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 A і B, де (d,p,q) - секретні ключі, а (n,e) відкриті.

Варіанти p які не підходять:

1052825857005263472733605821473713228513368594259321177951298393374440714674967980892187991791231280559712031735254521926905127697803131677093512846701785610634806854205734592129608370262432878197987571708335645760864962737742316316376023505646271033009428187436826317299709207769723849617524141369859561093335939779244928721908411126000069389689440893254971388354789901136782286710645248997295484177293416354660296867341104763168708776552837195526846746959753263787426917740949823729911572011833046789131289016788827997168525999870308766572794358125746437477185486023231860249816154166662305106760217956792295791531086134626575358938083668328863978512301697195736786527436888336378927894515191084644045953240153334004727913977951430324787659805782645622663457392510037897680738363887028313628978347253176245531969611471645492895576804795163148489110256108137933740245079139260959339710274931323817592476698305696999766569889363789527449358916222471346982878789938685696144982977347232125793614628875613979196712900782352621234495415329790965468421137563888760386009536512032327245838710329160764662244409839767378913827196486597999913214798353688566325194983762416738446021228170325818945123136195916620574959335346471851754422769830109037075072271328693824324555556752112375981900312641435754406284709886169967807248435723886604072889016085822364396319191448271553287388646190188677427897840492502911996284468521388098352973823120154682623223770299646894830256820484902608814455752830570528726038945004583108604525955217438221108630394573042580973252386332876338958387966885007033649074285549708314201805610459674124597507428786911027202092618020081603644273423024315989666221730117668264239049 9

Варіанти q які не підходять:

6047838429104088994237882947289285515998962480119805934757546720248055286025260368403141870495860511940089658869786487286091952516099743965699550949271860978561842938964741643766205992083425007763161715792313325708551687213851832176203149501377656131886295501302250513789541438331697412061862158642758034759262098419943503463087577816285791701609808450418973910355316866398294320614007596415315991012716946307647560032654341635619982276694870977086181425547803958108414352539993866523188113501618529373665851670487845567736474611732876430244640335048759059164440005761389311265760443479657120343089567183373814030164781115143268800820423717853145139548712658446133103569030646021833843888000462507702675660225981548030869876080308874850338227901431002368043590041055269468910635553217396947016522327201226496042553834050483480370612921490307233849120558662156546625709334229556590131977487618882408303080060349344144743203527330

10394721545786874753394392385579669765356729623156810070821376481714780860838
85897871731491222049109790306410588644579514966632014934122216214287293248820
11019716616353020725435790227604222676443741846006189638440078600175459201392
91600677539384878489834818929509346166516166520234420785853189546690244039701
98468023829906164908637202797311304959447911371580019687821034162440145087073
77665723547888096539006097117426600401141838496782928108022146842403066456147
11399424061902773630117745548574626799893848671886233453697872198882726633335
11550124576780450507296218047058599789336632243712073392901295697680623729778
82643732947129520834019861876570977408462522115027627479240969040718515977555
10669727104568195966955014974086976270651412706916103938517628586086140224765
79833879945807248999890653458419676998458445723397610565203245006807557448788
85687547676529979372009847340904941393397555101081381165704164805672114503284
60170738422069567825585638463080623503933903903962578016890194755701552554430
76675812984608845556594461857066442197034068884382336139080219806611866030363
64561392162767359380467960753553177639973817639626099462181981008451280799534
70939365080073550481513719810954911443608388739213108835053116438888452726777
66593830061031126689329631928311025313067468628830603545192329996561043737451
96397188354515968580970039687078182441128509338179880208998585007282029498895
86689002233443411842178598634959330493015408643468022278822497716059493630465
77122052497682077508463570022762485209810016056301574464672151834603238811376
85905616465285866569678053933725196812625469534383248795757977435296538804350
89511021075200589983594554216968697602290220573840573654670959436823460889489
75202232666396216116370599288098163018861032624390379664750874491687904205063
11452601570703729236880330410968903869881027882548735878632523007922956818481 8
92299183271250340594077486633204693752009845587845880255736943337417440126215
64167288056015438308409378079371039992972621925310251669579036077872870916209
10124262564093226004341442099093906821594705154399693974437263955865808138412 3
79016559159067726053146645758523829562257079928436266649275975079526910910183
99485724451237322512114864542026686650240723096897768912404316872664477467451
70161634180248711757130880413626261267543485720774224533868532841769193436313
62014873266058165151431064270059420217225794710163291876471498052664371996186
85041457537834469299539809886407542050743675080385008373072344411027478156232
84706122112633383556816805158520701448774858525668212788374174949243249327112
75045661925518609888583748677503594999486363378443832614567057745032708684680
87613141984145317240939748257995136631306327874936939788798356306710632955271
86102691225497667910982675410236143850888839135757298174553475569178775805507
82172093146938987298884668286215915458876177668273244361640847108958811606689
10680802513491533802389343273545587609432811694412866843789757015039159576734 9
11374313644016631527682280886073675691499240146727147255831547072342962404322 9
88950433666532429040361883053357884539650749969892855741094840993396399881698
92667734485354161158069520278493259100298959888860794096587123622670679076143
93211256181310586547561568197457933258199900183486018013707660212375851878412
84518916712992449027038496483193917514404125737668450388178284919085097843706
11427868435573903528000094037539961780941654270399204081145507085449763182084 0
96657304841663833885485342882881561453442241712876769748256903123979325721654
92434265856920508567586905599378604617924707876051906865234410230634663592519
91832955083976883089525118132347403004160576131133926615073677565184695503840
94508541491666305885653775982665192180611173004353820941460070923725148964895
75348580685825413970065432071058990737735795019349246190154421213263179140523
87066433097184472017316606545346756208930036318739117984808365949970119482912
10270093837896386141417570215255727721892794192818098719253001935740710214311 7
10234069816074048449184111527267650330358913303553222824061187143345650710285 0
89708734609774910872131405528051157037327874041836827357736940610829623003922
82542716491495874724656900613450411743958338107130366052792598549398032574838
98185113303044799850813676915355544431126836922219400874956245608610243949552
11314559378255093814121277985750209807773549412802524750494825007473845488286 5
83016423682522170390014762244748190804822223021065181702517816459946267424792

781082847945447395104551693600953213873307576809299572657184096991132690434829730400003653876397959352251046106906259681743627848908458980396354385590023686557212017884917452645638790238302231012227577145709774671011114262007596842876921021207559148065214756640264606687551343529865623918515451164503772418846734445866869307238566056320513749831086419162242684224189974619340345209568884038252053089330499904266223709374530433877528993384101834315019079464720926760385451640462859011955036807764922238105807383275582966765641756014829095827597636628841190332177122105255018517215742825884201842054547783310799933715010692145760202031997629967886424837645629103447333941464690091148644389802461176240955555559588641570071385490690660290879809693251720131348839387822947432110986838477725408202117212390468228863852510995402168000004281972098651765667950325127627746033134773888768951672576872979926925733492631950842258069392339551658888669425558222076617870511120917481858607076030280530769182391573322588391369901483195581053719066017934458541968211411919017915878185140658629086589242829854679628213647524313942494358731959626257882396024844698627352508706051388974200769980491553157960367945884071321236068723575575843245384071574886211628562739558099252567776941889087253173259138458736867863616875768954410633348631784305819831440575016104064618316658200186817004838105828883352557211058696004770901649560811500204021700559285235359425711287586914457880935486666668451446267457638356816803047199191414384202853815279261195686143994913421052750234768068122654079931038831015200208524906725611893589622089024057511715947027076802286182984859384673435253481239187686225430220689327079510264942411506333930643003257394077235868718443136752249077113157904007896398161341090411238224719262512992656797419590352941301755481853165749239656891515461939738910404257065944391207718340054312974640003203442382026391834782261742745613147311436551120056818054061703803415339833059436516402882461671385078714033547696377661661797298339722298869910005755915037304084622450716815093741917044142471877893154464852591472242966568182876383579580737086364826241592141856531484237581357877137272775265144358464606214489429123064569456946192721332203000370589232087128389774077303028367659183911474808796884948165728355571474001877810798164571630244987532161749652434251382570030473754017163366472728862921597779760761096619295303231344557693688427843276030815952773666102508635046445434971147247895004387755848399444365572348562444967834662984011342577770461504394488500407708087168221916789291625258563311724682261658543287162031210757729641871198674767682431808167090488697103572357106532439190680120631932179642244953860451676081210977094693895011114099078252833826039054612414507009508467649451021008153260671589878075028723541242302679658953212738205393284738838880029887213503727513521548210115238317957270591110724087756493694132462950960016845477931694580690208535929969177899476246579477700415713797323808932326101796686686269461508360468443751262247232346382037107553137094702713629219102135475908471952803580749616272280495875870322186950785602709485004680135727742536892510733812835061827639275313205909277303814550637593936274474159141457378205380168207376978636302645496563020585883730912569492492498277042062152482543205511139080023442244315442804782327423271947092440975532688483887374177659910685467817191041313500053486002854737572189541717393096801471715579346325378747223584971150388054372792371366362326863628115073675231193789413436658599762331059972174937081418970734248568883234487728735852590135689752173545592813753722791145051028078615976884724657373690293206680422556503721660673333681509446159746438810471760964835375079170024630919768184041082702201606224617040385427733810461053718782386304039934195084990831305319545499910913477562478571228011137567330170010395405216428800516585341873096400509711868063420221065164373820127114651285318064463134980071631276876967265294295342879406200628584722824956632105500265930971463627790265623268730289674739291363551211181258278399946555647697248107639870643803371547088228123866348141751927630815929881948598191275538296765754915494230885042962690636454848237389883237351481913683507968167037487440597849474367989141312563843431635144604909644955076210447425668169908295583347409615230705189904790869217981991346602904702507985895878307358338677961523070518990479086921798199134660290470250798589587830735833867796

845824633014352805298920749021580737402183875960026304551812415342291704708046087819083589082333384968956370978160571643746036040708764909294935820643539189516846695829628959718861865029111763463603302130790768986079488363533455296100351601964713134303592051096170641232604940818786435314299408354597488748644932022148512429457371394821658653007348027212802584737035709504846246552866319937914162338958871607953428937595935407663243007589985960377980439350038048258552758932470142155784004806389205507201966110110352746334196816198023666804795485513392643912063431367467930992928756829294211703769958589887862415349508178269517206752899862835153536908298510169274193965230065838492378745218840273906325876702552697248364436911509789992949799173640200902514335542967551413Варіанти p_1 які не підходять:752371482500977536999882205496262498957603937742051205211844396155983079293357854369234903771111634787726132319358343865256619629301036024432677553926870210156627935941215255449720633516327538735896052086355329842798633766614908991987389098313632236577378780028353522524862752981050483367268293329598095809537711269589775072251525782754800873244543659121169075302168941427382540610460627697732134790339364172732956667375863791052061579071052484461563329254453000949755022202986419540694565411768510016252084370378434718664238007284102915509959284127183863950105171334532183805869201487642144895927889431792943932706512880379052290490348480245838505480044315968539108468827783837709832938409656751014422113895860712105296775035079774424678603308911566823549915694494879483876308962023600755259033600972305125052693170443048573752108783775685904808362160014998142302228679129715523527090789372919173926861089483164255744886244566814195687332671118342764548305769854966420618286786585078000851957226138333068291706944953097756364274554007789998491368742149033114588496722383651992364458320182770194585689440218005696590181151689581926934178947518686556367237669756823671054046362071469062686196771878556646778176559470743603995547109374267788947782097117189224745701368275069435739911132887766654669228321094218187859471675170314628750037059071894775925011050938667929390060797724112004871435720722123518010110482083965146108107940692903317222970501408739190404717165371123793157632388314372712160027564317406989275646571585740213960949364905717909504182999654401619094744155185705557544848919620250905122326749410797578124110847945746039663399656273652712052619899862569208055744118594026574241661086083440508107811513298676303033744785021274144650808620034513065335752668135159964888218248873243186956199488329564125674447317197812312299095462922201725481041934327890708752432259006874393079645395134750008200537523637858101355117736315982485557372324519609982151250491958446797654046742470612966858202508376458187238273331238884464009818536633623544624814520382280593379030751175726905687835289010598258662003285113530406240358633670280199845987983245534985392948744341684459358203168802841397763950917448005635132097380412522409069721861888954060142601117481518113019812858828565117438772921942039882077028022340066108380611906762156878889845387827975390067573251421794091489503765020266665150105950459190708766025693262949226961572867702347094282450645744342602704308142978979931305985571085661485886333001598741397629607005777240361328237259540051112652464190416179458675633038760455504226703141498435611267932238715333451488289403694873548663012011287037636988744767382880220268680225630160489314454570676653350516193580753381280150823313693454107012434448049817320395965054197106545463925146035711976510185472804645691275366745390048004676782345504284353104086211235525766345801322834127024839748272048652216615954710120849815923200905444043776342344380477571464188388171815238625155138182511708068833886081201091724638624698172592508537145588650448345926571848432318154089138651393391619413142912658370614597617043310045729052887027155149769894129696821600148332311521630911603821937189402036214744202177909792732103322947536923196813810501295393510489436201432199040790417767277715457941290717120130895715231651293190641747307900106887042124116951393679499046987138725437583079861714650379991108726984421499606895647665918505402227652648521306431089106365649181005062547 7

7330169724983448570922746260429892319449439871929807137924467946179885815239 4
8967513332921476910295339217804758523942884589608338018026701354809389281807 2
1099949748314150930401119434257438627892731858946837133944633160277184916719 11
1024410553770398024107904838778842266088428382801495817921487294421163601006 31
7437158102916009756611105234947549414026702478175650506150475514286502593202 7
8292709945490569495521200329560086544006248516099840282698785045274479853873 6
8826574323345920076488148292362123323160240338541019040003809011422784285228 8
1014065536100543276113804595264474052581041740031449120554815839446558931662 29
7992196367426537369150355374849145494728464407615111086807816137109531462419 9
9986565429151159567402656922626190213432005422358493622637445027800314133882 8
8797409762613380370350889001870843357573799834079465809215866749653646625947 8
8296627443524548604080795831217724676361446606432950874611222715734042321788 3
1034799560165361277499779705603988237709503917695130515520523871575959924309 71
1037118373479319640168855372064912339335153899877648725513178882200512794555 95
9578688840989911679675341419428637925339915896177211681795720360449505549646 2
7781313415547622324149290803274190439190422997961183171135468524660419670698 4
9018167238512376845982835208597316595449336509689205379831296036158844723749 4
5933720743938433076994303646460878006703703431155234427794266303850481191452 2
6651119895467914547771947726936897243782296019194997776938235459595757835769 7
8348350914632603117740813263245311407714010378070606158460006703132623008684 4
6623222679597058538505201141684336865989120605352799098116629131162710209071 2
1135193682509543792544354381252261516955249614173582246601106101631562957917 68
8811875615097438079650617103465450790396532266546766400884227144596514634668 5
9429410383379924638148553876696979738468830130195408519066985428687775905754 7
7515312239904680772343548195338044092013710205737509698955311622910247234728
6213988948150532480619841322764336830722045850044530847648666198701420481682 9
7933932327129902130883047589500838751834238768795198628180568712310379512460 9
6006301411141091878952835401543883332566510378730279396350912978454444869974 8
9714392943993969694605655850154172519253940450633791407881646131951600811077 8
7026756833017943467221458559451571183125445683037962607365288338585522476998 7
8149223173149008371627312190656710156682180643478604669384874579911613795918 8
8565792465295555105061604641156817162835715981220670809701855736414245676950 0
1124965570280300078944041468168811909299384500990583156159605316574670687597 18
7798920090819659049298132198325609986157692000453921066110337172379316119521 7
1013385781596316178553947049987892337692593045606484246428153350839378693160 89
1075008199889388910834506812934511437106636036816602139242764377995886114825 32
5999455116836867795786201299748508366814380523173648385381577987365654522898 9
1044330156551458834733093545159781420829478654336341891379543736499083443170 07
6524067226234595426453063097715677044924220905929393536720650962578630861901 0
6024940510758317761107181451242699237185922714234535360074209240788869558034 7
1057950577656675845818267182860367061632349377471285010008056915346981815389 73
8414551831979832666382489561660426847337953328934774000391577704245343604927 2
8000429207810808508302711290730894710435140717787522519570461995937605772436 1
7288586663544189663848276212981109901905943465597893502819367495009887295959 1
8186786778174516879421286496501437411243582061262025975662002042285860580660 6
1035358075990827623344095615218028480282630954307192967810390155391835674931 73
6538754421995379216712487834786426991968491425430183511000033360927817163119 2
1085016908579843455318907930260143997782407571038494323687345352937174943201 54
1015639956910404166780555684316395093158110864322118477758299382818267821012 66
6079851182196898767527681782039667661750625968211475925493710954030925249275 9
1025257829228215769021685490773410088835756512101347961106959492810169989549 41
6877599191708643776198606445349769129512934203924267853643757174722847954429 8
6222698987899789992915757148212206444826704189356637324478796762339465012020 3
7366424085458140749670382381189812206456291849343593067361790008383823681652 3
6457917839719682706667428218628702486773282564877846209653633281110138927037 99
6286242164976384371967880822192287876257244501579625614227503629200934933263 2
1074097979527902668488874617902977256481681451043650108797336930995227601330 14

5906071600603400701995101537027746677243717602969032950033752881662795512855899104457433076604013628808265800084348146580655983349101287310332832069459269819202816704478533211411825339124024795188933663384920413842949026175134562098467718601140365750468621378142226772798037343976246464639001374187588865713299799794131864474073844290665790689519158199413221285662253782502361869365302839965657192745545200362460379188101426045049168355856182212077685628341620906526807003462683393708735619616911419028172086135379610150490024695656719575104629833970873561961691141902817208613537961015049002469565671957511029866347474117891610550544039891840733331713404237812942810981736298616784799854463173215425285776611224729125380398807691264012457230625548914619587608682690391965771631576792509597865587023912366797767260516513863841658933146115

Варіанти q_1 які не підходять:
6443854177175821237514724070622001226909593131379734343942755794545690418633296846318634138602370129130602129284466313032634401439822117697687876929197002593091216122356066027750134610042127348966485515242535455445516966954401699932272338264902399041067701509164261446208189995762254064629439798565397642126276297980134338399919548666643146539076965910034854467397631932414486495908856103297906212123965455465333319997952242483722080734789269286540915216306010979845934256994359139914847673849092087858921330181953987378905852217636037170007156224105543994967068590995028462947915198441563503071561582149316652393713478800038294546450169834562610668887673083615583254388003604780959002460165469101355819541428453678207760017241861296664635742391370904073109951805616800480967677956259541811234798121346061870388332336319106716439810917652210267223981062772630478552120503200885409010977596502944923378160560161718161108142890659854669799620412364089281673446712744119103790091243212568367412626142931578911109481200325456594487261857113311411551580000986238558436859055653237400299111064317900936318205577417008119723744661970473795567369973377422246537592368495459755427515624934174694848036987942110523152465609618091475438226655472847100442055633462633943600510769045828628659477693279439458138651690758798237695106456188737141069528212345082206092920700579582448345863293047546225917127168110763947137693371389413943472348079355044188606539174504937140072442936648580781766774931412193158703325357319563971049651425540893040436344195761877660101126391327023128771896286300616546428074771242656401959749870557541625188694421126332670063672552345092923088910841632568015829183122271900701299821593710321061603459021040871073605598887833545663810032362039968999757566267856331724581136012141529423467349229028299567453336222858109993231828066501676526754997776909900459984310896841479358362961994803719146736409275110256803957891850630711065657435552345065683208605182576967701601398145476701491037879145901389156892029269618473193271795474056147796411548977538934653889338363359956847692245648232940480065248515315809607474608920683373474364724354518905608099774451171002369667022792988149065246819789893318856251704552078505808434282577264913711064212781916984571762008431672011224287017135462252020845555205440412745878099931513123020242344238541454733683774868133695362566585698272867295150920819710742188175847628124116394215402727947881252021408585780467901822568234103552610601921094016817351860675468361074328974440676966932311806946124728687853208890416212846821346717124535820834669144023100751724246380854495445426996951582684770305891188541880048960278795889413829098582007997525930524846550094313039684412278182503923155981628593906053984667005505965431004365906881354744055190158789066363491655904920944024309770413749534283230344952537950180381173035115114645400421203853851103588569584481968395518935880830106552423450239049403911139932736854832860823525428454190048380152008714810888823180693819450917456065891854444460987735430260913827848978491847794250937287691364538775799685710136136060561225412892860242128390326923896611456158738708664759161684758642262354389456252062249256097200578563036433179801849800901714101190718554789331122429508881240596221995522551979433343646162509898268925601840059137361822751113537839937848857570957333054401983086108686587895748396844535384906920763498725835976380178043644534996693060489600311899079312403886485272326886475705 2

582423785516519646336821971243505743872943635052161070055070341951181467834286018600886523981923580114341796812704219970690893865386677123582381221423316676092217080523813895015788781574295611713155085079344098520551318959662507237741910906226218158473014441130416003091480772152435187309574107453449540138559759114369802073947638941637009517440818833911003644600363624381286368360832877930281641587885641490458833484631706726880900693567625969996751803830595025100467047158279504501591134130569173162389888922378340114186329468511242740856774990347703843260924508896413229548151055986874848642620189972574978120779537197565904658684958817323813185011114521641558489232223347420410818869772353385783619701262878286171331090044558952726735662380558880010234569489375043378699900176984796022210830053900656661230174501147893946129405344189081412363
```
A:
e: 11579273192669049550599259217597367254163921730009237885620382393264830053976169026232842959442470041327027651501886452793900557560504988954209707159355567
n: 64780350893255904470479107335351939654880763015548439618616547729590542914186771700141865733087215356210021441749743373462289126940980213192489093531153 51
d: 32648869698637710474669675314909854690902001937970480166050930798054614141318568278575789793323462508632676488267286376091089797187902521579193091741443335
p: 91652799695418215218181745839946494019442655059428659864183627284145613525127
q: 70680165918045946561822299516144554605093212011605560217601811318568856888113

B:
e_1: 23966298142872694469895536312305905424984184602990812775426299979092698544307040501392636664407572274027345924386357703750781596555360238596657071910788335
n_1: 82479716606532948337741506007697928960792968144049495799000959689282269263357240086710051526767928976497668015189264137277640334407239440415113711847455 41
d_1: 32495809830793743588559253416610507945061281714904009594787225214054832310420837731166030610950569263826166852382144240324351338108454560029675558263596 91
p_1: 11544799907874938050189285063971882111584968504315854258543105464785212615250 3
q_1: 71443175511662086244931447648331059716012181100361281925026527416003429109347

Start k: 31948526352980590641002473221819266638524837016524095613889497581867061340471042933897748890836223473174816149125765800235634845861395289834869194832085 43
Message: 52928344985768920266594113507753497473099522956352497559653056173153161994934474102625710195974197691957129467299548393210646843896568431716491448254218 50
The key has been received: 31948526352980590641002473221819266638524837016524095613889497581867061340471042933897748890836223473174816149125765800235634845861395289834869194832085 43

Encrypted message: 51418532122109519081633576097073145960951125014093651225286161073305950871319763023951791648983101986951538341322527178924592599682559073122831136240287 49
Decrypted: message: 52928344985768920266594113507753497473099522956352497559653056173153161994934474102625710195974197691957129467299548393210646843896568431716491448254218 50
```

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.