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 1 1 p , q довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб pq ≤ p1q1 ; p і q – прості числа для побудови ключів абонента А, 1 p і q1 – 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) , (,) 1 n1 e та секретні d і d1 .
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 М і знайти криптограму для абонентів А и 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: 176073808459464388439835558544850053007909334710417409100613241917560838375604 3
False: 175749416734707917136839045524659940089225582862213243465306081926952104823093 7
False: 704290565930823159778083253644115036648429397016299900215207539229500484148599
False: 693873776930927721665394572465055825137431346023234968940506423141723183162817
False: 136656808066520521454477467734797493301003812326143804057905660530197003081012 1
False: 951830993987200816118884940640443371271799840117089071707010953004884027515307
False: 157575228569993088125728946248291742372799619326271321922412819863209224991707 5
False: 461727220812429593200407184873769046596900827738241606806299803468773828256357
False: 557187230037171434929388235816291668060089814300039286388056574407125922281469
False: 148926475697647284909326568916268587243334866386376153852844209337875534490122 7
False: 134920802248179015256463372806562894235135012279662159859476296542070001073672 1
False: 158269681544016658228513800703958959618788175379611533922165427971543140491355 5
False: 110380661022733069995471521429821487782419829048795144738233157314538620031450 1
False: 606787911131420383488757179815897749978159331675015362355126209746579004769011
False: 328001964348915486536915166963237277110554862977315923048243750856210879869821
False: 137891088525347081687963257736361807133812113220201612375278296659333698270322 1
False: 151947118739120185272452663907034212743392632259717178484613869222421197027029 1
False: 134594106688419392595529338987267423088753325552114577038121166184492428344906 7
False: 946003278639686264733889322636965033322798463728144539721721316871630170108879

False: 766236783514896819665858518139142124073333696784331368446202471321280866956631
False: 449165181706746301856868621670106962411641953241502503162877506768311083121399
False: 14679851318790930927371155492899192169288090387186265894353909135927258849097 59
False: 283337095168232226807037741413718862516916231772344457454653364269827999414581
False: 140493514408781623937804313267737342868144072475876643545829910240454841830222 7
False: 158196270352366628804522206929791631514369546882429045104930543360641851140560 9
False: 652380673885386956251682499583630287787982662206036447480408770500080234276925
False: 472131138355353156603099249326564757071505289863889015057203648875474631436117
False: 120723365870538249839755543242413580632361059851370043366890282559905186015793 9
False: 161833699467815291092623978766653771873888224369937334225842310549380004660736 1
False: 122760241588765670842361178367882922593871902706485991903156920996817534554697 9
False: 627447017540920876689302923950280210955373223895099166550178830048581621013797
False: 100186524375869836851823097742411301767491740768155632929078259921147032096052 5
False: 471707871318701075666241106353760271859538073953152544741562497424180744193489
False: 177892551753505397730686221475590083185102009389927027778576641376543902887964 5
False: 146146746596013457504809298305659217456451198051107294248172066318274272922163 7
False: 163729695999168654959832619701812264985720142813947087611892609874035105725759 7
False: 148963588162801885644587245311247527430276480888018443418073169240294008645784 7
False: 613733065773894380415906082083786926166507526790326139937583039561073273522559
False: 555698528482381204081610767237401047400163711583594022487850053591675429775411
False: 147679040043863496611314007575554592031952816598932897821853504716373721010744 3
False: 167257936175933157999569728379730719335869826049859982811669998360129773604226 7
False: 285358554971128684166447225835015229020250565817454866090597091471812424289713
False: 130236917995592271102362912194571258210957650609253977473826886576457835692776 7
False: 138915034690306310118309260328619481429904908940779261205420846998829817350198 5
False: 323104261512669688080799335915071491545042302090966183045678730765938009699513
False: 143462390011952712201666566551046579751774938561576039373975664754795091360915 3
False: 149814994312514431707361863434608084337325530132447442766024042795745733062997
False: 143731135511690164423400869592532850588197631127373219522061868515042556525022 1
False: 653338237882614899881020682116221335202216625486722446547387534218807843799169
False: 113670003190900788030061608096874368950411137519276887378659400601156515403293 5
False: 925191836004803684359457412657464610658919934054726553254694561219208738903467
False: 134894916137453231073800095732296422802150311056748691345425333957976146404180 3
False: 507625215180801118544224450041843347133042393773143166323151743849048461442011
False: 158150413307593089782368811045898073970780060686440962429465223707234136230036 1
False: 148718084781122291135430375372779839427274083139043226765755400160381882147693 7
False: 605479150919600221703221195257304586779117304607703063474879005305796945675185
False: 506421588188986198265624487296471460960484783241052094477482324141592092517017
False: 144454670031241142075905468541767583689133186074342748735105967157882518942546 7
False: 174602925596486018587655471363400138301082511245568821289345643860034264565747 9
False: 103577966030890186739051640440424813273105392062851024566337547994152360454633 9
False: 126028812616862468140229150050861025586368311416912453349918897014014147276563
False: 173316638955375552604915508355392173430202463778837662800978168941458774809959 3
False: 817197232713229528199747394598570491130502862571730283866947723478098482970999
False: 173823677720481881083854602530927496894740993482516150949039081017954399689951 1
False: 172005207032959534699413665830431854708767097625994141205996725676996798406372 3
False: 540877331799882360129973632545635813004578792243383132644613033370495519246453
False: 108700089269972214927023397845237294314565652832092902522900260707092132561629 1
False: 735878826982209333668259823391922164148423603143280858934988132325551712728033
False: 151645253221254309926292687505237828665557421962170025874581933493716779326588 9
False: 128004816686628712105797668056499218430402961704434893858422785331603393123132 3
False: 170977286684384326077915293719257592478997755359771851588421725888258531666301 9
False: 175090509466706197647966085646383606823009398571202540544470481929057013969682 7
False: 109364763818872639570163445518399372054661540945734107675704686805370172713554 1
False: 120968351638275997306522181247091585154120112570068205807269380259639809112543 5
False: 142701988393768336912308971999318061483329465558144205242102228161703976942190 5

False: 96822638018115454900529059455690865842022135450299128594753550858109390565376 5
False: 15980088360807383743438894603094854340881869737782367131907040953984584801997 03
False: 11517645165720802265542550593160251638624190974645066198146554146553992986215 41
False: 13956345332877532114193235538174015205725980995046382881466361050986326036034 51
False: 37517810508904975950347296237314046158541132967483233996562083870030764812838 5
False: 10542488405559579249335841832655041074622088920240249639952371242108920951296 41
False: 12562549582702041272118953827531889260609580235139626388444808046218815162328 25
False: 34729042467844476158518959585696650310569124556040888394087039085594666650307 3
False: 22252275338651553435829607109949057128872199987475057971469079720072199304064 9
False: 79568388678432163482119991168741005601270624139059609169253096386770543362779 3
False: 38878852671595849193544763231375555674649178000920318726686041720546744738494 7
False: 32511925396758189022424735332305287147277038273928765094164133829763965507308 5
False: 16072014762513344340446424640209533363910711694371475264050213757023791643982 25
False: 10353641931187342565337216120692536666903196980787904662278867397562133480807 49
False: 60783090177334596861869383603999807640323502531335581510817719184710361974992 3
False: 33361733597979011769083387321891165891059684575649489831662908043669578253127 1
False: 40771735577538742709662924721238801892378337549037537799269490033186729249682 9
False: 12840538108047248398408878657764247849601023704357745901511322750294790114872 11
False: 12310101584449702994195280621517528446488555472450777007086282160912423270844 61
False: 31547688972888997102889292465723203852871545694918712218890285017693906287032 9
False: 23682683312618164559527384960635597990685323020563559783253872345259416552931 7
False: 62690938661063200288343543748285533457066924987376062225857431850787468704496 3
False: 19180053737911436395051617371175778134303382856027367790681529453557922780706 5
False: 15141874150543943319674657156378071269681790761205817093686561271919593724886 59
False: 73762328479714343166215955596752999386610421481039792597002995627304586335840 1
False: 17393829295580222536891085555035875834245938584399729502298737785971880263004 33
False: 61107049519728314926976915173731603707156692298019833675743318367013671869174 5
False: 18318396420572327150830394498688289872744110446164731533448276731537857237102 69
False: 11818405050328457854249843836218369792615383697171329099856690473435270243547 45
False: 43151139568271286036194393040545142310611638750385839701101634174006596780635 5
False: 13454598106611064026270748748151854590607660834648864839831332288790105674949 39
False: 47271379087434207770300217644208945430342826474177674474001175140787002635428 9
False: 11185515545334788777058097522724906410496619605426480549724980233539611880167 09
False: 18174223022022546872956543711199097857503754329705748649159642577227547158711 57
False: 90609412600262879003377428246591450576808601434841570845080991888853572608479 1
False: 82999831528856950343499806280369856891656901865579636633972763368785027585659 3
False: 69105798313470035768531371549395093091837829930293450738389073427102852445131 9
False: 10648714085035686177240674954566986103746494375105493065338940447662239045406 53
False: 17303166396391308049714945806550069922012160751096000925018689251314827866011 35
False: 48460885531036628545869986148400583407498360929598159265471652581702135351475 5
False: 79152970071233127508729945917629420123806191022532469184087391740431667313725
False: 16385721930820192624006351861506803576870334594252980756863458569640246626062 63
False: 10120230394670535323368202101516364769545573543823886199672516021826465230525 85
False: 12809754530244793629521893932595796371194865865853553750174332146149070913180 43
False: 11131979074572306277241326886379329293874684481394115696607650628520897148583 33
False: 10827448029244552849479640807647243842901987798266157508763736030222328016361 89
False: 18513206601394210847147943183665123851142296330143214855108951622608739855112 99
False: 71756532523231754998107424497762007409409471506170010329137672288575760479378 5
False: 74568678405373491879619768507438477494563286720869213131260066104007844778562 5
False: 46725835090000075927808179347936908173474035371408526452521484264398093781915 5
False: 17871057307291760584537039824854609888113664597437284040042173935084272792119 41
False: 17537179024803992438443355681131561334009481533713545284287029253028249060248 43
False: 10170564937035379136990044683361720679049538710902062489759227524616804325724 15
False: 14196208404781691437949912794073881997861656120913246975627657522305611977449 45
False: 62974942941364750602822088376118508469098845476788344893093069269020162654143 3
False: 15827755860337561905717345584217187304032866357580262492147304203592432667007 69

False: 158139708349169003470341053248574998173026283675993235519018011529460561576493 1
False: 140051109800583769343536106919432717338622074638662733586275299617798884391175 5
False: 285550119344192876020751133583754893012235329264947031336751436480386406865671
False: 134304259203810878667341950139032953451102793478090408753892280373737914825740 5
False: 161637341348381491052061307235725390041285901822889475311460261162320917053443 9
False: 152591247340407175773407580349815486566434396881616955935839237112182084839037 5
False: 9497913546203386629041236681960840881364845695811640310093078241702642009956 59
False: 102284832543849238357568386372178348725514336583363081820539301438147875867075 7
False: 11950416120941589284624215449364562718774108320075394767150117782793487514221 93
False: 58024022736005077601933913074402861342757681589752774997504745747295410180619 3
False: 11589125327796372610069868218693344298547258113075497249428072939459763381543 67
False: 14824898058467396030385706854507524645761118845368095870849860499186321292350 37
False: 26657628198780164790647487433985785283783525793549289004969928422764342790587 3
False: 15925958374335058430264117936334560194988620913247679688887844171568109245646 83
False: 16134200233001157666901065172716774617687491742072539775010292982600018615266 87
False: 16565496203496824725305840857119434607678658163673392131785763677064555347933 57
False: 39333044894617705174807473272233415291301607239280464738235767712301386846426 7
False: 97428340803754658159018479502369134153676903985714145133611186532687186407880 1
False: 14676361906421203089201026382248982573057465664277036026145627851186433245772 97
False: 12015386263897753533022016432148703186970253762904791568699050715321995297699 21
False: 16858842063919041594995023758658901151768486866738522796507400365828726813482 83
False: 13445801663774159842541531236753115919728932601962148560708452017663405156519 49
False: 17701794162135863046391139040220097756307560288416678241395687116399920374287 9
False: 48116097272726540849603638058914914986354088202635702833305668078169894063634 7
False: 61324989619222121674046773262186509832940250711895219939236624671378132699526 5
False: 83578143447558948622605840290039406562689814786425206643202071577691091567684 3
False: 79431797677231183617030327944683375629558483991805485947472671882101202922181 9
False: 11432839340139320613688456674378311769721238466549147487676812416214424594368 21
False: 68259158070832607468938732915361211147570587471763063394402598014179943218857 9
False: 17301185583498398451046879209465833545708103870960123496869170771353128059225 55
False: 12171296846967507146124024077156678669074539365175696427712518358380362797686 99
False: 27710074406096013902595967830200508041356666410918734690114145110319073738592 9
False: 18079982106837777204302633114223744019252593165869978753666340284995194345180 23
False: 11605570608197405650432473027704029092748232455353680750883649392082499536493 05
False: 84877108290542744640611584671222859305487024088768011516549509626086040503702 1
False: 11665311456236308798616674847254901871079371496238084476208262150452106743035 81
False: 41763762746046298895015130242986191068287466161999202860288948726104061143507 9
False: 18338269946878063327166693403582222715697861880175221631421905747671272761704 49
False: 13875659403510402801928118221333846610358016058105130328703760301992959339506 39
False: 16117375478328776503268032827595062969956197697677964973683822095711409053963 51
False: 10860300197877055297337996369274915032873449552517565403163709448742168830676 31
False: 17050765876792280793899105704440088387563551310966237016310538863890912520252 91
False: 14108167647915964275454419061452351836996476499543622664881244914560713474313 41
False: 70963989667005388846198768858991572300397114575034896224186276889674454178200 9
False: 13064554466877266737894219426903285945242553934682132613015394624648768729053 39
False: 61987911697813907593385993107978487832733910451805219396451795695976553170890 7
False: 97149938961540073442032653520719031047299863241117080099255535253630933115205 7
False: 10086603440469398788475620204831037061478150700528283632429297328191996816277 23
False: 39082558343179197255901108089433730336241632491829326618198988535816087970959 9
False: 12786083009819845780219762256699761346978772791152439491859228362921553403059 21
False: 14266916013320205145738352938742223485391795656182959427176153599958128673574 89
False: 16852152696364940830106026230691070001470656068209053471938314514285158233853 99
False: 94119577591840799096531102253672789325830441672851943595442015908042164073113 5
False: 98697373182488367455141257329990903526259139067300789676776280702174537833095 1
False: 10043611879902606911834204104824621597109649242536763022215684811616242021193 67
False: 87957969262451636421969447522781823231448613695385966157570295915397199658749

False: 738355196142446545913228203686054692711187896976931885810061747145530495945693
False: 462882631059107914882400871878992593199841883018224108006970888181735119587761
False: 49334900454433185493194314348316475243309042713831109843148116187487793547866l
False: 269664448907704638313267150150154725419176360174619679223289541083647684567959
False: 16622763081033461144079981594172695273962710395022631609387991119567191778951 27
False: 49684806255792721703829510117437086869440042417655052617526584862955751620l623
False: 30265011925326173377250232281086685928841616901872306090710571111961698216341l
False: 17088510665189998041116421367057005557910422794363460191210770871165833393732 3
False: 15220026302973364857267683216227942598154736474794368148845894859459546849564340 69
False: 16600907598938535954606106743730728316656948023383304825658707596726305282665 77
False: 34942995128339533615504213398937361896710110057935114004014029935427219821084l
False: 15031928435794239831959353753387266348096569937820455556312427002694177390425 89
False: 17588076494383985351163601856800365095493167349332707741537408844416654917816 01
False: 47004736776488003129137759944909147938354627140055919739594626503932562379357 3
False: 12475251538359956800413115166200510740276122734837515163641218913551529929033 59
False: 54251445260761962902845086672207211685636179367320553644668243275836062922420 7
False: 73858504872390201433237245514736136644188761793145719891865332234120291872782 3
False: 66941699627406608513957187039265217675628415534416019712551298288161140608l705
False: 11841805192419671720228899279420018714180075888614719548241876033125936848623 77
False: 82713342579380504125691840962246678000889910635816717384915366304236646414370 1
False: 11988817559514275500082521759067266111458821816980201127775382930145381711633 33
False: 16289007581640577213042746304611173565258041091376741411221114716556968783691 17
False: 13000951940502693176083814974672820033123305536905496168386861874251432374635 51
False: 53942400089941669070748418366772464839588088351349015591689682025552488574862 7
False: 46829752155813163830818069345116502464978048906285456196217223871270995293028 1
False: 90087661171343745552806123738184399225019904098817179409522916348403847501803 7
False: 69726554683510620042833012609206900783613243110433082330884292006563214955207 3
False: 14254891703706638575738037322253648672237453263053724511953698487221231274336 85
False: 17278267086078334538687698407802051791154346419063823403461951838582898852331 23
False: 16714248326133807136745174831449033364447007006927654616308818775852631736251 09
False: 10049303524277387663703418850960693790834481976001365645799513048592161646783 91
False: 89262371572827524472487180126637656643296258551036529142999007306424397346472 1
False: 12052177645248103386520956987887759728015288658270164537520918731035824572533 73
False: 37848262112353253693533814063006048457637310205500426029826012529413017697636 5
False: 17242403524220540709028737737293420411858368614878105994389765193202015678222 27
False: 85177725195102806842525335905114520725837674465230225251591652198260077060812 3
False: 37068825774053762946157458163388196659714868167249042716759620306980100468756 9
False: 16586699514622695864140202940217781030817624050522515094625661758596610136526 55
False: 14608478664537170139891515154938891506556149591301233138060564362202898794638 1
False: 44825152851697953109048023588555735432769141465247107990649284050724425697005 5
False: 16901768105692362677002668603332181374893085631591718532634851267046266472518 85
False: 51777387689699703837442592692157753928304423900782314485076545682650494353839 7
False: 13142044369740764552208361238995585781873335386318188462528004715246712288748 27
False: 15380754355010625624806561795661435315063809678754369395297939795218457834937 19
False: 75412707845293769904824467345971646245288029532210324154802486354567484435222 3
False: 17641938632145033008500188479486508064320994752572848592664149042497388849959 97
False: 72763544062573968263063719019274757742213696931394716219252505908332591788553 5
False: 45116056298599457711877210002478103005936138853914248707644856615248818280878 7
False: 89802350163348458252527918290283451433107478782321056272325877864095973700808 5
False: 13260024335442460911509675878059004047890406249696604076288633561050184059956 17
False: 15541565160814212051690128043175230840101610596426471044905561022036853489022 3
False: 16844456494630265800059480282440053341631729368894896647701758407991891452991 77
False: 14751901539048482082563226449992442096108920465080211135876605422081570247054 39
False: 15001503023967517187881878689494668877423140805816697166868520459115258443394 65
False: 87726990193949466690300331076125362580175213061430787073612921249356760362989
False: 18277846915378190864157886846628727566929993607432277512176126429474685327732 89

False: 45464454123715176689574210300672935491663296790691850423572918537411972538097 9
False: 75088004860973234790628811660026098019028403002316535326585585987773650343717 7
False: 14870620938657544883518577913584086817877175497772041608755274236211206296049 65
False: 89783841390422391092222052084913585196002840489108623792301554428403075716397 3
False: 16075598868860941609702136774208995645537719000716958840898601443923617433056 51
False: 60784811448141178541950756876331441181788810483164103016950932278120169332907 9
False: 53376910868190355063181552369140752013093578182536683375250536373746708901 1097
False: 16998274281333480242951620974583711168878046687465426219152396911425174491330 93
False: 13628129642549041451812654864402220817543047927711038073566084403707222006687 11
False: 97717225397688140265171142345208449483533651216430223206463030304114441225807 3
False: 18347192878981208904947661924258189965510288486885126468645556840861138855984 93
False: 32531874784929402945405246820615895763588468660838135008069698470343039391995 3
False: 17289106933019465861464957573714143539166692839131081158272353344256745231496 47
False: 14053462505363840540152821330477141895811629239941356199764995814210268837907 27
False: 13168948838023795544742012539684252370391028377395438558509213095287616291193 43
False: 40249383027684832717560493463664207426617860339924895608724586915654723512287 1
False: 45123571180998311300648387383651830080542057380470765984654900937821403134157 7
False: 15529020202299166688714705628406546816523858123745440066057481304953100520725 25
False: 18525404830376305282874607079860446647249434975086379111138765721724018181071 5
False: 13016365958570097370995575496741083048853982583162445735964271025075611206606 63
False: 62409756648463105215180234602834426545379017965189970826967286923566656689749 3
False: 87372275268344755902714533138175155746641168185653481363373124474668009564884 7
False: 16310772431290312061990451493960576424124556264184897198936680671724435623363 29
False: 13914659057113676381734599606956676314426360204837201872524180418532121516071 61
False: 26732642105542273421029915719701247999402041321913596823710609094581933242746 7
False: 19371525519267302086481195225338798625750236638822028423182523996220583157047 9
False: 37378811966628500153654052570130666002887309751512638595161258940180181144193 7
False: 84231621247016027619395057180988480250953261114980964856975016795448048037353 3

Ключі для A
keys for A:
p -
16522512061792056078232702673391660251623810974931364363496564848096556956778 07
q -
60264564463485858516395543235210482767600098190572601666384992104927159034478 7
n -
99572199324659000602543543791680851872909883449329568846993053860564270325366 64376729010446039385894790851634700726870919105907798958123099154369487940421 09
u -
99572199324659000602543543791680851872909883449329568846993053860564270325366 41827760502305397456022533854721992198487098311919174427988035095780215080195 16
d -
48825369953305155478105756318256644150586519128593368764357958958554571105294 37566642505619012798235557291309235995448419569995977616444198826764213924651 55
keys for B:
p -
31593431564308065642343308271211917981472837789082019107243619056663305978130 7
q -
14607003720162116913475521550214648416008315384395840798606502277496264120139 23

n -
461485372392535163675018635571697490180139551111291632847221388739307330690341
080985122640361906801998901040109849221805430443691454356512390903171819137361
u -
461485372392535163675018635571697490180139551111291632847221388739307330690339
304350434981069559031013663306525827806245514113287183423425972586912347342132
d -
225942901151071259063810129925751636165048117227194696870406999180373801257648
464056401935027289381188464357251617195981217219904663658310249157013857089313

Шифрування теста за допомгою ключів A і B
Some text:
817881205855397149413248076923785776341239833260943023157756172324620781534442
584735666200627038845856
Encrypted by A key:
120502823081118357838555701991948866043680129240234327883909101815639953676891
083862007788859503949019068608396965690950271294957555842962026529446216026753
3
Encrypted by B key:
476875292967095413407251709611324772591569806981788709834548823242208088660515
752601554132720176869834104038207261331544433594928301878661036639850030474888

RSA: конфідеційне розмилання ключів

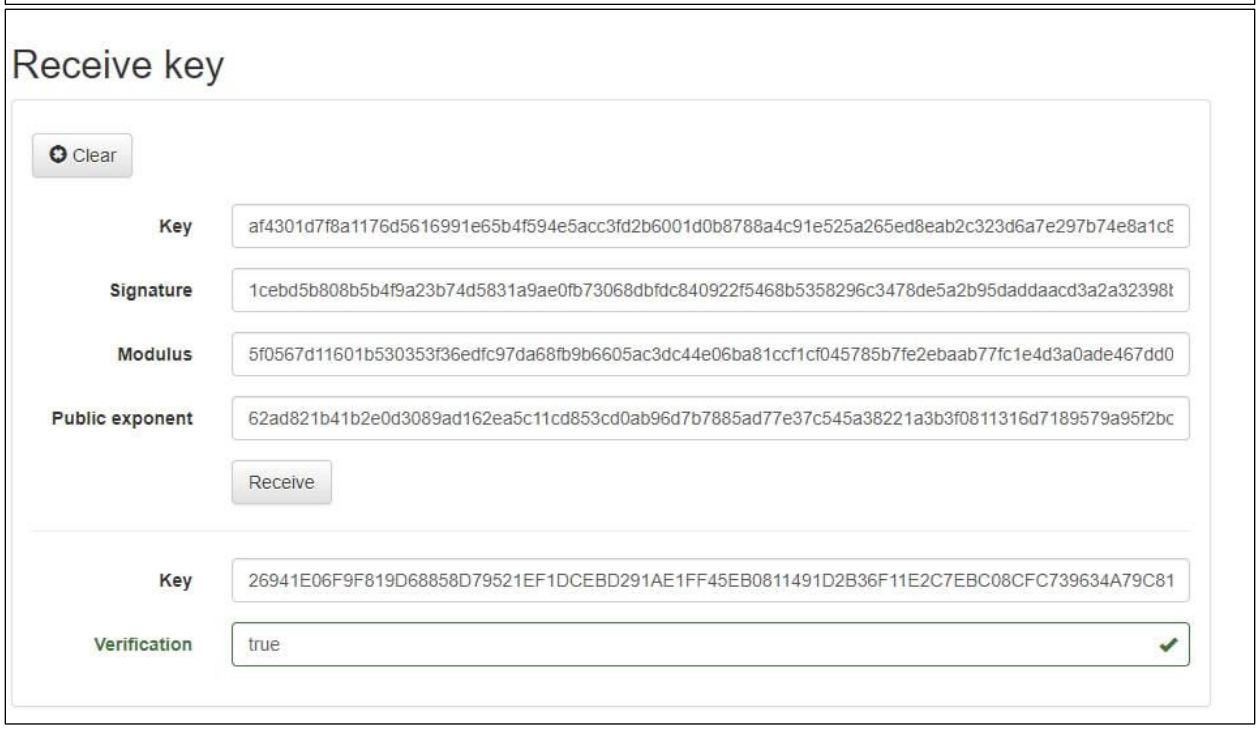
1)**Генерація ключа на клієнті A**

Message -
868593012844820581958312693148385291095688427907783805239384897383834016746445
408289068885198304258055

2) **Передача**

S -
317379812615065945335043975289081139676804525820091292563312795574846366271776
584462125081615051909391095098814479436162610939209773578312840434965301157 32
S1 -
354277521224799619607958894955491635196070869653702221811824288267012604864828
436241791909079976727165254311055835544817094394888926596680186501546281295 18
k1 -
129408367781942816748624623539087377413223698468863572786143247094591591242435
617402804136524415068598137669758808042812147629282556319873295887382636661842
k_B -
868593012844820581958312693148385291095688427907783805239384897383834016746445
408289068885198304258055

S_B -
317379812615065945335043975289081139676804525820091292563312795574846366271776584462125081615051909391095098814479436162610939209773578312840434965301157324082890688851983042580 55
Signature is verified



Висновки:

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