Міністерство освіти і науки України
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

Виконала:
Студентка 3 курсу
Дрозд С.Ю

Перевірив:

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.

Порядок і рекомендації щодо виконання 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 A, 1 p і q1 – абонента B.

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 A і B – 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 A і B. 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 A и B, перевірити правильність розшифрування. Скласти для A і B 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 $0 < k < n$.

Хід роботи

Вибір простого числа здійснювався випадковим чином функцією random.randint()

Числа перевірялися на простоту тестом Міллера-Рабіна з попередніми діленнями.

Не пройшли:

579723703680075940017793559015817583052640287003426657507102682803266101236 82

False

413678457262371005141797262360377221503080002439520048104187987967775119524 19

False

376537477900136395744289653773574963680431639042519656502479639458326302458 64

False

758871068722484469282241780186947296898269816518864746830607972967718492319 7

False

343618538702575403957228873015578344219947709393974796841143484121882543834 16

False

777453191579569559619678721024119700753153256364617674745676320668803286317 54

False

626258816954703826668087965473434599624765013543979130211519353417278368636 89

False

109287452513082781064621336948933905964403015817866343505267697627916895083 978

False

939109919226856107174058253079736033570346370268440831058364139373028737596 52

False

912150203089344588484347841567393021106747964317128717153826988501008937679 80

False

649283341407333522080203203902835231312964662687974321137951556968954174861 25

False

876893817139647925068609587524060275531588530767387939968796108339234257284 38

False

467448413570450504892043102289755711630925704718016452574457823680373162890 76

False

227953938683285515697480836680024436246594071012554348693749708026927961611 22

False

823087009618723318767118089088923209382402938198283748607210470717312652328 03

False

817011555235072983972759667909240010627994013548236682160645199403248358470 23

False

113117357027210050004546311502266456080443966165854592075473678255532667438 435

False

102707321775030796208497326535479191844126502977620237965947038523195411395028
False
999621386680074027518826297043087176141798462428740349276194885033392344758 95
False
210888321938156789271607768071475768840574003222076517838149911574323526431 25
False
108408655054849380075717543213307756894035581993560218763715331111352357515099
False
259947026884974166446792713502422904560702275955310807317150638823238655769 29
False
409116513805103758111877043691968315110170427964662298674439324944614018341 11
False
113417318372640417357688860044500845236966727848538044823842570349163751155040
False
419316494169744676668156144205331379513917172341945418744735007817062075631 4
False
796152048451720093803495515754973613373639935904491243789640951286788628628 0
False
116241789522298899425453640827048746028710401852691085228741118540838971552 70
False
275206486795686866520983732598824258758279150761417701438842168780299596255 0
False
202142884281686168849733959502858620189990144558117840077990001477573605192 35
False
901730797186602166882142089169606445365931825714775529149793171436918508953 22
False
389299969417518247768438496243733052165371519174398034422697976778619569773 76
False
224698417605667236290238973835650085980097095256199652038486552630957027689 12
False
122221481983913305736534116904080456502784424089215014544221341785869909842 07
False
873097280610577817677753807509791712839542912080864708997203734557082701307 38
False
755988444482527495285882775676301574785284280416873021437723285371462510768 83
False
827567123866736040528598555152287694944778293881711284605507782175815903647 55
False
940344829097461007948378364448794728648603984174233761071719903019868745305 72
False

610467313632735279154357626701248101310508771441617295025371323963538014105 07
False
106949903321604117831705769105461133405593986071164139062566713631755742857527
False
283651491307382311161148498549902285643294109035906136772927490845755146461 21
False
505142372712186544613325263239114752109559332127960864481927129156716997748 31
False
186331459873303331529934566357193215086324918771199233425789439097944617436
False
292401610125426476200354656710512051971087647317054100487008092535507449048 6
False
595713758717232735167838974196202948543033498310867812525697144290009707078 23
False
328516157998941332219642729604919658866927777767888856096642849395530422750 2
False
834001718788605979021195194495762366404912109766852723281625394627070896426 6
False
257522210677783278328915401448056619396341162716840410517269002808059655318 69
False
720436422561897085654123667785641934983940338712616194170484021323311217625 43
False
402352839650257259687758120847264193437850652778725861532319166580725848531 37
False
610642619624326824086602264198905433315256362949461491149045709079327055487 8
False
109359894914362837686141080415508804680735527501559738849683145880714867246 335
False
103116453889259725833983474686829321048840637959222380644321466628506969144 96
False
602964858911876833061670902415295531447502898809060904482982584813120684210 64
False
844272080753324035003847186913777094538946010883468498239588214928796122431 01
False
630489666318568844143364504939016189726503281160790623871567653634327395 75
False
993506147796019789680673857387994368388483940473602446456917724927084355996 25
False
541778278789179756209780170977629819632824877136870418181452915251171911100 30
False

400237882289494185869911526234275824867671612810651108987796835593997776552 08
False
977721250795754264015410570201516903647359478213162695098135635610155860637 07
False
794221470140764292007837309782370873681139205177843921078662054026512504448 16
False
1033337260912461104145092606558043271346252336856499827808154035417792099942 76
False
807116042291592483033428165933679411759302406438846168512228642201900091561 22
False
563740816854965363623182161265077266691083260449310405081079954353336184247 04
False
514662348817582130306621111535294746642344335931288664441550955337736575096 13
False
432186680756656767869065824360562054494064816264670671109443517809735141237 14
False
615832075684022067199328236306801292511237696538359076755217186837882647802 18
False
494496244348531418362583120459020801201534073713532562450252977434279263374 76
False
195108150348551370519365069587676796873898449878010203089251128067144428164
False
360913025644691659545152427832437743317882006881671382651149239946057469770 95
False
503691105163485398429182146013764139111508952632440821362513030120264059923
False
391546904080091025629977668840395699649944071438775444595637673514712439656 24
False
817901384908139730948255575980515299292220903689403970412025403826840507235 02
False
986615198112595200969962134637020930753334207723892969756136888894707044563 52
False
131857844869015068802378691441372493631908554402212095818777554748528557543 33
False
340140832191684428993005286609331028652913588386542672325267988051496961989 20
False
598764340750029149053095744724376599612228936042256674225159643778776331496 4
False
318766711811054269078152722521637762092727592121524250744778223998186200360 07
False

44481754165107946710053431787733100676525581312206644804393848491921366868475
False
40208728130305421063972304702300255530847267603917948409284470660685889315832
False
84280447068572163255707758540434833086456336886593750396627818378178025794 70
False
54883991096060465767513931536657274486698587606451980415602706637218555733 75
False
89889366995486805179487173355862913139166866028661647611412551842005942575694
False
15079254694481173312640114646098734516522595761304895210190660104106951708 77
False
57264273908699243280509708925665369932835671965376017145182684249751546362 24
False
10868422467986450479440504964415730685964677999194097256196079989940587713 5972
False
10163046533496253628864309558999302270784107118134704791445984707369045070 6830
False
91978296374532402066226625308555695334899931428348347199748720614761907257 796
False
10337521716151049593435275970562806455312510243016168057482870746374595914 6554
False
10883363248923455127619262559143946857137715090820190534457325618285190842 4789
False
16906002866028140595314825093153664250282543774012749819059431587165922568 593
False
51043361099628652566281639071124029103511277594386236603622730240005162914 115
False
10595580129719976674153343623992832581062376332004525594713308596864384442 4755
False
57825964293169366222818810905276571775634521882076309468464573599083585100 518
False
10262855211791483373147581116261915325201310895978283266573577648969945002 5709
False
10182367587076706694660205174240846188817294797547004628721527651812047231 5902
False
33375488633481528176502194421247034650316513665237803346465375356051506345 142
False
11177446175626761372484845374242460617295181283864811687007780527897820075 572
False

907095699243576146470220223692393825958283793751344631656662986928356173942666
False
33457843222596518716628709534455589223911129878883563581565128117903027130984
False
736152162605066100218356972919356580459143218519186739574240217816589359333321
False
40298547034930279852852644260586317486883429918354634627604299925898152591436
False
11597492129238662943044028252983592763373047236753154561485984206466012360846
False
10508978092924520711115459090455311510487966541544858058685755627376530435212 5
False
26844714588228676982963532656791636350995931926791404119636377755119267000855
False
10621827068055247452431208144881929514953021567673435674995541929125155307745 0
False
86294462054749799878111358417255569157054795629056589319199141526176362721993
False
59082343501716172569952543824992299880576166102247218401054348403154955190264
False
10319624442697336683879072743083827553214791261712720090682718872698009727308 3
False
11519743611384295558807835548410955037438904507135142038028317263208178058656 7
False
10771125597182661858104492046822487810129404455060605654502279775107868842337 5
False
15920662667593518531077094680114842241138077111828674135927668878458152782 47
False
13334914287819234697371029818374954670159055397924665630065906494401540440105
False
80784961533720083707830735805767896471010265444908270873777206617286142572 12
False
46534285808110164436516496325754077890755617183596701496991631933067791739515
False
49066984729302437515032951998851070218417453097535177629047352523408238406798
False
89704622902821423476441987573247575818727116371106127153617389831113278989967
False
10361140548066994123799777766745714871431517297413888064625887757397669397045 5
False

722819982653859915750294188893629585364292722508217288710976709330982648784 33
False
183723453837094468087102404179393286179567839280522478356973332119688715161 28
False
876241277297713886432486550548009690552935574197880029489067067704839423246 21
False
693243695394150056064697423999104514068500060214979201206838636385066647566
False
485676806118449156995933051569851362732447027562359913658287918754466317278 21
False
101173172166712201446534870044640309800636998669379059433069536988225538296623
False
527272549018215736554906965256855405898099780800056617126421223024500415409 12
False
427425888825516523666639193745768935493914580152965708855842030114642135839 82
False
102193791447788756422519595891487292575457603897698481930698703047973845878875
False
406087804159621421660096504265614262278947405193381593814003393036771852181 41
False
653339893807496836192686128790276818562661104989678239302366670143483082538 19
False
760397156635541457531555424008610311544586940044218593021818397741314019121 20
False
747285097488529742517096500110259306269754673933877548803457923376391202980 51
False
980071899426822622389550104953424556429597980182937785094875383842418625420 76
False
844422763839117339824867795417121555031955293411638666326564271166700550042 49
False
544627173404173114176361785252664414033907239593573360631246671706064179131 85
False
921571396173072073140618105117972197660432262071544649204348911451620401898 08
False
462122870633990783257149284365379960199413294538178365450922687409776265792 60
False
272180072522128997454378545920588295998620342989498907684591952468307073878 46
False
900050931876635427052047256684919650597417730841578203744927897420037094975 15
False

1143489292890252948465212815991069022261729828637647264282773505196586931573851
False
2519802164358301188845638268404815791672927461843211234939233853714497651052 4
False
9725036695644409651797405504403140840990614726094226869606530906794647204351 0
False
3789942280962836717311678515056545845765970996535332296480080930560320153264 5
False
5066638500311710528234295912877129826735070117872288786098993878364107508287 3
False
2776402458127893941142652952237791481521655389980468244735416160916425174936 1
False
1056544685213465229228391573915210842699528146579115248399397554056202624241 3
False
2845700005528760997278214817544771784567362398657937191459351096397969502922 8
False
5950793228761180214343302920471652282572483269119804137586836165358548045061 0
False
2930921293095649400965678993183624857595795233985109449165805817086116834878 4
False
6912743932350797999477907940562583978582337068905323376766739568180171133298 7
False
1182457716502537712067516428892837872201233174507119128235712218581067133410 4
False
2975992348438491742504181398980151379134632859575309877533133815337156542511 9
False
6890529791667259054632893655273952020150417242889613771422534105346793475185 5
False
4524264920070349842154098993110251449416640023383406730282602761908966496362
False
5716650323813834750890685601409399776045050860091279821728633277749925691104
False
1582969070773334475927538734596434632119246879866832562051976336451574658041 2
False
8285549448082191697319950916440282293346297396337987484196750727214590269193 7
False
9343346493061536173980800811407580924098913893406471272873552726027488344959 2
False
1928216805507039111154617161861463944669501177217851652424113279687732434 3
False

60198514541670458142798176490957850248408775072987371085932007916762898817680
False
503584660652309287677119783356662140504684659126558177393296309804229559355 23
False
91296971491728346309443147076754163844889365965784361052143214826102829752730
False
25392994222108040468125733835726983661682102662237371404456608889739325548749
False
56046039074536482047338405099764287645436576814706415186703988921065382703321
False
55633582138637620354129316990562770643303987576291977146464585958542731338325
False
16543369250761550282038149082737533040914837032463730886499518609368239304874
False
70107761286209209134575701425682292369824984224326041366858438567261509507425
False
48844151277444556957674597345411794602666983202991838631907480956864985446899
False
13313133545899856559098737238969402556904128713432485140291313444314076617163
False
22008721690562879513809524867468254594700743722572476158027022421070264803 9
False
67190124846333735192465433446135442777219392965343539196755337721239852605500
False
27173543802677558618994795228502373464017955059198548846306320587399339175810
False
38792881993075947672456187054205023454817918307302072169642273192273374737586
False
10800057434691734118164222588662640731791071241901062427381045367528261490987 6
False
39931748614759309299921143893239318315953021351540284427604703096879871649398
False
10583426541778516151333653049734597108608922742738364996350652397087937709975 6
False
38155038935311774634552656217252531921737311867036729068139655229846499413110
False
39815960526358829260206396576023966723769545276273048046039323954806681460279
False
49148629655987613953956838484940628864699652854722358534184424808384873700 2
False

32485384656819626539254921854521334132248382817342272844246265631851348494 32
False
36803654820754217111867306870882785031209556329676032047492780026480380211826
False
64951492309804231923556978963774416699356763012801229567879604269883644530165
False
58094189190621741429604512985779502915629514441785336107021796316335790820606
False
92735870131405353837221258972551721564039036080731447138465947061152027032893
False
42888713529273841438621242472436615855117634546748463883069109341579808274 19
False
69977318249406145061135731536566630767429660659437128395861234935657269892328
False
91362619979345843769276841696118429760347523786648338620520056743019681876552
False
59459197368992205247674066991879585796498862749666817559689021655723426487 8
False
10591931742770741910809602223482123503769561590491738563783803010023936500924 4
False
63227581225810631510941554025977029741154248485451962843889816627361371732006
False
69806250347803188260481999982508999870206485522287010888563057268918651596216
False
88390828252665988008482337917145383094761112090224144522876724963919050880379
False
39443210229182785199228137510805411419197662721901894119119826432094509197613
False
19054012996132243669038259050399639369599622799701838835720661446659933289649
False
45764912882128997674889373768940816838851570613095870690696868825683015451714
False
73640374529181756486320242195711108101949063828844971682097662724054782519848
False
79793200821589287920012848863465154574984626440949457306021803059798361264896
False
84724449955745402593279941982969611358277204031191216731195981882706811944482
False
37825550036479693344361940658129014367037379513416143022773940828766243357091
False

297440497543406956455290607330414454490897872966034362573910431595682653050 7
False
506812848673735402175489294997432441002986255287365163250295750798782726189 55
False
993141174276756455852605729153595312797057953176339252705775371315974653485 19
False
114708640780135701802891376737661915727913522188480288433922508637327926057 136
False
168794183554910100897436334989915483678024158139054677063523574186592462682 96
False
369138049654911211864805316073395847840188367805800210548482691824390529008 34
False
688100458575495068752807470507057629597658761412574555127797562000068911934 08
False
544988266980957881472806543081005645216516091077119160898205219728119386589 68
False
100057576658373067223668270795722433710873543067646694275404247280250509277 521
False
666237298531048620027301470877434213440265536238989220583025611077902773334 3
False
734435619300512671778028251976834104679610299091139497614347294899195891967 60
False
111563176323082535954825587300895609779520837488795162573137246674515261806 717
False
149463776583119883214029925977311898707439756297185497002464939052362727473 65
False
479960196773527360751707734221559200675694219520022091873531175918633162927 57
False
585574827753367892958612212259575928399367011225656244566104600132967536077 89
False
171337710133975980755611187989771393687368828226967191229598251804374015353 42
False
415367224681352422446232663277800113126377616396190274232319517125681794247 02
False
111483762860032724772661194744452111801399741455865188057694053644050656414 904
False
935852530852193091521788362177453475676376762464565988971121923826588245575 61
False
114975498550776221029907264512831734419415043401954632404737493371488184621 163
False

71717024817355709566161744041265206591535490272106967875483041838750728333326
False
736879321061084228880720462204998184133758357511703434105668543539495964326 36
False
85428840982003146790265454427416439117051973793018762664648104028108939789120
False
501621041188064835064253611132737968764986764744313932469199984167264886468 44
False
18273625255181492262472268731616630862845317392179604541454836488412041587867
False
44367768221396472330147837362521395731073047022645621015724314093566456241479
False
20046222429734349665067341015194656098974076331438619387502206327904628020267
False
10482653087374057657738051849342701617916685160841008428343011936916064996805 9
False
10707010141200119488083411970968671661820233460412748294228302075889128279516 4
False
45884902586086292060984768310998749697809722664658072822207956305636247415048
False
16445860464233811378424878373373961567569667125301117974666259311104678822221
False
16932388415982511000076244364867857606010298656926549152617588557981828291 17
False
19136005882987366905110046435088041733696660147853780484825792935053763068415
False
49641148513437125787151818904339071452247066694474271612310156926601487110507
False
24872664046233825357179352649875629062407811032299281458459453404201482461335
False
13791998390329471090266358295733043861842872015107381560681208619815765985154
False
66945011157479657407380404809355414426957338089996004164148737113397984453260
False
49505745834676084668468918751916918939816714730588378704689195789020109068722
False
91449246811045677846324516270266108120130352883773269319815101252872401382199
False
73437598327490581597171563902169794274426463369866178721822466920369054705747
False

5252812094415643801380774044418517529389925313585326612708039840731537022233 9
False
1035287698747392929396958039775462462683243162635493895457271900327973215079 31
False
7381943473115910289575861307860938980589128678915241064152881740974506810040
False
1064037651849809831752890253874533375056333946057926775238440279650873005804 08
False
5668609959546373840735867454434084773108756139867497465482641071715942862422
False
6508850120418667008933373308163793307191012465720107424260961895000264800918 7
False
1022314923128225285931129784447627957665500486351159859062792930692602916831 53
False
2090476398588967208527760477492557693691293116295503497304848770133066974932 2
False
2372639773997817976129626315465255704154181170052067165758230413891246236736 5
False
4597241590510346014610302584298319187181014915832463719320398430345425636671 1
False
5190032753683510011400045683663128362330249890286549743113471597592887424337 5
False
7285057063848784574207439124194848192164523011784724539091564743986081526884 4
False
9218878575152010286095181802806693906657756621474546607589426417306131800646 6
False
6727593725464361177666168493503644685040384989916608071529937178342751400377 2
False
1009023087298816433739221620040627732310549224450645086081548239240113836599 96
False
9753036233032256354791850694347565331436383799915663045408618730182679473871 3
False
5349320162157376420221129933886281723489036663146361865557908533068156487790 8
False
4272787771544362748057817984151022864563877593432664603623106747898143844 52
False
2597428243630981633594614163357161271643445826407209283130380529103973230944 7
False
5345740385974878502180776974544634469365177465924651512956807866246882720542 9
False

22693509335744701431305842773203898350553262758087553407159382974131839126 69
False
22040631620920110192786200626065468728608445206581551671092340930164674121560
False
96026857914483527579104737987776543526861944129344757625649650507901110949032
False
16825929622898933090665614981375553462604432089864760897726265510153215218040
False
26955982469876921300288552035929356224084709033895451556579833552001143734212
False
45821718779627733367981850936416386369025302873767274826624355908807806535208
False
10032879951207345327192844036925155701856893800659240337656372763734651945737 3
False
91342762748211619548882910850327404378468474145621534278483266785566025026008
False
84085099782659998302921032301884781649046752802412360128030163211332584189 88
False
33064465860761695111462428045616239503228766371373498700945132072356611741217
False
79386073422166203175866340331287616938800385878421084764078570835499000953519
False
13542839583473351527247091527004662757450888540731809264865482714210487301285
False
12366254838118340913360585657685418007565626869795060912123281678691867538401
False
61010872203230513195076986687550754029365535014576285080097142082086559660330
False
11108511825446270075595266374210721507701351235477984132042398678152233147087 6
False
17318997309854319086083294602702390075224792047335838494862853094073504556001
False
14210790462168621275510739205532816161489219286057943477429830846263492365275
False
48887717681039181704848736629546007076987622904334366338514724503440140911239
False
51893053546683504460937834492624685262378493685361906748753149063384616827694
False
86098442120418376600307577980206930226079302294799606253590702564787745157620
False

5308064342767008222002321789667779502520672767930706706016843416305057018895 0
False
5008297775654997985330564310037799182097632990105821546431291380127829753227 3
False
4273609044199110064867233015939283060770699316855846278323672477851343044225 3
False
2072677468449163732516275168309822553054593796340209311093022469210116046831 3
False
3314998280560130241412071589170171636516208130979151000799672126579607296258 0
False
6541717402504984690071632529511351378966129257597127547901926091573513416043 4
False
1054011319773997598559633806745634517612141009257076553503577645283587564553 53
False
1692746166986568609093919140552177046014636657124078007932919025555714350999 1
False
2087772502333050732294061900324051969841277616365146641414768059302501176951 9
False
1001513977375160414264519512700596326237346979051955844250798630491487616600 63
False
1523696825900667550999484765150393926705917192766132314499256933225023654206 8
False
4389642855617006999981534059589305201593457230514689074715639932405184288208 9
False
6967754650215762263734360768089237108728234285847955226294393311423378548160 8
False
5283637113781605959477543425469326361841955580055224625310062183018574249531 4
False
4518556795062236654679745133379418450255557285100446472870676872031821292576 9
False
1060028156983481227602424289349538771671638581489630799126695995033738425591 34
False
2944905682044335787233723509635190995663665787752014913851034514081267824293 1
False
2742988166333254779750316319176070004843220373709271554639628237373063709515 0
False
8065605241206121619143215507822085945113225156685019770217410522052569141099 7
False
5371812776639169027215130435214561615456528442072167431724680373981468275692 6
False

34703416660684051733945076465269638786172251988391747097304511274457574388364
False
43242376513217797408735127157979903866028215495723113892148399030233468368905
False
32540485821012191678747102874600003159396764611245722659837496447173669363892
False
50099281590796648013000736237165571525028881922505003837241909970746658219168
False
30969190071936109740573202789904246461501225438566147351660682844900667008527
False
10399659719555245499771585492167776230978112952689251688159053004379810913470 0
False
92682268266395740357731158973328390043070297839759982994462154187770246455308
False
48723186204063101254814366597133095015318081475977694370051945802238130130050
False
31733550551382880851338958508023754621173409029815483177602730173011032627462
False
72820513503555876607071589129214552164591785863903222948668593877998145935352
False
11320718481180807662838173351465744398802836760239418836535209716554837237188 1
False
71754038087666620761043361530506542508215579534349886261966565331098849653505
False
23122222233018054835161018543804954345932777058790188551943334002325975637026
False
34220809065126008451391695765464296739523589092760288922873900520810688629298
False
24861416063490643995876535531097976907285731018143710328237775158092950263377
False
25582659929483414271953769463015967797892795374576186472598782986899401711974
False
69885132009343179505257263706271595896371450998303916563975134601259959749990
False
15652489768584101063053483239276892779813053785305028966398731992620416550733
False
10591365972644180456021078934971055191187588569945408422964762749860835693345 9
False
51378097618014577140048587760815576718537040991960572378821037909299208643738
False

1152420226061120103052977441466170537300998301540584300776439122352039459559 69
False
606229056559563340643090680035774838928766302941526651515024535256395660802 31
False
424398018294577952857935751777142798514732006677785883858550709592310883195 36
False
794719395510273812175214126510653390128016603340660635461022500483421832593 16
False
784222904967185181747746123172994570838561782993482537670096445601106566600 01
False
156821189506074654552785442440761144822008551750283092235355296530265177754 70
False
674264617622645219489158165124693400284015691545700202066168798115909301700 18
….

Пройшли відбір:

P	45231284858326638837332416019018714005183587760015845327913118753091066265597 1
Q	45231284858326638837332416019018714005183587760015845327913118753091066265603 1
P1	45231284858326638837332416019018714005183587760015845327913118753091066265609 3
Q1	45231284858326638837332416019018714005183587760015845327913118753091066265640 9

Параметри криптосистеми RSA для абонентів A і B

	A
e	16615819792915349664376146357648254978002878321690350934170885982263046687279038198505517009507478074534588842967365977460386858489070649533304325932216 59
n	20458691299350886687582435605172494701354012787769154934270571050600836227529306430590154730314575647025079813225260810983127885102439532820809479566131110 1
d	14934172428792861317905006898817665522285374194988680040893590349553152217265727275511461166697678965534387065358663545488343602413422758568156230702363383 9

	B
e	15526008223248057671277272680146950529129320993758625737507282744668166332937510891676110882308648788032438858405755542200249585489867391568284834249459437
n	20458691299350886687582435605172494701354012787769154934270571050600836227551922073019318049733241855034589170227852604863135807766396092197355012698935003 7
d	17211978155773251575910620387938252949037622268560408307459037881695337081354537965394729730565816831693165248164226311783907288122351851025411796374949757 3

Чисельні значення ВТ та ШТ та цифровий підпис A та B

M	18474616013857947621243127612531914821540199317338825870466831166922251632378124599155547999931112804204199873625657662975312987125078858375649515300849959 3
C	18988446754673616343871436028628208475041323175137509179676619238475606472869314203357848885664314657332905279482051033550846232561529406307184212885781494 5
S	10790012766299290183485606456336091791898353978159701364989808689258077103103636579138606816832489693063543799429263328576597926449936217107814789206545252

```
In [454]: M

Out[454]: 18474616013857947621243127612531914821540199317338825870466831166922251632378124599155547999931112804204199873625657662975312987125078858375649515300849959 3

In [453]: C

Out[453]: 18988446754673616343871436028628208475041323175137509179676619238475606472869314203357848885664314657332905279482051033550846232561529406307184212885781494 5

In [450]: M = decrypt(C,d,n)
          M

Out[450]: 18474616013857947621243127612531914821540199317338825870466831166922251632378124599155547999931112804204199873625657662975312987125078858375649515300849959 3
```

```
In [367]: def Sign(M,d,n):
              S = pow(M,d,n)
              return S

In [451]: S = Sign(M,d,n)
          S

Out[451]: 107900127662992901834856064563360917918983539781597013649898086892580771031036365791386068168324896930635437994292633285765979264499362171078147892065452 52
```

```
In [326]: def verify(M,S,e,n):
              return M == pow(S,e,n)

In [452]: verify(M,S,e,n)

Out[452]: True
```

Розсилання ключів з підтвердженням справжності

e	166158197929153496643761463576482549780028783216903509341708859822630466872790381985055170095074780745345888429673659774603868584890706495333043259322165 9
n	204586912993508866875824356051724947013540127877691549342705710506008362275293064305901547303145756470250798132252608109831278851024395328208094795661311101
d	149341724287928613179050068988176655222853741949886800408935903495531522172657272755114611666976789655343870653586635454883436024134227585681562307023633839
k	320250543651210761079015977531952665967035240647571315881264249091451071303690697713214668423520000009644502648766522408529193184998491235304835831321877 39
e1	155260082232480576712772726801469505291293209937586257375072827446681663329375108916761108823086487880324388584057555422002495854898673915682848342494594 37
n1	204586912993508866875824356051724947013540127877691549342705710506008362275519220730193180497332418550345891702278526048631358077663960921973550126989350037
d1	172119781557732515759106203879382529490376222685604083074590378816953370813545379653947297305658168316931652481642263117839072881223518510254117963749497573

1. **Абонент А формує повідомлення і відправляє його В.**

```
In [467]: def SendKey(k,e1,n1):
              k1 = pow(k,e1,n1)
              S1 = pow(S,e1,n1)
              return k1,S1
          k1,S1 = SendKey(k,e1,n1)
          S = pow(k,d,n)
          print('k1: ',k1,"\n\nS1: ",S1,"\n\nS: ",S)

          k1:  476309394682571092873752115139629715979655981144727770592654785577705291291993174027789407271035817988305613279825406262547712295020612854842762939148842 14

          S1:  187907483824358781462059550153521628122427001596311019267999935850056279873151552645169347974623061810723114597070920972884076466848896035441096508161596217

          S:  933289563542185238754268669583488073155985812271769216677196365336502857035351953333875665622705877609669925488353536435482990941081204835898520963425605 24
```

k1:

476309394682571092873752115139629715979655981144727770592654785577705291291993174027789407271035817988305613279825406262547712295020612854842762939148842 14

S1:

187907483824358781462059550153521628122427001596311019267999935850056279873151552645169347974623061810723114597070920972884076466848896035441096508161596217

S:

933289563542185238754268669583488073155985812271769216677196365336502857035351953333875665622705877609669925488353536435482990941081204835898520963425605240

2. **Абонент B за допомогою свого секретного ключа d1 знаходить k,S**

k:

320250543651210761079015977531952665967035240647571315881264249091451071303690697713214668423520000009644502648766522408529193184998491235304835831321877390

S:

933289563542185238754268669583488073155985812271769216677196365336502857035351953333875665622705877609669925488353536435482990941081204835898520963425605240

3. **Абонент B за допомогою відкритого ключа e абонента A перевіряє підпис A**

```
In [386]: def ReceiveKey(k1,S1,d1,n1):
              k = pow(k1,d1,n1)
              S = pow(S1,d1,n1)
              return k,S

In [370]: def verifysigh(k,S,e):
              return k ==pow(S,e,n)

In [469]: k,S = ReceiveKey(k1,S1,d1,n1)
          print('k: ',k,'\nS: ',S)

          k:  32025054365121076107901597753195266596703524064757131588126424909145107130369069771321466842352000000964450264876652240852919318499849123530483583132187739
          S:  93328956354218523875426866958348807315598581227176921667719636533650285703535195333387566562270587760966992548835353643548299094108120483589852096342560524

In [470]: verifysigh(k,S,e)

Out[470]: True
```

Висновки: під час виконання даної роботи я навчилася шукати прості числе дуже великого розміру, перевіряти довільні числа на простоту, познайомилася із основами криптосистеми RSA та реалізувала цю систему.