee21134de524a83c223e7dcf646618c1e54fa9f6f15b5a17dc0736939
q: 0xad5eb7140f7f15fec6f683b4800827dbc70f22c6e69a87d461832eea45126511

B:
e_1: 0x68340064f0411f9381ac03ebf56b98905b61d15d16988cee2c6bc360d327448737fbd4c22c9c890b0e8993eea3bfe5c624fd4d5410e01506d9bdc
cc5ee452f5
n_1: 0xa7128dcc287ecf04c1540c161009d5e307dcf665bcc55487763f71eb906b4d41e7411353f5545dd8b478dd79db5440037869880e885cfb48a7fd3
386570f55af
d_1: 0x860765df9fb7ed0d040d90718683f93fe704de7f1874cdae621a23999bb0c6d254c343e783ab5094c10d6a9388b2af036f7103602d8623c406d35
4b01266f0e5
p_1: 0xd21a41d866bd25990dd6f1044699964956cd0e833b7416bcb259b43587e3c83
q_1: 0xc91e37fe9fedfbf977b4b367816766f46d06ba7bf930a48130847eceb8ad265

Start k: 0x6d8b0f5d3eeacf1aa4a222dab47ba75d2eb2a1e11241d52fbaabd0f46a6defc4a32afbd1b26d5f8379ce6d90158c5a17115abca5dcf4164c5
6b4cd0a99a61ab4
Message: 0x66d54165d2a2cf4fe00181fad5e0ef906228abb643ce0f5c75738de651df63d56e13a1bd42112b66fd7ed8ed2457efec8724ccf8b8c12de78
c25050365a3f984

The key has been received: 0x6d8b0f5d3eeacf1aa4a222dab47ba75d2eb2a1e11241d52fbaabd0f46a6defc4a32afbd1b26d5f8379ce6d90158c5a1
7115abca5dcf4164c56b4cd0a99a61ab4

Encrypted message: 0x336d9a5e7b55810686af93938b16f4c1ffffbe4ed0294c53453395bf80a509bc3174e273fd7e5dcf88ac41d899fd040e7b7525
2d9078d9f407416eaf8587728
Decrypted message: 0x66d54165d2a2cf4fe00181fad5e0ef906228abb643ce0f5c75738de651df63d56e13a1bd42112b66fd7ed8ed2457efec8724cc
f8b8c12de78c25050365a3f984
```


Get server key

Key size

256

Modulus

6D8B0F5D3EEACF1AA4A222DAB47BA75D2EB2A1E11241D52FBAABD0F46A6DEFC4A32AFBD1B26D5F8379

Public exponent

10001

Encryption

Modulus

736af06c210f0c2b54095338ba0d6dce31238ee40fed2885fab96d3f7858eb9243957e4469d3a7c2082997ca375033

Public exponent

171fdd63bd06fa505b1c2a6527ec3cc91e276c411118885770d41cf8902b7b500575f2cd8cbca6c3a3fec97e76b355

Message

66d54165d2a2cf4fe00181fad5e0ef906228abb643ce0f5c75738de651df63d56e13a1

Bytes

Ciphertext

336D9A5E7B55810686AF93938B16F4C1FFFB4ED0D294C53453395BF80A509BC3174E273FD7E5DCFB8AC4

Decryption

Ciphertext

336D9A5E7B55810686AF93938B16F4C1FFFB4ED0D294C53453395BF80A509BC3174E273FD7E5DCFB8AC4

Bytes

Message

66D54165D2A2CF4FE00181FAD5E0EF906228ABB643CE0F5C75738DE651DF63D56E13A1BD42112B66FD7E1

Висновок

В лабораторній були розглянуті методи перевірки числа на простоту і генерації ключів для криптосистеми RSA. Було спроектовано систему на основі, що кожен користувач знає лише ті данні, які можуть бути публічними, так само реалізовано методи, на вході лише ті данні, які потрібні для реалізації. Складностями було лише перевірка числа на простоту, але вона вирішується тестом Міллера-Рабіна.