Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

# КРИПТОГРАФІЯ
# КОМП’ЮТЕРНИЙ ПРАКТИКУМ №4

Виконали:
Студенти групи ФБ-83
Байрак М.
Бєляєв М.
Перевірив:

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

**Порядок 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 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 ци**фровим 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 $0 < k < n$.

**Хід Роботи**

$$p$$

$$2185472314945588735294549079519196621454146110388009570372772079857250808885091854817121449144647962510153507118735134514128853219547209977516921585693552991760930692700548482524741927175188312856638073113136424580629019436636610052531818501611659604279174945243948358213255436419770454357946785067251659579596651673613513061175814360426310391995108471263222916971277635345434197850983665931368505357439238220493064538072159129808799206302278235192616558835750965962371339230486559131753866364866510629230633512029766265044541481062887609604988022016227540298657200283313339868185979073591801201983367761115568931934570837812229506393690731063597149877197642841730490047398824037364501956363302552682371514389963600809649461938276007040672779708610042290570657312907473500869359411803197630773076550242136281781969237146436774935977066573269689920322516689171833568533400067916266546360894533273678311916219602267951024718653287096609221362454239142529321641628769286413945419704973565752688472318787627279220454342043963214372205933059231337898121257849843094030789349833216275231883304501681343661662878115646140225224212462535504871546158577998273444757798548897709061600871919274681530544875978431981296917761890896520015901723263390833398295821399901660468424750549700727955757561453218773996970303306219542430045361106872239859804509244248411771439727317431451888011706099129548361016166145843101301181489473249744655644013385248691915067647586563606219155473748285002223467381826847299815853937675047429687686308398685070646826188559435342680662847599851670970521480006454966179664214687183746327299823380921241746626919850427281321951428625468292785028018260112447216785173232460180106471027046468150417068171 

211896039596444431646826003406871678311223098999066812220186004026390602444977

190116883393843015924550059947121262679184828663672862849463251073336993583914

211640211417876250846313542886679405060414213174296434311370237797335051572619

181734345774055635813546321474517437597574562932889568463793085595999383717067

195729159232723366776012359066657307604694945221234397503949049697668622997045

146334712617836802589836407402011923486031314020970434199935434927962932454620

143239150920827053571178230730047774726624191752475737624429255599492859680008

185924454272477917505743090178386908039731473320305967905596014336662237955243

160151813808820137268284126848726042430303733884785666539379330123544463291796

193466227216796425150108126382508870794267121746542863775948411365490325642614

218239390584437900468796323160677626502436185644019485408806871637510035700194

201618829206380913010723815868962580097388497561888838987757818294460189483942

167589776877028782594588334126167626576094103212950734199891574456271887246119

215354789306366740139998182739322579824302417335825928424570333683077691023103

170690495485884013846865534922559328957043403334630131973269336523152626125035

169595571915881388612048345034847333793462246441276287603483527410248787231879

224188635332170720138474634897447018635644576362467564795428449060126794837865

214903258390869432063267053066716371271534779957188441619327881399002021550266

191001650332735553748034992233909909082588594261843471667361905320050460948583

208851560555956663245088050855521295733628431136704471360131390395720778337577

175106836143343680949737661270210802873746814037572104086756232359318347108351

172394790293610141858620513292468331227398519885119495682466251313692688835628

136690235030088802077204797768228531887749118160908911739385695927698071894354

178456423593164159800231052448563411971923017956426865317141042656160874045831

129248441082343788150809234692159844793225383835993707340852019384040282789303

146373646256212211516947233706500494771006364543252144855699361442932927167019

186954460941496681591531550183522025990111923334757768197804786566257872784 72

169547785338740556146050155000370503239005117911478424687157543952114079251756

205178429135172273643578785587164960856026850744059944716751708086817177405527

160745425805621168652460990960437704424144960438518298507796426597407439805565

185485391223911109016877663738974824059211264243154808114591012708558904518076

121613412646836380629738772294024025863950917351697484170005606394601926908094

156345964673647859925083966904068330666019694731283132194057711023004479581543

174028846518268406297940720381967695539784085169710274838309610713159962992043

124948113076429502475577168171231800221950549288664253766702184747126065245445

184939555376796121760969766775339564574389666595793618583767099327997054765728

143060843797810813252943062103997098928618990671288742343730662073935223893254

228374258994943963043334894711415862517735154362438851876300812011125449748960

162484979787529217012725134787229121666919489856013773529193896616300305765166

217179667214347854670203307136878772242358683828847745944250897117048252094807

143934331640262872598712593466574967063349216780423196934509894429610741322946

179248096650993566112623973441673919474794847704816177804534735613928052849147

227259571250381787222276363779493803295555618390207187643044400282225894721580

193442280673385402002022789347857071610236312411241484455635215541503158581461

228949028578564934399904342305111449331138719680863304634499959122009921249820

196971953787612160793138285313424644771934551240840916427212334497375329910174

191898894863096905283490691248367864317481724009282078077082736797828582866661

120611858372743484266059536191105738623295432710640165046259468414329813320825

120659209350466152079741772400603810958937621431921526939385301064580337734659

149972539101245992435893051451947656869119773542775360484003873513213229365546

184708261267194199890791490849496098497953803204644487105606933218431908536703

198755316342247489979303049969647298234428798693594461043022261291503320120150

150384963185859153711453101834237701244679586301088566898071349595263922702867

172828518166558139082768015212474679063197013775397393980326195163196332743867

179514145054148603034734950638651365108667069925225583455171575600588141239950

143961387556209038302019173497878339543030615779254312904972105092781506751957

153798058515816237353576232559043696274361854928135926440555464062178561615019

148629206056702420155558301865542556027405906941923988341063601862935102452494

155654824497813921672071809491417146405969782416250851350943329159409277141242

118533800884395306139084325568252303268331564675477992874179301134307394559840

135140562015719295793049280272754657246864949123085047367222803033596559585750

162519127489252688701015690298959110478102600528921992064435032712498803824334

184057280831539574638445269883408800711634811052724458190170621190688472962409

183112067493032064828568123172855187816778038049537341367141259815807406207199

125622407304161762197568153243906995203298578465179465568415613016161395527851

229377348182042827095929915591749806249945115672452550243682992247641049492769

181224688793220541077100624240259674049682728714686880915430723925858120491312

148463833253855352527961518900844461730841884869750786446296697438785496477412

176136624079852084513149035744304885676424103047681360285602215748587105065874

226335361268933954671139639491098135664797483015024564625267449721166831442960

208740031995600733510585990710362222082929064888065954807409275847065213745205

186548003647368453838590402300014051384415039481461820885605423641753219936459

211730676302119526715741870832255485319290616640322008711816138383500789460794

164809024773492010604716043187003436813383011202005110253069351535163740801875

188718947452602586075141980388337902789005869824092013735150258532748131428975

148295662816924983472888761647359983616773582461091424041961723813107964889158

190797254047919544107629565706208854499038156239547120682208581150430067128086

207584394003277633951587038049214931343327412526965293026187818273853358203208

149179502229949024474143742977598836794715124863822556486220823378444153751041

174302221682530914860433246989968296048702530860015873510536647241875219449285

136703602424304310418089707656811542321117837967305031023449856875945441695707

130556485302360568003556908472418646801055450135133913110458298614338722584963

122474445234166789215752386060004235382269340534717499455178420266678454189248

164103931818538592049035447879509226487298728559497851551095536509034061039565

217213112013703855115101226991097090292042619971379756719014578874212853322483

171458769660409193251726647245406446998350785993805176424517257189224075526444

199425618581146162844920390163918920328880061770265234782062701089782298790303

211577801306063899182265462400118821803243165812191424069312430590229143649600

123908864717679746191516768044829566576925429715382644953269073729016251996525

151080795433725556284965643754339356765743239456135780606847448408131555654933

221221176152010416868483957834130815383083736951610410833480032329155375670367

149708578381908649024084251116741549770157116474368518038008634505345605933312

152475312738213514807795952928651383479642917624159079620597706212067155583097

127302300723416651507011298233422280800912359922526519021598028654019303662180

124753639944348122425198528976560666340357314833840184979819560753685791630718

176458679967271327980098367983327180217014814143779845672411404079022712395246

187458711924554298561005421377208411444467791159947014565239706672425513674081

177116845319280860360536022878755488224587303555538166870706457025045335106658

203033865225739910116415944750435628225139014068263887495491558305149391349749

213748619019075433885361668746698729724970991783412871927963773147615519919562

133570063809574091713596413023222409384458694060591297291976619711595050333999

192272528457270742768679906603881522454939733624279197880324473983846920080621

194879799469022312941585533022891363522896501472705937603075984466199118530190

117114279039268046541659201448488137966317367229001661313405717633880775226709

201250657889021367593232836602017858605525506075708909297626380173883929683040

128008004791611632491544235793953914875521295570767132646946615559362884588892

188620665328851129774257673655310936256250691648864144418691770694036205906492

188048279885605017732390189556024366255933955629760099492513659978439041428422

174456452024271255524837824137908482606755707093061393627911191370603041494901

140961227920521624834357485988010420137399920032496146608987519280858894043826

222013432566819686374060788018305315042995898441585571596688634016223578621339

120332451417365315778196668469097951601637105680350659432361793494359670384289

171863377029264641456901017602565237986524662375628413881307205014145488941877

230251204791246114810317148011247338631560418014026612734889512555269806488142

152804523107803424131776956870411321719423954650794222967021389223580857889620

174694877912019892602579311989991259551851355851195718887539148198103829115702

166941392680271716376752414168690780466656252031687100618499450053914149212511

115923827279331300566793165706478456832258152291929490527921767359353695284072

115902541825112213878966955022151036285982963892606465395392889038355993435227

174805775592840040025308278676668220011372673252452059123679359343479982684236

145020496929582701057815782528726169953742987416922402477606542847287250488350

152416458439561513296695302012080661723503440478363620790369933851231098230260

223141230776309296973172213514987831585932899176129587851085428359449030508583

228559792733011453790681794379003882583861218301722326778768920969398873170288

180395462676327305204056378140426525625876616178575248289027929506811293677435

181670015913901125647559541457803872077255608637269782792938847550557900709461

218758568662122860689423759486115524689978500491648554166707690306842817757131

186265484538861849119750328165271218661093659540885868155384188791490460382436

14247120126129540512971079368007348484392648527713891996950354686586615355743

16733433030858792251274641545842352251733933827889361721697246582497025068306 8

13066925327002245393405628813453179849606985661875929297595498266601571165874 3

17333171741545666072814108241565263990443543844397512047118880417862370478575 6

18752651535435761317674266047567854642837726456755341533926632675774251788826 0

19225670904174289920890912794601192856402541210336593927588115370226081878048 6

22561102598175433831855815685910330739444290424392821203817416977253662516253 4

15087017163671170171199107844791484267109262661492905881493629808098127595263 1

15389148788978224178562648930881347513800359852340271521245747076959413157612 8

22311246854266113860400846570564963678073201192683628847940869350519213030234 3

13647612396168342655956849164170033268646566112541277209571202485633241861125 7

18671346187179954984586089875468136911554187897035979719306049357785403139589 9

15173490211613648391815827642069390704487102074451763861893175701986646079830 5

20675449800709060770175707698120718343196150493349884133322117759176249082417 1

22455658453592746180257936659226340203718691684651699005668407132956132455835 6

17398515458279558041387159595758657035123736693661165374015844745849747633520 9

16736471667071972578327797997088662550000684354942489485880935315594257890189 3

16718257159854085974659331195513603435267429200849298364951746907057030828974 4

19222726727130596414947656275653674471417652770312446969668248464566172854679 7

17817101779035258480662176115796677121971389187620993370904191936998062350452 8

19797432125993444715035095474469154048727588931474976381522988949426040880892 2

13781534497766721249625025737483670238941950353027990306172064736142870547669 4

16661728930489399690420509359841949249370549128396415926697710240531448653720 6

18788725622423132516785681450597357494578271461571452835463249795394408893108 3

12919799961181795682821771007071104793081633599647740275892593051474249006112 9

21036351918704687682310312427821493385123328716991035154228126094482187214335 8

21688044877946446296898227166254623221211428421740404978817771636578415658024 1

22233475896672681747931274177424202511175016336506340958493408181616758217995 93

20992406572642614207890030948722688093084885414977717265185404999656105317168 2

20448661131019721552078459663661425644386760564045253956713245827417111836040 8

14418040064263496306385807447784555204878148881609385408309356619115055911839 7

18545408714227211092150934649500541560307897375248897196991448950813755577725 1

22229561771432664811829864306953659724205326743166367201485259876991980182999417558828627276625439082913833794713269669108030260396986908069022431709420819317591276421619466719232369358068638521346977791966070466025969962995216543057721382522069695815554767597707370340572471601222593468450283922748615674837101811834298533683833751003163363579966042186973579713143237904497330485322523616111674430103996411412424974911837385018479804767867820053905644672511852350880621203687018110651518037255850580463692290116724281048715706062284957697052973515622976662469499043532432086049160685117533247122468474314536050347832354148922070101325986549258792415207577125714000113493535007969883600273275616909413612849616863477047549054824690678676947864281212838190634711859609002068708014118537012391028099596819517905297978291375841375957777588997519793560625458109221780060283104190449095348523590164509595605821770438847380135976479593543170814823483322705832794104624059762710719412653685071146324662725103448299779006314205052851268331524840846922813697616720738297349641238363437408510779766834119427100708180569366878095413645699641251923122144915973119536557169992875263921048437049167225364711123660275010582911462450935933003294393724019512082391513965780896927554384312913706247965928204931632097372994821366354223674880197320921598682320742815199231715683729331587046717995067486951820901233941947212525300487953004668231353313819773423349747640114252042957770266633205646227941741212003705211742149151082783910768823781768148578339920744989444488582406563992187794168938583907069506884431728231285996424061995998405998369756676253920661564565155148138518130301540687417751249624348098324813267459921034072760095312139267551832214101202068216912905867009304819224354488571994713553546975148952229555389746797532155522862851262894091671989913352263912779559084598269637151240386854342346369658406275638471179282982638316087061541058441254852744795141205215381850375802798465743628028964609016589573023552563093947209823955156352207558773168841764303041409922161895663692233850525400441014450464735147149431530660778243105463117118668658405631655727613108679196749701419906283973522201967441273246882866409348488419366379391623364744820951461011004314530518654841212345678910111213141516171819202122232425262728293031323334353637383940414243444546474849505152535455565758596061626364656667686970717273747576777879808182838485868788899091929394959697989900

131122308267124161748845022772426372705121330713814242339388146367944000437762

210034052747950810448845502757488248848875068939644328915534913322727714729721

182151121696908174223472392233325063935169228714149658550258544211662615570167

164241250089409547402657774400104565055617625595089623373478394689878012000367

136755456784405619542470520904994917938371660630074639901394818314173054271355

166131702567337848517735196706125020226332317687189697392202529292089300552791

154852313041477546415467013007824995017455626122510451983158056815858285076842

153509845657747013411013416957674966342872987475345828256290340046181449172278

159909836434357547692427028438654827252514677837998485967704172334727039734388

117590422986895934650571796845500568736779688070122895499278279613117211748551

182767426139465583261836751683179735395416928847155147310934415284677190069604

223203373560568595720392623494725803601020966882529977654741188091068582252681

222523236034421072689236831304840567849834924883918760303405099002596696285117

131441872458102627604612172035204322053990002590501371977873132042986425684220

230251908467945235728000782994993856066864015605513597351547947168978112183408

121472080669671967851645672901106611938018921388782928484468288944687411820761

201714853574826905039973842749287175966641481348050231951313807980032805683893

200102709183625830513675067134219934740786829776427204071667564883686914645750

183339188866702323138928073955340977946588995641587391969896281928851517137523

144171843331718653200326469786646900281344871666752481476810269470031740252744

165033071108775305873921100904860635150145426884369366106297874457550351845631

203835219400871308314477090415794381404147268250074790180843508840124063078015

144384605780640522895680299137286756637541203618128615921307430182324112947441

222165401300771207220530794682081171060460694216254372314707096117530973245119

116837664511508625111938296809898056947727209229182176897719117254451983762846

# p1

176617406204546987122841652862188681139868260430035164967068258243648739793746

205583036520135120876332051333706197299619420435229288191466230523247051219421

135285997001074566778266228842551890552120505938801812574809662081420870572096

124955695509286203045049048700834579769839153591127329989489409696977149396576

230492325545617772171082725857193307843401257379475512499337096685491460992643

20658093224539256422083522247587734019325905776924133115019591764056949869104916325992955920540014608716991640980083762396628820926767121260076935816901830822822492906236259077785481951250157021135346978054198166720888652036460100847622824531146602032511362618763215667491606726554867021486066967276988407580595021885945838007596505633459921991411733144925618547856144695693066072529552689821598193422415707162791766757891957915477692091474858330488343715541034306932020107204010860562969642755749099424996671017326928798714737534152276767058631514654969690257670023578865250349961104123640353654863987501675885727607772881822216844755503047298868522322742637779762309575284806398633754381214509881517111661652126234939304478289349259312899322009841851942893035570654020735725787014319588946747550707320982483692175298456256209975401475509784744179179508314120293425551019426705605119111792268004815460340786561016905670809996969510909622417202502409138233470865730472001852560375043826273019689616971686917208136621421630427055872030288479656355801363995182608827221940426201012741714356840317830120658204955785588489874853241842092529410810799524393478669528241552309918014081335995900860390061500391516328462200196299856923457575707028147176085018957101508828556305559668204730683257682246567787885495104470256558680526023311809539575936039939538953993853189016421997737328649803655336369388501275586721018232921881642205210586775637493590613850247791287428079866476176054394207217641503103271136465567974412422933491597415243718600715833857039143295338474421449038331214894722239716114740311397045353659707753604812013869381335293051519088553530212465136784015087565287955657099650102434024860940996291440910471017685263754239270559718772668780024238244853071541968313528337776451231901816623090815683713505552430454993943859940917002571008580946489023423586422933436618524164117910954601393436396210981695618501496159849199181792712633047366872202735027842661241993549710229336479658760441029631205871075786560914196132169199720219110097374447655180250454030808506180297293397012088207179600510281383179597271569186781889061489517658509274871314429972391710884221648796544857185155463368779780982542217128048319118886908998130446949617699826673097889949982152709706191624201044332561614693718582993082402898618490486064672520053102764180791162984312567257668571962316746955195416754320001171257470355358961125671147178333113657536910465230825306598827017762030730180625232329313140745945357

148315703852475669558540788609727423783238416219007215368170579453455298156097

148508861910329935661765407036629533106466031185949139705331323654309706242346

188673713605076779902126655475867026660260467223475029003512896719215163991359

152482989451537946162679613368650666531434384742336396633739753525244662773104

209607319412762704973424719441572281437641642262693067153191781169731461002861

133798458401277546730409467267798729138405359431822848710679099150895936658693

165848644233267977071063549666728037158050734089353332699708606666030436515214

165371948489783831083402515553951892983286078324415418158284519724191907348502

192797554287065904923102757213859573249492085442908970170596774533689926197373

141152425714147868527342982576892679853273651630584187078980469492090165452616

142007264578332697000218325595876702798296767826344222209908466172948208846666

142557238767675475388002259584494748265819764476735298025605364469688115292264

149466570831724357256266677267319305835842174021499536720528467012671468947982

120167210561464683451374746080740627748950860489434538705984824749722397993278

189001910082320612470412497066219379222285835304869640195367545705370867132615

205722062098980969743773145800223287601033912167892209272109431418588500223859

179294736970857203925762867114723126814507714009199123850108366395573875477294

170761130921977610976027913685667019762500394702920475362310147630091943832 63

148758568820412667144486096917186947575251675331355357974478570558014117859446

217245481504409325948961488211032207995200769000389916171947408386427909966967

192740706474570731005437352707615897357198696456429360377190408333480168652641

121192087742830893431840819713557119918018448296956375340726767881183969180240

210602624966404737118700527294777980745944643237264469200080111310491497460614

144327999798168444577437882988602302989250464800803519228707214059163306693936

192480759825608248923867049150685553517540424508286575687768673527173702462804

163579344550421154431455959900790992129470683651374085474138775255395888994898

174609975178858046728562471713479253817798457047861629943103755817555996087203

138149318164198742413776612147786207742526155338154386774459502978014161571246

224545491133674249528174559866408228886177058784628372930448426821969553491466

161098049976496943140294457812477839262183289801062502242202841324663437035473

202658321551290262054951891552735076815201314774543880051205795424890334856299

149046430694097814716736111081742942250153532140532889094502446801191851911358

171362402699848191083024332364352867293848808918586024346573739395932101293354

158798695258324380439265069910647462121448124719343473258742335845269644183148

122516937002106450169268317814232197763047485992513124700710760881034761505155

193651538908696150868694775702201836567290619868976267430513464082922428538337

196139286480307270856362517900926992251305279403605019811210013055250974610842

208780282843248025769388955688603719780120693684643137257652435430993673022500

224985272324547377322596680474595419466963608781409228079555267579352708251237

176047925037979330323706623938556376863304274847199502364748349689638562994582

129637689035027456173050640076195818656796947960487288694042750974694441830732

170286858608952993582807585393788068369572519631251682318264646908137592550607

191659924973810750798023608637456660909971543041538540137281676984911731528441

159309446586793225385050150070646376510220886212897422279391288687519502850 43

207509269449199623090828433085139503345183490152477572442264016811333388764988

163975437158372972305291290629465523697907242708017235497583579290531578911476

135854517173689058913895876730867704095216937786787352788698053319476169918809

194726645826882244043182391438108879986705664733876076792936449400557019978638

213733584885548511984671088109386268612366142266237294636079117868792117541409

138910389358550632830737562196611323000292192364933311315283816401014346615368

196375037599282905500174121527852290743456758552665935883816799661881887764520

215098032251940184219593536443344956234594122703093690694148359604112667719476

174097827255148837063428259896559179987677706929843865038415165563506759965763

120201262560088311239126789197711590588331040218530590703275551283998319445273

214205565687735745811004500024024302641826398473530717837758609709429174464079

213496432653320256332314642732298112253092124843717753011382971949317460265715

149579160862574164117534609281497677323723459108711919426713795695230375446588

183254050304329382910446094715744847335755763871289655666982394689842955882983

172974520462573008072438508927612982392302160342547503401590979177609330447296

139958569249884675984561672331070388466965991945700916887662240575512274687681

199176241336472669723150648659855146121662970409315420599217525162695995577345

222375193694681741738770193390686543871468889674741937526678744085576014605045

227858187919109065718998892001727118543469464687360792114253193867001872565970

175921889978743954870925555521659035218124766928325348683877756835342690612032

149855295166423620591527150542661278006062019592581033684964804421439319298027

171021039189631495252109069714491919865220133565481730928618541745808249514873

118044343041814645614801919986240209028213158229942200047563525185804225705952

124861326225917523366586472076623311089293936906910746983263100653424520714936

131881452346784628838679371128451156555706401194774807186794295447022550675835

204759129607903957378421408147810139428290204568831955904445554642289289639156

137687974710534417394185071391856022077656944067422276021896815714418732782025

226408818091390387098077492260632584907421080817419005736445867754552492552649

125979947786370756558490393685220134303584632831494795662483417733459434171405

202397673899163679390339226465345441306364081780949281763818884716675189990688

213949054533461267019863214535057054947464543824891914971257237667896452113336

200828194052964171296031833624824200597775245479751155198533985265380679831017

162287684507067247126832335368694180194765736345809517296589397465912940138723

136264725042239010381409983181332872186217517450960432714872608624605133492253

161400580719577275603393865235277720924532588286786221964955095195640499042047

196440115021423982775900151942540662083247341380848238517829637283945007797901

218583263649769352564520814492664872979090232828002116012991661668482356555782

138732760265770203769048845716487797229710875980804103670267375052617513015979

207133596575474986744335300588452433650948722618430469165091721346614128626703

140754610660002369857923431489015119256587935044207460916418114907879930987436

131205850613928397613351197365014010954123536598536743914318349351570660864321

146111454238935413317962375774715776608719994692784869519065269502834576794152

176652960952056430934366222227389290734695412464192006483052770672680261810581

203512553606326867790694889385703349831793614285986447734024919402796286736219

130775897384103122992963487441224194770551280128434645300252883372361123871570

153234363620416297649995413282937603647062710398483408115334084674579516640019

177989182492749582053355252525791474074128213803164161238231505386350484689825

126525133956190668557653252305046586429727994893371392708881244068930890164760

144383108266823934266652693883336834347120979322157550009378624147697979332565

127847208601375016222795364789333206847176868949911779192499023122070952173358

129269903457924670309540888099899530221971333099067631219040677040333599565740

145632835689157616904331056873836523688407982194288379008282116043525321907821

184855199270148839710988327390612539651447447108303993723417639144767459088941
204197322502846996538804540333065369315445650355347352687756847377693511907670
224355112587005931043614498203284542494723797948667890064966177823489999874381
172345915167288049714387884111849901939187680644430652225400203546923723102496
157195313228812191280642768901619359956016994379945009729616747328165245638717
215254039594852364676483134890126234643737653209693272010930574439303582912012
200013572614592801552259314483201384319504293178075813774722408098103458946987
131718634712630597859515917391601373488268825876209749721345406965054776903100
199227658984273388058559503491498751121536940711732534393737982340901072055646
160396417271670648847289493893091176275187407711309166207762472342116399446868
213551942815030009929801561211838362075615023000455026592913628076075587116095
196383037918197221656165766224094129938048768709398075628665254491396484431187
214137334197603255171745680295317595997938916027327076221171547414831916737405
228288393773139010217150780625614030611194958310222533515187490766970045870978
179223455132034266385286506836485998893173113133628232402077851271565207200550
146862280923879937345876754738519328271847549318088694765593783257452563489237
223464039823969705364133863856334231316458462408355909053429258389454711020054
171767610589992502718588742046908875902125291554407140986328663633212067164517
216382938210583894631362178852225460782044361888473215520227628268142215573813
166489434429438441769095591467989316550910449814036747346509102620388826551239
221972706020230477372141671618147129389955787819875226352556852800432112658778
132489348921069029772559289438624580350213539403787248387448396051689508616991
222967104147722495310939705090978984307317097477566682473238645778136050719673
176612703752511735193895125172819470773527585410935679572147790405615555120749
150772901979462977128484231761242036874608479707657577071412068463419262413781
188882253761809390350242362530207007118451793457927166576363894405573202937260
116802110373104131003170768021765052499080117427168037162138605603142171838337
178750135193805504469189255455337094383496385723583119810138629903526449080788
213497442363479124476670380990422862683380733548932848939105995650988304094612
159495960645768763282034408846834133760250032332007616373340235758577273981729
182692234563986950007213286777744808233153756622553516929508200823477696600084
197553855621393363733031547839049582793376824942990517401523690282108580765070

20575712725619664529970875256622077867395792721783720249532977593374734124159314762992737804417968061412121386435343630419462481514685522390185002218828972617911814289387238449307954843173584340272020100913337421185321752929453664616117632296466539394451571643812659859887014096051758961848042671485343048824868620059101793136924743623980963283035116700081322960398150032759245779616389045713998075009277785490423069141639386075212593408560817965509071641073357860379122353596760059674919778433133870428362284816729160415317382455783494313073851617185047369992383871675080986239324657189891911810549272144055130079664798965117945067362505367290473321961448318527505598741341920597789925380081848961772611765995159934063067429753190021480523930016580032376897922136122656574624109715256103979213628929932733089947386269542551176056254221299246758383503262294117545474780680767906704809033125900707876459593109342885481401074540725309549716907920762787809607532666360912663787015494854856066781423284186153968770442414829455883838325646062838553199425512204323493769272252626502620028505717145812624448402943383750518818442376250556989730934424944611340860592584018698892914158673712160032601721749256022580803980697567494144215941975890846360178481621076576536987740607321965305893302399176790003835381525553527706738978600388822337869021285025143705788951842596923272564743108338794422321175765682371296016906925440044751884894227917814012405107379142377103106883432613037587779968020390007214722554037225323148378072392759504751718936069231316291379385859030613906554585833005638149042053184105172809459715887892622146977621965991562919208495847914660465308055175187317490186935720590308562292675657102286696881302120436542921434314400919994760113801610982024345788503862468620444951199352075137195204238978029466270147235702754184564252454214392334834988927851164347388167480675696102966904427912365800646389508693726661142479538546035094280851828169969299959649691972218418871422063895046632918206208929751523359249940262397216318829189808519117890744235639976908434691795292699777722615046288356129777176872758666636593849754775864919343116241660624362347174917138364507091384106170739667290212776113067236368855006195053147093560843944738704567214673520110157284626051452046751483838391378881697819936442284697902400281712917412682364141624005206649290771827000826762204814076320836415581797879623166745720691511165099388257556667798101805250940771439037406229753180874408119438742484428964

225338702714845382450312193487984625054907947380851715077884128902016199978129

128372903526896432521275901362586627776204989209030724736291903357145633447850

116272401740352772136096670684582873310868547008039722631856206833214429480814

172777919242964593286564032215264925372559206768249326574291348218405451218400

117442336522109002170603782033328295823001676930669318765378973636987041888084

143394553058623137319785654171152191939207616518732855117151415309511654247308

215917217403746805617136794485535668793085640014149787446427462299430454230741

173195864305038962404830666491441779206641278175748506699527782556226926461351

131096731018249908327603926008568412999917653956998195662993548510654241614629

147444560699896467931230507982401391685597406281385950108247571276879806488474

154110678675912693221011529544246669329726254674525919128861390678192207099593

201136966867573395370527330582197828435659182590271168532124175154419400315636

194595660088773591120361912107192157937073445810335364731317920785134790252778

127329712630568038063328038792696506248138685057473890300000989948757946460719

208256012574648288406458879110706486963645459739895771434495681314729787818416

122974772191935397936533547801306658252711485698066862963304052230808640898095

202260465757119775105341171615826403798132165300875588801826472251861270995498

217863000798662503745369820255171537832911759026786172459968675071843479354375

182972883657761228754143952955975518719765392845133365231649695590428517947662

181248417841930587737625214107283754053851914169001873731956579007659384282617

194362187892640279229060381152641563014268585011483131628969362599659661416872

149654162264660727501824772167778462796872022062965569780828451196555975682123

201090964835288755493902123663963990262186620922237781162636774938815878749928

218484736846017633865054352585484661402856355200215377088029471447803102498508

186639688362087869442803010346539853147205927386390606199607068913239840144131

117897505460973183604565333903632630412360221214387579169074517890492771774663

191112120082200443610038612020455559057773558324641409075813602814821849293623

121791013733967819264264703597369975040103430909493427588323558239882826699339

166586814191842718487405156747669358271955546788162187450999190066942820727028

204083974056810563219646591485455522787489878397667350030722450092613038471141

205429038195964118533614586411726149039157614922748132869961530121971931123704

139893210840077088446463550925671999702146850996931090954754563609518078188229

151785258195854911054417235872912505052028978441485559581762276150475654009368

162085290195561882115762971987227519327510782379928325021410890644454359925405

124018468335994046468274041521465914549334874910077665285416675427807347944483

171546220939298693103340985315088297931208317930969472928359386310633228033777

124928544533637504451091040066640659993653358863775799360476784989089335987043

134016425674851886336177212816738258697363797261728344775153563309570143454183

121240505527767733809500841909883491969774156230019044167465099035431106195508

170539291651175509851051815573503945156406986021251646542351789409398192271337

123349174187240218837356857345547643205020143272792679593459659494335548351678

128986567936876159752262264927188628126218257040566584315412635598009860694399

168823785290745909547692873195546842780165036163967887187568360263340120601623

200987997706941668623915429518404401445006905076393373511237232021542521766727

178946125611556716993064726277347143866450667889686485978264827846470322592766

212906920357974683656089146753630264862004902566664323473287475790385375261213

145373504687082051036238032120972110038204685779849740723820197611019502376245

126786287383458933429788879278090265919622209356736565653623105342952178593153

192878676700436537325318113966886093319995426360340310533030055660143475715387

208378961933666599788952298228319251401358214729064090359577982220484091394695

224544773717885586201548274898311486414822392185201968836042601904838826000238

168434872970893134563777993381604856716916757171398710455753728513162435651718

208342366368983589521885589204719052894686158419506331881349642316392190903042

149512822240557551673801005486009350811850958006139507209039775328771978628309

211958829089423363040597753239653660584670723585719921362498187955442047093109

162798384833813717984647579104433695542061838190778685311545063995248374969053

209442286583890198711286649604481269623590291547800885681659006608578481485279

188727571254520926840465351572498473102459713090629320199447882606654891730215

213714067206043899867169312376448014597439022995917580495292526129818219902337

169086298790546669319292619858505226551985790678343912220961318290183576731144

138130741861920969791725918411634367103918512289930211659062608304770982607172

156688431592797178280617279878345858088166584816072782682997939056896006328746

151542390143141630570752130372827427468502222556841849553147949464767026264362

163932517088768871528236121799188581390397849722235144983464737412668282922231

189015101457397020388568410182138851992138345958608619977246723098409129258986

180176199103323079784802854647111091601413402207724657453797934433934168423422

195617407934937465867787864856822497391590304387161541866177365535125861691816

231105710468323174453125821031839663641822838086514795355197367270358741761969

220931544130735475758160431339325606880547459453838873134458336899290143380353

224190065049100456512218571246941334480067077390429447256517397838819978585457

174789800929198393208050278338037102174346913050337733263338704813148295224657

131478913654589626420384127015657872893185566460925639970571529139477333446458

216224633239108034603991628202620732286057069299644422187535589868484856670541

199289526405512266746940264567172098832386518993822081367769453817729268667032

189019195286976135392319630180728624628934059630969847601124967060944719504182

176593211345484878439863293503149631901417174971270991672621352557003193766549

168877793564141693256457747980691137404130510047265745961700588481354806803370

165670940107856017523371109781564077359694110463312159827874600625588720784619

118762496932867471306019076279363196637803142812688855993279255815532853180947

187691034114570480078335929155860452236270999164038485270710045175203880656583

225098789595289090802133132927402728244630188780714311053435008494042108586596

171441578493557795238766069062341420452056119134520511889944346892158883195673

196222118825943872895239755700142497529859012283335599323271276428662340672014

145240624440150298873146714680831330664651123508111195156060115603685307691503

183902398049926121648684613750873540354064265203908137309965843256449446902150

116779162008557409272703290393657769029532522191570959943734663649203929062452

118331416090736925179899918989754788015604812501193103824749522817730960164004

167933343715608582300656252199796331735511343297392489186599884254708340576499

184392724268638503593812958802285461653755525672266822111792991175545670201161

225329264645957910104506080628908877092428136279948125255594789592516348201970

125481748921180987590369466468696244925551788677719024752477878378345990849158

134077155788891133971982505552186501741774934558127893202730681273288034353588

208094424322817106058634754030207101842180426971487080082396901121854517327838

185866045200175429758488217218929750614908762146078306485954854935494493964897

174505235483234527334908204271938150084317587793133282574175890206899243343069

150127002269450261187285716595881107945308818090657815844980149332155459084100

230553394194944974414939410089302041986547016924383665477256194290406290208142

180370110712476697050008720387994745655882530460743965610066718208733534694125

196626891373733714502530117339089676592749061082943246688420829040962547533390

190683800365948360514147123326663701608609278163652447902596748536656587053122

129527170897503028264985203635596960072468022623381613382502390001014049497780

158997055191837858409921607187961944966761018408974045789669958186605284851604

189085310974427667805851650456563090638558816648598310513876660971322587542192

141634145420820814149078597226456515973548439524827268053734830914869965185477

227054016646574972813362919781512094673252808809434770828557727579504487486156

191041979119016425459953679019648873687389268583476965386854670324137331309596

179051885566748663144069391209575320811148046215167516299719194705489004009740

142872724181997061209527395949873154385578044491246815889838671966899983720896

118005481093326465988880447289976966731704999683727156555479739327659078631686

137421123443744271664357296794704412529152669578519036405318922991341185921174

134157566915556734308744741657259286855271298769876994550813251468871645309639

140718883152979379657068055426225915990486707449276892555038478973357606292607

186720458028559748203892231082890818077636796930711681453570661352330869220594

141413195528139745674093826927354519404291771881680650198374550720538296965165

129373118511403510179443303210584346910443751027363572948822665777493460800209

151418543281583261447389185202817593433836866146030727757221074886505092549124

136618774813055905815162374583870302548817492303275700876842044447128905048081

179196370380596130657064938734858119916503740791917717507935335928570028272679

199928666560168715522128502778460813646546117412169618922746757336479458517144

148187374698826359006741911227304337258808229524571522996632620896400850247067

197125160258507694573119914210331327892144638945642513074697796424405028837725

174260411445176246115274641156757437953960676766782213898356421613846320012538

129422330780097562950335039425342557230881327405261574797765823181960060881720

166909917637127641134518985389754359294807263361140642960297902395411994603366

193805250966420712813299053991709099362325940818479151040422785418669481919169

181115398436741364957705283803935671873097346675082080081196107842430120883430

124168341539873519798461540947909192832805062811085962627408049940534563197786

230868716477785608917091026852818706804598970699799818620965596607639556117161

193413583148079474667333165351001883319532326108559920982652089252515387173297

160323770916666892066246270911314333238707948925148891919904411781360576160827

187334721529294808729285333633385533858048554683677546091983841046515323521519

220109399076946801556694244501822072364067298624675180886819659869777220791027

122873347293942633628180106600958499238226030747010051154896415635985132614773

195395501512655744419114012940687594337025980813988120450454996586022669339235

161884767436230414475310123463682183944298387605346927184359727980019636639610

148304553288280792249791405823332722828740656686284335750949343638331211792829

141707096887913582638546829312867937846307119765135587910191386432538470890100

180178111510100260840536632920820844584485983551840395997270892602645600286361

203174595591222281741837241014111693331611697053469289950584625968247463871019

158758413341927033217173037276728161027513224333998913959616490717188599223309

126788323135561116682301329229796817706024576304262428171634834739937369780710

206001497078101625182672198969925284931872061710851521999487199100396998060195

225089501983897116339404497872548491041410207409487977402596886829954863136058

157990951099626984806231503233975829648083316768058454029989637870102547276107

186293626657316582089590052602023290771851641909652139757282005069224947531636

173240310528124091423719903997470814177885713959810845698914332395801224413773

133955535724256828262029834567012550503134730420653932931089749360164768695303

187905852403597163046350821499981512459409907464373603964842887262254221273568

131901326164028795812575095306807808721025873384255764156354880642297352048093

119725418652329686249759240851016594540302509848751518658606803392103220755091

199468713469539764914936838751168036751883919479828975864218153262285623764328

208527596389801059548536870171919749900889397351287506606635407767073716486704

134565376574494519965311748055832217706854938258274968946437618834760533552028

154591538016003331611039411270971729597344446027988569396158964930766427681284

150924442508880815545170768529481231381383405714721922688297945379841875356705

117862673974242905610307484731367303321359962260244168534058540040957743746604

135948879272555174814919174283156388433113813758538874726197049088064560873884

185223687308662166592704420187861825243745212593836321788337113951316461297071

185993123319679257218711950285715058432805072671291113964496425417546875266823

126848984513833461496467564418732429831264496512793436239236441251211168198896

155598569304321623382093873880051972726611108428151403472540383172552456444020

180863270488805589098344428973771465981209641556573635117365449526599133259927

163926395582046764141915298109767166085706793368968668829207775012576519059333

116337570041899004273189029952836654165802298787449065996195386382592660845692

155942773608723019937963548217408907247090496950391724676050514285261127255708

125323197757866063005073168343002473239915390064760101778461944262223066098464

146243280768074182741121696791453604751093507796797611349007756269366138637229

186554337059474532653894076396164232030626061004200145215910934962681711821347

# q1

227129688545112223179889299300088424951874609985068737940364383646617639134912

163511003156556485718315828413926702974668465556725402193625796800352563811503

171994581207000001283215744968402252606726594557176439226607773528369340125639

183228086846279037090377704412027248222861716903245424086571412089108509926088

158205509349983680470469188393255450410179724993693968325806833478723806314443

207366406192362137021044440575672742888781552218081927945801193562511741422815

178974866811716909269481765888876524470116854334583139483868710333101247390169

167614240393108942025841919891558409521982768627584318281244374471261956884371

153509917174344174166491411356476264468136714547469979036827407167226887971311

174090502066030032781126476421727185122335670437789192292520181605841806062638

144204805583445508679483010957520965018286138311151499608459269406218022281803

162906872822296328499522856720978721567454180562232467543340337277283246405992

164173369494744495092702560170332241429862740885300000692560453958576912873797

202884816721409228480718282818247807316613126331124537854534705731381093432439

125907584485962286099839214064990287779799410019797574099694301923097046973702

212217479437666734407007869543443162967529720817093700976511487662086380248783

134369368181420157097524860719016662078320104371429237470026062516464075142840

150763012835200558962887526165261978637889124890292636161955146977185828740730

119791901772690515417332120215138467637487570705527504785480777275508520822728

172545410554201784792656017682084595342818450345015999597767299061982421403929

198102883694764450720393876907788000133962850059012756928853420449971105847593

161036877882529840958129370965707089420975097776731753442263806620973656955687

213939042401442896846886353423824900279655107071651778226814282639853655982319
214479193957456943924601618179463766704494447844448894955698052270422828832825
179668475364926055634868514946475753845403999058357114889463639144252845536988
209370744833852238027602211814075980070430465965533041262138702209569854678110
140112896600694232534230877724173700453141087142063297969142554583715968211907
204894154082756743777340751642054903472846919004641158793996422267973670045737
146284449690724696325381753665435387112317792560468844475439328014796336563816
176484293756396593205260281903066269642077636459444988787908139723419011968074
150897802647558198327648138888770383067672757318850783482892025907262160590098
153380167565925521806910121055819346811209029598460035504379795709129819246544
120496514230742992969068989600349695741297692775749845383121365546846301074001
216505384859701967660478368580019394836708221777238659803830817750477442209142
121587103561709061302418678582089118868290739682780403551496866511591279765504
133295480633222950034648171049573837615426215575815515700372313841002296963399
206445640582748691889923570964962883692207231615423280138153728701223330476002
139475382292981610713119537004709620499084184076327357891034906756736147292013
159871596373427691949493992567651891119770508304646457608800099885669630608801
184018815784378219505726102137584413202251301726154887471739819910959117640427
229769480776940627862147890610908524319237988288388695017701956658816509307196
139898712303924223140277896105088596922953485302379797950979219164515179096545
126877486886180203444227219013208055762341182827858203067829365023232245756152
161311937442910690234242885799182785008158342464165070848379089544125168173831
202201688393554505972712511966122443016754848341708270290318559643770735549388
204951291204395715078306792106035999825424806662202214117204973793060824793653
218147399994032239951179658195605485723821950817048278333773210202059006970426
142521645448745337176702569634564020653937444691072970341956504984981215403278
214676325552244401331083126910261365385244264848344278700039734564532858606941
199079804213467365015172998648899170401247094203025490116148959879614373623651
152438531562065399329471469277068930779498084056766230166870009816912421489328
158756132620133251309620475587230213131947015809787673012011676487331395521187
183968688731401520655790238410375059864325023654720708279283527424690157977490
210146272206539696192593105104520343154240123461941566738397592379606405397060

134734477727579699288958714749070548068882414359468298521935989165019659776787

191368631858893395738259500816079433536075809407096514235750135987393201788357

197170415449636009872183964276468983501607380146382743051646442330792583161648

189110975940812344620539721187512815491757115186597052748342028209109573282175

189604442630058762810196612072051723243310828817215695820726308500600885039860

148548946547541727708880722864085561102010619154744904245893710327288346118486

150792088806604568730813022562444923273723586669058346521255535802730974244005

130082719365967905968472039248126738385188872174227329485912942728497311976437

161651288071526511179736861680589992745057124551624294190126214519696692331203

144720963746914103013446951580832826886986484367825961206523857138405187927272

149384899132906329433341336893835156143731203008463499766435030445930640565492

200375201532417448325352276377589007919679654967193370350375004097683078539846

158172416693006473238936861032009070929427854934877797821175030023125395697037

213439453977408799141527941600558235910731988446837904551925371470323223073280

187890744049358772659479653338968023979086097898068658921494119320407944133891

211628732689175549225319849265538278652029241432025569459148349437314199597978

144845380627640684710845176894109314289969425411817041283196332405046145651429

195156509782345293788803681406645350764059370284499505551635290039443820165822

223294613985917724903768385315046232813032413040222138863600655643958732568324

133890054672554704134047160010211131862657534083024426279013978534031079414543

181039608072319194218601515966793648686871226650122294169683707001735336958392

209669584825489694766479950392948885957152608385057647183509360345739273773622

162298285976069036616047626987007055246020285704596081698950187852199723250011

185990242210690001294188875339505950817837236829106250799893922195470477348224

142649930947122481481974499155381435000925876888654861073824769435955544761537

209721269666080293104008674732475676437917780200930668581461010942624169451428

132358664896942365855086295721839054473982080103557224396175064009184764274660

202388132609463064289563329684360938198113773373709004326656677509561206839917

121240014301891651770456974486923987743257097866531027251522597564451897839976

202828188637110092550105113930967055971551916406627711470539982935420327604519

227606932184317352767091548383099254029904866931599888191749132091789663143570

137816717505581991425270202608197535801667383246182883654423886324877146517860

164667775138523793659255423602766750042353516732391859301991132322207604398318

152654179683407871825877634734236675063233932251627574213309956619990031790450

155552569743748125475792887942158205022547115263525071447326904209002365148476

218630938780555694969064906765619626783643809090614565898722310601579432605631

139598473593521304127823030977880931280795074106481362705124495004632343656406

149627033777009762775315937386542544944710183069466659484557516222578939701586

182077113045277203260858131869820667409709541064240664625267370118799660670859

206576462963546283939251317676238750538095057131181520059651118615690528245709

180093603885535763734992887104648935476258014986753670846511400132863118555736

132017341800870999481017623165122720272674944515634574483830876868414916957087

193888279062374653557568819281807036718770005260617024032938065041994457276428

199485432745930485987120027913956808038034682628030688826929298705742820412251

168965518013666933257866539115249193248332580329358706372727153348967465824833

172182919635184071877625897243782668206533909797557276048647675155115645123513

166793315382747353910250294830665715486710089485206703145631358049021833791327

143876015231509702299494659231705721612696474718293756950789447658943665448136

117751036756797623251975043373920089845435591773600376129657675313881661676670

162751620946049286528099877237752223718307082983902271118447145818130691820775

165840442394769375302381824606587379888497254793351638556407614884333512859656

173619556364961687505687239242182922144722873743158439878425537378929030420804

206970959176519315733214296923119263483204072687527131310209237483627083704520

192114773047152343726140739425794123284969423261054873911783673680412067182992

222846462503340826585868300543569171998018849971335275467144835725660114834716

142163070309530830749947122505949057480704186526986274052118902597279227237623

214081331994384774500509194995945890911203433374763042475030455116517623653480

204048658562676380305105721689987257071754206895707369611703079202823493333418

206605664118543994093814043798494048532046415842638508142268214478129422737203

202518003794434620253502984886505810424776572050486934860091493996952823820789

193788484018882029380593192426496712447653376461787045343287436187093752443878

125334818376946053462376958534305345666936374914792369073942926403394942729929

229589501237176950269553321620935001653352288193494680879824111598003961735873

147485384217722715143850835211790074152779227292205596023145302795739548528000

157995961097042446584219905758248680610522180869812531926864637184608604852377

123561817507973043246222113885519229302246979236209975263657848699568808292496

225174152682073867544398362303682054637985709342864929790489093067230249330263

168322673115164391452052752717344478322286881335846650096673760889609265987772

203192326002297200799968944531567680411283172307759754983237356167432088862750

179293249942864916059812001668895478207687337526994728347320792212030211093989

143025062668173545858191034430293975874029254904237447552396407492006289210186

215805429671675287798386786676843576596729170092739643101204779076949593756522

147558039604982256492160869615730990740071609251484924226523361529257305800634

183530646127912506207514324004415313723856617191296251816234875926750066337962

189529477520741582292989749574757140467186331616492674183494287830823560883293

222558699524523482929237054011819299511334958998617490670474981463175787137628

165041397509767472847851851090363175116461532601907273101912206938259773417133

127898035850903161893340821067751760169055784550344974732366200333577021547854

128365905512079852955450759073292230372130474647904990426398405914479381480888

187584224382768489141102422662679173015242238754533242317993281092119691936043

192791825802783480631824760821432905367281806491846768480812613555433175615211

219611055759123900143864367377914214082163594458000920500560365078772957853919

174771722624186032740507129462126499435510825634015993603244200572407910592631

174825577369272272586361372864442496336091494414416230033381267410256363358758

203347300567230988730421213753585318616103327576789689803704950898925383706520

167286521597688458005369081992712483244725848098063795349513376981580792779696

131296872241649209455031380990803554320173442994637245754359278934722674695647

169543636725342621086571962371779125925072903449422577895627845245307222528769

169358848382068842079290737524612340137098255098977194097467978174650262652790

222211938808475860053054617212677274624816833686464104029383021475865562085329

201406465337461586174845873840360065993670583302152372458760886262592071418523

157787376190556564203702614185848996929759275464412418776991616444455655404481

208304442583720281843942287170580504816704360670442609893584977751879218352450

142942119817123875895255337302174777350406712424021055900316892017663920686560

200274073157056114074521741977231282929588085891487986077839429163342260781680

127277720527641857633246566191019487459675464707740265706125498042723535403424

194392304223338543284218866818566745471412575440228285280326767849117242117494

202370604249687147294436125876261437898698842585400607615041105005695709954110

166287154818398500153416248883411668775019275526208448391852364133983124620551

158149821541354391943708805760674724122125003359905217822391678168762887813720

223187699268331806329696812112371456180513529361481325252187885679785061739045

222501477614154006298507587161332363810729155461435982870547675250527529500810

227381312847223892572748630065149741520386200026799084285125966014893388006335

164059455426669979093542951658918516437839925678037992196583130467387761469031

168195106542863365086987226796545107997105575991877516315378190588287347138192

211255331564290416219236138003076356423029011401731392296644246772245892519464

190589078129436474893842571954840784906213774317699226911683591716697058450875

192912396698041614639000144512228629458560262114128553677789115535206325432657

170924337922808036291999044432489137418664993386001928216964509239795790032536

139148997311614981792743623067701403882150308613050520528973662959766145149872

209446120156406563818684940442123190043170141329867622388829437907604198932566

158694388563013192441006049299233763830410047778669637699444732615155886829113

229342269360901601649936104389122424845490888516335765154445429488789372863371

160104822865969048892952273113488237415511505135983965518279876727142331637370

157741597707223775977031492943526072575288837971012291906292411394780865988937

123180808064363535056907652703115095798328144689655802071452198409107954228539

217006987423853826667614373495398862434980854360226428874444973833612935063201

126522673748908667553014100299102358091535431112101069712577639273921234394159

227398400193421752389920691916721559638678670739419562861067566838277662904789

169818031685741777581645786415196686114721423780575096616945826959976084254195

230188261714018512358739040586740621634578651593157430406941899148693118597236

210247970739812907804429751358477610125531838546903604404929892639437164252230

206065990337610436215631552709310501111051010266616307943483105305798584772920

176130929241355660013786876733103633933320435014906105801257561669369543332620

231046442935655201269546564780039176618746219660325637222050917739706543699766

163682050724330403122966862968163640585499822680283380924862610899774126432077

170993462996452695037807988903568785522877423968908642462085078836596515788859

210701032993987925914798112500425244873465791123007517042934466063885300052660

226447250275806181323144878462629482590915788142682944339525291761478376634839

186814212406146501390123855133015052996627542156159433470264082109507391724026

164867697252950382469852365771567338304131464927338571410981276986773133415765

139148789600070539199047743161144445842808921617035636622527835674177714866098

214399486894496339745040315227036419249149744191307269861141991403588065477334

message : 1840127005

B send a message:
823836009309903234072533497684982534783752445597933430992656676937298284948486646482303966545347445882452615794075038523675849577591411011731847434888850 8

A got a message: 1840127005

B got a signed message: [1840127005,
130912666410286439554864813752421844360419807117034686424953707661623255591595563104448815859937433006795742489563791286285752510841509055529545847685624 89]

Is this message from A?: True

p = 220236145001606712001530891752706508868268106446852592422453158438791598756101

q = 205422310428853138919085981180711688648996817433770880858071022900825223688417

p1 = 195969259958347614066678599969994825753599658098626169711014740249576521833597

q1 = 127335767077891540333766527737842836118528025220172156009524413207926516130373

Sender

aim public key =
[249538960404829290060245196242970893255607738056264708167252966710255520264623858325047007602431507585537522470752390699620259826522364943767958390635416 81, 65537]

m = 1173924430

m1 =
623423995166335902220611379483835102361859166177322037803325838720950831905754412965967732487936062765634708448398147078774385891521951830202485191868 2809

s =
112212702818570487296667630113037788791574670026909945675498256880464764085131613688553883713235246958809195834647049286199142072504513167592780769170557587

s1 =
189934961752521824321274744673294514283404150192071171647455327597388923978501210618893657266621400936351380835161021349038680742322544137486594914444729 40

message =
[623423995166335902220611379483835102361859166177322037803325838720950831905754412965967732487936062765634708448398147078774385891521951830202485191868 2809,
189934961752521824321274744673294514283404150192071171647455327597388923978501210618893657266621400936351380835161021349038680742322544137486594914444729 40]

Reciever

m = 1173924430

s =
112212702818570487296667630113037788791574670026909945675498256880464760851316136885538837132352469588091958346470492861991420725045131675927807691705575 87

Verified?: True

**Висновки:** Отже в ході виконання лабораторної роботи ми ознайомились з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA та практично ознайомились з системою захисту інформації на основі криптосхеми RSA, організацією з використанням цієї системи засекреченого зв'язку й електронного підпису, вивченням протоколу розсилання ключів.