



Національний технічний університет України

«Київський політехнічний інститут імені Ігоря
Сікорського»

Фізико-технічний інститут

КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №4

Вивчення криптосистеми RSA та алгоритму електронного
підпису; ознайомлення з методами генерації параметрів для
асиметричних криптосистем

Виконав:

студент 3 курсу ФТІ

групи ФБ-91:

Швець Максим

Перевірили:

Завадська Л.О.

Савчук М.М.

Чорний О.М.

Мета та основні завдання роботи:

Ознайомлення з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA; практичне ознайомлення з системою захисту інформації на основі криптосхеми RSA, організація з використанням цієї системи засекреченого зв'язку й електронного підпису, вивчення протоколу розсилання ключів.

Варіант №22

Хід роботи:

1. Написати функцію пошуку випадкового простого числа з заданого інтервалу або заданої довжини, використовуючи датчик випадкових чисел та тести перевірки на простоту. В якості датчика випадкових чисел використовуйте вбудований генератор псевдовипадкових чисел вашої мови програмування. В якості тесту перевірки на простоту рекомендовано використовувати тест Міллера-Рабіна із попередніми пробними діленнями. Тести необхідно реалізовувати власноруч, використання готових реалізацій тестів не дозволяється.
2. За допомогою цієї функції згенерувати дві пари простих чисел p, q і l_1, l_2 ; p, q довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб $pq \leq p_1q_1$; p, q – прості числа для побудови ключів абонента А, l_1, l_2 – абонента В.
3. Написати функцію генерації ключових пар для RSA. Після генерування функція повинна повертати та/або зберігати секретний ключ (d, p, q) та відкритий ключ (n, e) . За допомогою цієї функції побудувати схеми RSA для абонентів А і В – тобто, створити та зберегти для подальшого використання відкриті ключі (e, n) , $(,)$ і n, l_1, l_2 та секретні d і d_1 .
4. Написати програму шифрування, розшифрування і створення повідомлення з цифровим підписом для абонентів А і В. Кожна з операцій (шифрування, розшифрування, створення цифрового підпису, перевірка цифрового підпису) повинна бути реалізована окремою процедурою, на вхід до якої повинні подаватись лише ті ключові дані, які необхідні для її виконання. За допомогою датчика випадкових чисел вибрати відкрите повідомлення M і знайти криптограму для абонентів А і В, перевірити правильність розшифрування. Скласти для А і В повідомлення з цифровим підписом і перевірити його.
5. За допомогою раніше написаних на попередніх етапах програм організувати роботу протоколу конфіденційного розсилання ключів з підтвердженням справжності по відкритому каналу за допомогою алгоритму RSA. Протоколи роботи кожного учасника (відправника та приймаючого) повинні бути реалізовані у вигляді окремих процедур, на вхід до яких повинні подаватись лише ті ключові дані, які необхідні для виконання. Перевірити роботу програм для випадково обраного ключа $0 < k < n$. Кожна з наведених операцій повинна бути реалізована у вигляді окремої процедури, інтерфейс якої повинен приймати лише ті дані, які необхідні для її роботи; наприклад, функція `Encrypt()`, яка шифрує повідомлення для абонента, повинна приймати на вхід повідомлення та відкритий ключ адресата (і тільки його), повертаючи в якості результату шифротекст. Відповідно, програмний код повинен містити сім високорівневих процедур: `GenerateKeyPair()`, `Encrypt()`, `Decrypt()`, `Sign()`, `Verify()`, `SendKey()`, `ReceiveKey()`. Кожну операцію рекомендується перевіряти шляхом взаємодії із тестовим середовищем, розташованим за адресою <http://asymcryptwebservice.appspot.com/?section=rsa>. Наприклад, для перевірки коректності операції шифрування необхідно а) зашифрувати власною реалізацією повідомлення для серверу та розшифрувати його на сервері, б) зашифрувати на сервері повідомлення для вашої реалізації та розшифрувати його локально.

Ключі, що не пройшли валідацію:

False: 805856315524586451547607734791707122206167976225752295623304396756850960158565
False: 469769216349145593205671597387046006155135526786447028308475017726910872431207
False: 1760738084594643884398355585448500530079093347104174091006132419175608383756043
False: 1757494167347079171368390455246599400892255828622132434653060819269521048230937
False: 704290565930823159778083253644115036648429397016299900215207539229500484148599
False: 693873776930927721665394572465055825137431346023234968940506423141723183162817
False: 1366568080665205214544774677347974933010038123261438040579056605301970030810121
False: 951830993987200816118884940640443371271799840117089071707010953004884027515307
False: 1575752285699930881257289462482917423727996193262713219224128198632092249917075
False: 461727220812429593200407184873769046596900827738241606806299803468773828256357
False: 557187230037171434929388235816291668060089814300039286388056574407125922281469
False: 1489264756976472849093265689162685872433348663863761538528442093378755344901227
False: 1349208022481790152564633728065628942351350122796621598594762965420700010736721
False: 1582696815440166582285138007039589596187881753796115339221654279715431404913555
False: 1103806610227330699954715214298214877824198290487951447382331573145386200314501
False: 606787911131420383488757179815897749978159331675015362355126209746579004769011
False: 328001964348915486536915166963237277110554862977315923048243750856210879869821
False: 1378910885253470816879632577363618071338121132202016123752782966593336982703221
False: 1519471187391201852724526639070342127433926322597171784846138692224211970270291
False: 1345941066884193925955293389872674230887533255521145770381211661844924283449067
False: 946003278639686264733889322636965033322798463728144539721721316871630170108879

False: 766236783514896819665858518139142124073333696784331368446202471321280866956631
False: 449165181706746301856868621670106962411641953241502503162877506768311083121399
False: 1467985131879093092737115549289919216928809038718626589435390913592725884909759
False: 283337095168232226807037741413718862516916231772344457454653364269827999414581
False: 1404935144087816239378043132677373428681440724758766435458299102404548418302227
False: 1581962703523666288045222069297916315143695468824290451049305433606418511405609
False: 652380673885386956251682499583630287787982662206036447480408770500080234276925
False: 472131138355353156603099249326564757071505289863889015057203648875474631436117
False: 1207233658705382498397555432424135806323610598513700433668902825599051860157939
False: 1618336994678152910926239787666537718738882243699373342258423105493800046607361
False: 1227602415887656708423611783678829225938719027064859919031569209968175345546979
False: 627447017540920876689302923950280210955373223895099166550178830048581621013797
False: 1001865243758698368518230977424113017674917407681556329290782599211470320960525
False: 471707871318701075666241106353760271859538073953152544741562497424180744193489
False: 1778925517535053977306862214755900831851020093899270277785766413765439028879645
False: 1461467465960134575048092983056592174564511980511072942481720663182742729221637
False: 1637296959991686549598326197018122649857201428139470876118926098740351057257597
False: 1489635881628018856445872453112475274302764808880184434180731692402940086457847
False: 613733065773894380415906082083786926166507526790326139937583039561073273522559
False: 555698528482381204081610767237401047400163711583594022487850053591675429775411
False: 1476790400438634966113140075755545920319528165989328978218535047163737210107443
False: 1672579361759331579995697283797307193358698260498599828116699983601297736042267
False: 285358554971128684166447225835015229020250565817454866090597091471812424289713
False: 1302369179955922711023629121945712582109576506092539774738268865764578356927767
False: 1389150346903063101183092603286194814299049089407792612054208469988298173501985
False: 323104261512669688080799335915071491545042302090966183045678730765938009699513
False: 1434623900119527122016665665510465797517749385615760393739756647547950913609153
False: 149814994312514431707361863434608084337325530132447442766024042795745733062997
False: 1437311355116901644234008695925328505881976311273732195220618685150425565250221
False: 653338237882614899881020682116221335202216625486722446547387534218807843799169
False: 1136700031909007880300616080968743689504111375192768873786594006011565154032935
False: 925191836004803684359457412657464610658919934054726553254694561219208738903467
False: 1348949161374532310738000957322964228021503110567486913454253339579761464041803
False: 507625215180801118544224450041843347133042393773143166323151743849048461442011
False: 1581504133075930897823688110458980739707800606864409624294652237072341362300361
False: 1487180847811222911354303753727798394272740831390432267657554001603818821476937
False: 605479150919600221703221195257304586779117304607703063474879005305796945675185
False: 506421588188986198265624487296471460960484783241052094477482324141592092517017
False: 1444546700312411420759054685417675836891331860743427487351059671578825189425467
False: 1746029255964860185876554713634001383010825112455688212893456438600342645657479
False: 1035779660308901867390516404404248132731053920628510245663375479941523604546339
False: 126028812616862468140229150050861025586368311416912453349918897014014147276563
False: 1733166389553755526049155083553921734302024637788376628009781689414587748099593
False: 817197232713229528199747394598570491130502862571730283866947723478098482970999
False: 1738236777204818810838546025309274968947409934825161509490390810179543996899511
False: 1720052070329595346994136658304318547087670976259941412059967256769967984063723
False: 540877331799882360129973632545635813004578792243383132644613033370495519246453
False: 1087000892699722149270233978452372943145656528320929025229002607070921325616291
False: 735878826982209333668259823391922164148423603143280858934988132325551712728033
False: 1516452532212543099262926875052378286655574219621700258745819334937167793265889
False: 1280048166866287121057976680564992184304029617044348938584227853316033931231323
False: 1709772866843843260779152937192575924789977553597718515884217258882585316663019
False: 1750905094667061976479660856463836068230093985712025405444704819290570139696827
False: 1093647638188726395701634455183993720546615409457341076757046868053701727135541
False: 1209683516382759973065221812470915851541201125700682058072693802596398091125435
False: 1427019883937683369123089719993180614833294655581442052421022281617039769421905

False: 968226380181154549005290594556908658420221354502991285947535508581093905653765
False: 1598008836080738374343889460309485434088186973778236713190704095398458480199703
False: 1151764516572080226554255059316025163862419097464506619814655414655399298621541
False: 1395634533287753211419323553817401520572598099504638288146636105098632603603451
False: 375178105089049759503472962373140461585411329674832339965620838700307648128385
False: 1054248840555957924933584183265504107462208892024024963995237124210892095129641
False: 1256254958270204127211895382753188926060958023513962638844480804621881516232825
False: 347290424678444761585189595856966503105691245560408883940870390855946666503073
False: 222522753386515534358296071099490571288721999874750579714690797200721993040649
False: 795683886784321634821199911687410056012706241390596091692530963867705433627793
False: 38878852671595849193544763231375556746491780009203187266860417205467447384947
False: 325119253967581890224247353323052871472770382739287650941641338297639655073085
False: 1607201476251334434044642464020953336391071169437147526405021375702379164398225
False: 1035364193118734256533721612069253666690319698078790466227886739756213348080749
False: 607830901773345968618693836039998076403235025313355815108177191847103619749923
False: 333617335979790117690833873218911658910596845756494898316629080436695782531271
False: 407717355775387427096629247212388018923783375490375377992694900331867292496829
False: 1284053810804724839840887865776424784960102370435774590151132275029479011487211
False: 1231010158444970299419528062151752844648855547245077700708628216091242327084461
False: 315476889728889971028892924657232038528715456949187122188902850176939062870329
False: 236826833126181645595273849606355979906853230205635597832538723452594165529317
False: 626909386610632002883435437482855334570669249873760622258574318507874687044963
False: 191800537379114363950516173711757781343033828560273677906815294535579227807065
False: 1514187415054394331967465715637807126968179076120581709368656127191959372488659
False: 737623284797143431662159555967529993866104214810397925970029956273045863358401
False: 1739382929558022253689108555503587583424593858439972950229873778597188026300433
False: 611070495197283149269769151737316037071566922980198336757433183670136718691745
False: 1831839642057232715083039449868828987274411044616473153344827673153785723710269
False: 1181840505032845785424984383621836979261538369717132909985669047343527024354745
False: 431511395682712860361943930405451423106116387503858397011016341740065967806355
False: 1345459810661106402627074874815185459060766083464886483983133228879010567494939
False: 472713790874342077703002176442089454303428264741776744740011751407870026354289
False: 1118551554533478877705809752272490641049661960542648054972498023353961188016709
False: 1817422302202254687295654371119909785750375432970574864915964257722754715871157
False: 906094126002628790033774282465914505768086014348415708450809918888535726084791
False: 829998315288569503434998062803698568916569018655796366339727633687850275856593
False: 691057983134700357685313715493950930918378299302934507383890734271028524451319
False: 1064871408503568617724067495456698610374649437510549306533894044766223904540653
False: 1730316639639130804971494580655006992201216075109600092501868925131482786601135
False: 484608855310366285458699861484005834074983609295981592654716525817021353514755
False: 791529700712331275087299445917629420123806191022532469184087391740431667313725
False: 1638572193082019262400635186150680357687033459425298075686345856964024662606263
False: 1012023039467053532336820210151636476954557354382388619967251602182646523052585
False: 1280975453024479362952189393259579637119486586585355375017433214614907091318043
False: 1113197907457230627724132688637932929387468448139411569660765062852089714858333
False: 1082744802924455284947964080764724384290198779826615750876373603022232801636189
False: 1851320660139421084714794318366512385114229633014321485510895162260873985511299
False: 717565325232317549981074244977620074094094715061700103291376722885757604793785
False: 745686784053734918796197685074384774945632867208692131312600661040078447785625
False: 467258350900000759278081793479369081734740353714085264525214842643980937819155
False: 1787105730729176058453703982485460988811366459743728404004217393508427279211941
False: 1753717902480399243844335568113156133400948153371354528428702925302824906024843
False: 1017056493703537913699004468336172067904953871090206248975922752461680432572415
False: 1419620840478169143794991279407388199786165612091324697562765752230561197744945
False: 629749429413647506028220883761185084690988454767883448930930692690201626541433
False: 1582775586033756190571734558421718730403286635758026249214730420359243266700769

False: 1581397083491690034703410532485749981730262836759932355190180115294605615764931
False: 1400511098005837693435361069194327173386220746386627335862752996177988843911755
False: 285550119344192876020751133583754893012235329264947031336751436480386406865671
False: 1343042592038108786673419501390329534511027934780904087538922803737379148257405
False: 1616373413483814910520613072357253900412859018228894753114602611623209170534439
False: 1525912473404071757734075803498154865664343968816169559358392371121820848390375
False: 949791354620338662904123668196084088136484569581164031009307824170264200995659
False: 1022848325438492383575683863721783487255143365833630818205393014381478758670757
False: 1195041612094158928462421544936456271877410832007539476715011778279348751422193
False: 580240227360050776019339130744028613427576815897527749975047457472954101806193
False: 1158912532779637261006986821869334429854725811307549724942807293945976338154367
False: 1482489805846739603038570685450752464576111884536809587084986049918632129235037
False: 266576281987801647906474874339857852837835257935492890049699284227643427905873
False: 1592595837433505843026411793633456019498862091324767968888784417156810924564683
False: 1613420023300115766690106517271677461768749174207253977501029298260001861526687
False: 165654962034968247253058408571194346076786581636733921317857636770645534793357
False: 393330448946177051748074732722334152913016072392804647382357677123013868464267
False: 974283408037546581590184795023691341536769039857141451336111865326871864078801
False: 1467636190642120308920102638224898257305746566427703602614562785118643324577297
False: 1201538626389775353302201643214870318697025376290479156869905071532199529769921
False: 1685884206391904159499502375865890115176848686673852279650740036582872681348283
False: 1344580166377415984254153123675311591972893260196214856070845201766340515651949
False: 177017941621358630463911390402200977563075602884166782413956871163999203742879
False: 481160972727265408496036380589149149863540882026357028333056680781698940636347
False: 613249896192221216740467732621865098329402507118952199392366246713781326995265
False: 835781434475589486226058402900394065626898147864252066432020715776910915676843
False: 794317976772311836170303279446833756295584839918054859474726718821012029221819
False: 1143283934013932061368845667437831176972123846654914748767681241621442459436821
False: 682591580708326074689387329153612111475705874717630633944025980141799432188579
False: 1730118558349839845104687920946583354570810387096012349686917077135312805922555
False: 1217129684696750714612402407715667866907453936517569642771251835838036279768699
False: 277100744060960139025959678302005080413566664109187346901141451103190737385929
False: 1807998210683777720430263311422374401925259316586997875366634028499519434518023
False: 1160557060819740565043247302770402909274823245535368075088364939208249953649305
False: 848771082905427446406115846712228593054870240887680115165495096260860405037021
False: 1166531145623630879861667484725490187107937149623808447620826215045210674303581
False: 417637627460462988950151302429861910682874661619992028602889487261040611435079
False: 183382699468780633271666934035822271569786188017522163142190574767127276170449
False: 1387565940351040280192811822133384661035801605810513032870376030199295933950639
False: 1611737547832877650326803282759506296995619769767796497368382209571140905396351
False: 1086030019787705529733799636927491503287344955251756540316370944874216883067631
False: 1705076587679228079389910570444008838756355131096623701631053886389091252025291
False: 1410816764791596427545441906145235183699647649954362266488124491456071347431341
False: 709639896670053888461987688589915723003971145750348962241862768896744541782009
False: 1306455446687726673789421942690328594524255393468213261301539462464876872905339
False: 619879116978139075933859931079784878327339104518052193964517956959765531708907
False: 971499389615400734420326535207190310472998632411170800992555352536309331152057
False: 1008660344046939878847562020483103706147815070052828363242929732819199681627723
False: 390825583431791972559011080894337303362416324918293266181989885358160879709599
False: 1278608300981984578021976225669976134697877279115243949185922836292155340305921
False: 1426691601332020514573835293874222348539179565618295942717615359995812867357489
False: 1685215269636494083010602623069107000147065606820905347193831451428515823385399
False: 941195775918407990965311022536727893258304416728519435954420159080421640731135
False: 986973731824883674551412573299909035262591390673007896767762807021745378330951
False: 1004361187990260691183420410482462159710964924253676302221568481161624202119367
False: 879579692624516364219694475227818232314486136953859661575702959115397199658749

False: 738355196142446545913228203686054692711187896976931885810061747145530495945693
False: 462882631059107914882400871878992593199841883018224108006970888181735119587761
False: 493349004544331854931943143483164752433090427138311098431481161874877935478661
False: 269664448907704638313267150150154725419176360174619679223289541083647684567959
False: 1662276308103346114407998159417269527396271039502263160938799111956719177895127
False: 496848062557927217038295101174370868694400424176550526175265848629557516201623
False: 302650119253261733772502322810866859288416169018723060907105711119616982163411
False: 170885106651899980411164213670570055579104227943634601912107708711658333937323
False: 1522002630297336485726768321622794259815473647479436814884589485954684956434069
False: 1660090759893853595460610674373072831665694802338330482565870759672630528266577
False: 349429951283395336155042133989373618967101100579351140040140299354272198210841
False: 1503192843579423983195935375338726634809656993782045555631242700269417739042589
False: 1758807649438398535116360185680036509549316734933270774153740884441665491781601
False: 470047367764880031291377599449091479383546271400559197395946265039325623793573
False: 1247525153835995680041311516620051074027612273483751516364121891355152992903359
False: 542514452607619629028450866722072116856361793673205536446682432758360629224207
False: 738585048723902014332372455147361366441887617931457198918653322341202918727823
False: 669416996274066085139571870392652176756284155344160197125512982881611406081705
False: 1184180519241967172022889927942001871418007588861471954824187603312593684862377
False: 827133425793805041256918409622466780008899106358167173849153663042366464143701
False: 119888175595142755000825217590672661114588218169802011277538293014538171163333
False: 1628900758164057721304274630461117356525804109137674141122111471655696878369117
False: 1300095194050269317608381497467282003312330553690549616838686187425143237463551
False: 539424000899416690707484183667724648395880883513490155916896820255524885748627
False: 468297521558131638308180693451165024649780489062854561962172238712709952930281
False: 900876611713437455528061237381843992250199040988171794095229163484038475018037
False: 697265546835106200428330126092069007836132431104330823308842920065632149552073
False: 1425489170370663857573803732225364867223745326305372451195369848722123127433685
False: 1727826708607833453868769840780205179115434641906382340346195183858289885233123
False: 1671424832613380713674517483144903336444700700692765461630881877585263173625109
False: 1004930352427738766370341885096069379083448197600136564579951304859216164678391
False: 892623715728275244724871801266376566432962585510365291429990073064243973464721
False: 1205217764524810338652095698788775972801528865827016453752091873103582457253373
False: 378482621123532536935338140630060484576373102055004260298260125294130176976365
False: 1724240352422054070902873773729342041185836861487810599438976519320201567822227
False: 851777251951028068425253359051145207258376744652302252515916521982600770608123
False: 370688257740537629461574581633881966597148681672490427167596203069801004687569
False: 1658669951462269586414020294021778103081762405052251509462566175859661013652655
False: 146084786645371701398915151549388915065561495913012331380605643622028987946381
False: 448251528516979531090480235885557354327691414652471079906492840507244256970055
False: 1690176810569236267700266860333218137489308563159171853263485126704626647251885
False: 517773876896997038374425926921577539283044239007823144850765456826504943538397
False: 1314204436974076455220836123899558578187333538631818846252800471524671228874827
False: 1538075435501062562480656179566143531506380967875436939529793979521845783493719
False: 754127078452937699048244673459716462452880295322103241548024863545674844352223
False: 1764193863214503300850018847948650806432099475257284859266414904249738884995997
False: 727635440625739682630637190192747577422136969313947162192525059083325917885535
False: 451160562985994577118772100024781030059361388539142487076448566152488182808787
False: 898023501633484582525279182902834514331074787823210562723258778640959737008085
False: 1326002433544246091150967587805900404789040624969660407628863356105018405995617
False: 155415651608142120516901280431752308401016105964264710449055610220368534890223
False: 1684445649463026580005948028244005334163172936889489664770175840799189145299177
False: 1475190153904848208256322644999244209610892046508021113587660542208157024705439
False: 1500150302396751718788187868949466887742314080581669716686852045911525844339465
False: 877269901939494666903003310761253632580175213061430787073612921249356760362989
False: 1827784691537819086415788684662872756692999360743227751217612642947468532773289

False: 454644541237151766895742103006729354916632967906918504235729185374119725380979
False: 750880048609732347906288116600260980190284030023165353265855859877736503437177
False: 1487062093865754488351857791358408681787717549777204160875527423621120629604965
False: 897838413904223910922220520849135851960028404891086237923015544284030757163973
False: 160755988686094160970213677420899564553771900071695884089860144392361743305651
False: 607848114481411785419507568763314411817888104831641030169509322781201693329079
False: 533769108681903550631815523691407520130935781825366833752505363737467089011097
False: 1699827428133348024295162097458371116887804668746542621915239691142517449133093
False: 1362812964254904145181265486440222081754304792771103807356608440370722200668711
False: 977172253976881402651711423452084494835336512164302232064630303041144412258073
False: 1834719287898120890494766192425818996551028848688512646864555684086113885598493
False: 325318747849294029454052468206158957635884686608381350080696984703430393919953
False: 1728910693301946586146495757371414353916669283913108115827235334425674523149647
False: 1405346250536384054015282133047714189581162923994135619976499581421026883790727
False: 1316894883802379554474201253968425237039102837739543855850921309528761629119343
False: 402493830276848327175604934636642074266178603399248956087245869156547235122871
False: 451235711809983113006483873836518300805420573804707659846549009378214031341577
False: 1552902020229916668871470562840654681652385812374544006605748130495310052072525
False: 185254048303763052828746070798604466472494349750863791111387657217240181810715
False: 1301636595857009737099557549674108304885398258316244573596427102507561120660663
False: 624097566484631052151802346028344265453790179651899708269672869235666566897493
False: 873722752683447559027145331381751557466411681856534813633731244746680095648847
False: 1631077243129031206199045149396057642412455626418489719893668067172443562336329
False: 1391465905711367638173459960695667631442636020483720187252418041853212151607161
False: 267326421055422734210299157197012479994020413219135968237106090945819332427467
False: 193715255192673020864811952253387986257502366388220284231825239962205831570479
False: 373788119666285001536540525701306660028873097515126385951612589401801811441937
False: 842316212470160276193950571809884802509532611149809648569750167954480480373533

Ключі для A keys for A:

p -
165225120617920560782327026733916602516238109749313643634965648480965569567780
7
q -
602645644634858585163955432352104827676000981905726016663849921049271590344787
n -
995721993246590006025435437916808518729098834493295688469930538605642703253666
437672901044603938589479085163470072687091910590779895812309915436948794042109
u -
995721993246590006025435437916808518729098834493295688469930538605642703253664
182776050230539745602253385472199219848709831191917442798803509578021508019516
d -
488253699533051554781057563182566441505865191285933687643579589585545711052943
756664250561901279823555729130923599544841956999597761644419882676421392465155

keys for B:

p -
315934315643080656423433082712119179814728377890820191072436190566633059781307
q -
146070037201621169134755215502146484160083153843958407986065022774962641201392
3

n -

461485372392535163675018635571697490180139551111291632847221388739307330690341
080985122640361906801998901040109849221805430443691454356512390903171819137361

u -

461485372392535163675018635571697490180139551111291632847221388739307330690339
304350434981069559031013663306525827806245514113287183423425972586912347342132

d -

225942901151071259063810129925751636165048117227194696870406999180373801257648
464056401935027289381188464357251617195981217219904663658310249157013857089313

Шифрування теста за допомогою ключів A і B

Some text:

817881205855397149413248076923785776341239833260943023157756172324620781534442
584735666200627038845856

Encrypted by A key:

120502823081118357838555701991948866043680129240234327883909101815639953676891
083862007788859503949019068608396965690950271294957555842962026529446216026753
3

Encrypted by B key:

476875292967095413407251709611324772591569806981788709834548823242208088660515
752601554132720176869834104038207261331544433594928301878661036639850030474888

RSA: конфіденційне розмилення ключів

1) Генерация ключа на клієнті А

Message -

868593012844820581958312693148385291095688427907783805239384897383834016746445
408289068885198304258055

2) Передача

A sends confidential key to B(RSA):

S -

317379812615065945335043975289081139676804525820091292563312795574846366271776
58446212508161505190939109509881447943616261093920977357831284043496530115732

S1 -

354277521224799619607958894955491635196070869653702221811824288267012604864828
43624179190907997672716525431105583554481709439488892659668018650154628129518

k1 -

129408367781942816748624623539087377413223698468863572786143247094591591242435
617402804136524415068598137669758808042812147629282556319873295887382636661842

k_B -

868593012844820581958312693148385291095688427907783805239384897383834016746445
408289068885198304258055

S_B -

317379812615065945335043975289081139676804525820091292563312795574846366271776
58446212508161505190939109509881447943616261093920977357831284043496530115732

signature -

868593012844820581958312693148385291095688427907783805239384897383834016746445
408289068885198304258055

Signature is verified

Висновки:

І ході виконання лабораторної роботи, я вивчив алгоритм роботи криптографічної системи RSA. Я отримав практичні навички із застосування системи, організовувати засекречений зв'язок та генерувати ЦП