



МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра інформаційної безпеки

Лабораторна робота №4

Перевірів:

Виконали:

Студентки групи ФБ-91

Легенчук М.

Осьмак А.

Київ – 2021

Хід роботи

Кандидати, що не пройшли перевірку в тесті Міллера-Рабіна (128 ітерацій): із попереднім пробним діленням:

Candidate 110892330872443418338008663682228690119523171196867636198254296142676199710433
Candidate 100480603314620212942236904794335388708511976367277831988455554747636021603621
Candidate 104851409622522861436416129690613956266587674667625106274180581253249457436157
Candidate 71073485533492780909482323669079876900872465902315324142598419802962935362733
Candidate 102452450263567805365519035934434122444195506965952961803272816947044005759903
Candidate 87424348917915967061204230923806552812698828635110774548243409819544037053741
Candidate 99678014323358542469562913204613211726248254899591914719939948745142880495215
Candidate 112010423532344756231589617782307831866476987324680218998418343635392088008643
Candidate 93750991091025732625326044213409644181436964439813469659019123282861198691003
Candidate 90916798628389124563142846295341966566276448800830914669726870118765762611677
Candidate 73499194519982323986902547562313874792240876468710384828103401413000478690501
Candidate 60761241641945805676273452623816180020361851759243969033768756115146362703409
Candidate 95655813916532547120438820500417703393059454735708737302581810261892438830271
Candidate 87603736689187432455023232047437177506413778937438565612305734958563635659451
Candidate 64777061603883797583973675621273229407747478404963504221137442156476519407115
Candidate 63610873404717576895604673533578954192296659006532669209164430383655859121037
Candidate 84887462187985080817472772431226222653174406558673450921243712534168369635593
Candidate 79499504567700967431202164487900509194153399882930071879650875690141681646319
Candidate 89774814667409870227387831737404681618746025380782916569253954574068191863627
Candidate 70051986201692388429699048860552232006082187252107672184772337537519085157063
Candidate 105830488325093234131537895455719666514266901438414903584095602898831042014567
Candidate 102945882246417765153327648642602269261701924161933207549516806990518476514339
Candidate 105552888808682394780270840697987132424222687982406617969720190998582511655299
Candidate 105375960410051109023936094249320124685653366878207168771752267520461928047851
Candidate 84352746492850714279305304096820577436416111516735742164673666454095206647605
Candidate 92592802420762377743729657551494357844181575018894509177567110991103702548017
Candidate 937558587025899215499707173827722122846728584020050061270105946492145610635451
Candidate 101773755311816954447172028605013418436620797832690569478434535422021061524687
Candidate 65264779051391425197108301578505171246204146674598085071455712858933593960563
Candidate 95443972109590587062740949481655952083070645017878881188802751909287252285655
Candidate 67335242405514477186373100817216300118999902377532336135026845115741215972889
Candidate 76596470412600335274943493560523393319414634357617308337803597006271002582093
Candidate 86852606542791934663841430939247383446530548678752955213227714914661974849439
Candidate 92418923816591151861004702434178501647628647581431792440315151829992337499901
Candidate 665505853222138380118138747183407183457599593665583966844827446189813816810226705
Candidate 103993122911476887065324321050514837700115035253504431820915242674428923360985
Candidate 62981514044501328480179930795012121015476601018935153069750990823088339272023
Candidate 98282224161309851933260612295603274705912583011054422281447416271836819637553
Candidate 78077951108283643772294583872300061214779667281993506781631948437848359137745
Candidate 85438404697555978569928585561316605276048635973900847091354780769556447885481
Candidate 75002499414415975743278535862205215730026529186679426683259904207664465528147
Candidate 76360817479991642319074702699636027660959899649494602516277096016445357881167
Candidate 64181375938484975182273635312417581413047817758892920647170220226887234744843
Candidate 87887560298912675099022581780191617024009221647937715348814035319289699528641
Candidate 85636914151749831595120147384418011635302471322445570758350426126205848630341
Candidate 613724471833308489208170844791205485283597209277521403077563773080983748911
Candidate 1049533271338451579804076395641786122315458732620393828557828912594013276661707
Candidate 87055410650767316952883543098942826298571215653100934573571570997708911240547
Candidate 109297687349125704305100438406119362870420696495160122794593856365181293035519
Candidate 70934536652123246420950498108439385112993432483200481980079322562355270197931
Candidate 97490778083703157811073354569141133120417970797414410671381775109045917178269
Candidate 61846430610408384616808180362423145268165458514788929602601370036866285719151
Candidate 101769668522158108186164499673168375954678225997860718030829253081534477579015
Candidate 108439535207374953281842196675981786456693363504126734650410344498293049148779
Candidate 65152085519388564976807599550439599908982553490273048816385986876252107155525
Candidate 76287234150046873105737005878407194363146453997500921138398055803300622686827
Candidate 95677187071889309415491066264343424394926943217234615737489254289600853481105
Candidate 82960967676144769811156449161050365101882441892777199689840915125196145786675
Candidate 80975699018482078177857492254430202948228048390810461765902420256284560435111
Candidate 67057440686040758654826014956941023320562200439385657459480395519180925784547
Candidate 78805256151392677744570072836059652578859293346081156784062958922042783553057
Candidate 110365903133314381667370185183132785693092784250793526365210770248226380498247
Candidate 68679640357112496576735526441388118996136246777742935656786637819681687150899
Candidate 101845368915657867365069355075051368970519448854567519463252022329559341415129
Candidate 67156436810695318188852988766786266363659565428868376254129545511219439209123
Candidate 66870596259484208531790174757446909913242072464335400418781907919175209591639

Candidate 110260394920628589957101146245529100030969386519661205864153486045813292828455
Candidate 111658986763852310036491991534173824014373358788744236940180218025165523822331
Prime 65620629053331790136688908026169806950420785748631833292836535063668149515787
Candidate 4
Candidate 111902591519313331922229928829913678397353786601616755252221651259618847759613
Candidate 71570593216303865113480850856924030672803874442751123500255755137680854768419
Candidate 107657637291459327343968227170384597270387734935174056088110817192099587707557
Candidate 107191525372158919740945997910597295609637026603504734718022700897520129652309
Candidate 89042326454462368496483515098170965710882921060002230514842054012588664866137
Candidate 62501165542155917691510807327191261305758654185583428357699713987380301683891
Candidate 93876773878315199593373293206056265568048377059278315925663214977360710576769
Candidate 95857766071193303486423478783165072965942676610568925869439862092365722696603
Candidate 105853205910703908410805721161281889460353337015086018458245574611537509345705
Candidate 60547271820652949364984606751764550894558569271202979956835691055130617826349
Candidate 73651431336180396621814913473650443735985290950430477187065085771891376431091
Candidate 74679288047179407284083865095474310940906314739169088744852673358393229537823
Candidate 96064208771193981411973098317952633429190465818299712840995314855231188415497
Candidate 70691752750561531434759412075735621763921118559617614434587750436429924782497
Candidate 68013533446553581615105216833763752516486537649898257668034671906964858952803
Candidate 58200109818973459212907502863562619242489181590782904263357543582778794357627
Candidate 71809964680946695185754995880438209312705905892184790246192964721105626348597
Candidate 61830489737213556606086371671651945207825297075717129696019624790173759755449
Candidate 11096276118632223055227082531521275747968388243385224617982547729780909031939
Candidate 64386377031299974346671571794847953831148330983800000005511131806132562185693
Candidate 115393084660509237790635298026171515106783654463729161246545678375681842831311
Candidate 66964877406402401099628571232362000827619840761153015999503529483997426992751
Candidate 96946224015349995631291597973838497155213311859908257556977791265613643461231
Candidate 10406241322588959576807376193043886416300261124810000989632000270910860108615
Candidate 92120119374415719418238224429062490215516704104358230686576529286377418883619
Candidate 98028059829654830370022578296354951565761973398062667327784175647147139454903
Candidate 109251982759027460243161850363344502903663947005997840425412392726108692436687
Candidate 10249547436618835387377398543350761013410144248531818633100754226748780463195
Candidate 95849439128398000327336198922911952122185266768188940265388875670976323910589
Candidate 68873529392007280046093337901521204307144844975265078050104212408253070596485
Candidate 67963385735574310850017619805600495830138807248329484578488395031823496311513
Candidate 65715661032954245888394365086091911579940309362077787135838251253687345060103
Candidate 110348031308652191520786863070271914774368302238792600234338826503468204258815
Candidate 82298166921077699872016864251576284615705251351535196400880871281269641802585
Candidate 61842807128626449572778071526960023634572487928363547750946544719354774293881
Candidate 71706314732775135839165843338008090475148538960305185302345084835268156474889
Candidate 101833419773875580128359034650704658369075501217547041693797815748985919983445
Candidate 74432446588206574463368337345584320238613228700358990050530846575454933567479
Candidate 99762326752345005736548237759219254358819945461662003750220911173901257542317
Candidate 97471793160907358835254406026282986637478078364976638385313889480906490355263
Candidate 104304056310454125773270040213038528430443044167955969258433523075431259728555
Candidate 70805272474435118433705927819932810533201077128257273350564106190872400147139
Candidate 65913336255752819135720509272335844781316531262919525160566855408772941211123
Candidate 102806321554718222781380801137807634193945217665497277091542179024144388721879
Candidate 10943606700284240678321647037462240691278183273188943022438027238497021353925
Candidate 66576459990508037949868165769196674090490763493512100700326835304045073826035
Candidate 104965800420871896912868630820967328338135948150283081877309020204883043340909
Candidate 59983567968087243426799279073939044651001380596026137189740031569763618984033
Candidate 90366289161142600241274655601814379550390106638273719447052592494012978308807
Candidate 8389677200715848350722258574560748558291592161816898594638866941118437234669
Candidate 85850743738548612111447677195079412429479107228191109429693214954173538865619
Candidate 60319157628247833852101873843783071566845404981917249755575298962289545167957
Candidate 65249649554525014450306066554929185880146522018897047450739505616581925204525
Candidate 101254568670025891041373711437296694147789325191948690959758038305061286468523
Candidate 77988479727723894333296049943677722967302543908371231896130892159904604561253
Candidate 88796811384088864101687752103981116359865807546604575388171177548226601521685
Candidate 109957972412892613695383174152971443608978486594176984488751747708942579841
Candidate 88637559369708615282320976056981031098125794246656845901843742547336589259017
Candidate 91914491239573384443709222220196610900419705141736734637566676390338868648965
Candidate 110826807835116465733307119169624424877920577581027000181809208780211280802035
Candidate 87386102320949608908520723273451616260804452662308730043555239696361943693845
Candidate 90066110880473141192985827878040550347861266256670124838648901567116321616893
Candidate 90334882050535652211123326417385807933847718289606881285143475787806892902101
Candidate 67453206375156585840067110832241557629287587576829794892116894369903410382921
Candidate 68359598214226460545669616770884491095431531371185785512837010913233426564061
Candidate 65270670334703937921838501079965987000904761015466693919024280121704990954457
Candidate 83359501474448563417946086802663896842761228687785877430829976334623617633685
Candidate 58523001306642618408880695930864684230366890621569662935950851337590353089725
Candidate 6337996747757170546464603562579605729972875793910643160550014641836094074045
Candidate 105334368318462925826710055623438931608081285272606378837312547697088645445181
Candidate 83320701233801794555003823996538232563839795601685747604872827626178864892203
Candidate 77425962928072069493347000530282173862565413423527540432138638447926335917451

Candidate 108679841992610978498449361149720625342999862957059561878908436020407007831827
Candidate 9815278752917403701614457519711683029525715477174873559590264375618772480589
Candidate 75690314616851730327856275385545243129430367747951634854303516004656708929107
Candidate 105320903175488286164887839898325973632205234807515015559931933635771929223337
Candidate 9591552606035263954619756845484919427004190183956478597520928769441608397951
Candidate 92742265824609981850121326786190748233017890219340146459711696823049198719649
Candidate 113483344081939221263240869700613990025123961991658160331739866474827587852977
Candidate 80729433909491815506374288203047733195368494075274825918723461689892145599173
Candidate 111921119642206614264741477996600390842922467500968484390077164622245026071229
Candidate 102786194406189755960875072254173462635602946071819149781418461705247515500227
Candidate 80518617496327570571464870334625171299282101583660411877046679942927212272395
Candidate 58473381547997224685204581051225855068897488843944472869803628708678533285561
Candidate 112124815808055364251720573337454092295175923747824158790741496661098748620363
Candidate 70366506214234528993715651966024705119685919031145510067831697220096491607793
Candidate 112253048671395155137434116418738311066345838772484415434505458640416312014531
Candidate 1086027740833899346681865827722932904662168774238672151684176862578779681589
Candidate 92148230302527987799419414091292373793103975835667788321101886919810493045705
Candidate 87585516863211988882631682923310926431649365793869500368138987802456790539497
Candidate 71874966503339558394071471449058841262284193449292629586446142504376476918059
Candidate 96843075056105713462107239606021713092222902899544917104446887565262727750661
Candidate 85719800609471507369029198465988988044597500762285993263204486744855974476827
Candidate 99610072568626092851711959141867390784201362979491925049945222056825998922469
Candidate 7014106454462110596245327266579544693700654812865987123742358506589060264351
Candidate 65412951657488165785923686242761861699851321304949533001016282403001741217087
Candidate 111006186602551906984001121218330601497230041689960558869678543173588225064723
Candidate 83240794092274773782048157504021939951505919653566288586344551511662803356223
Candidate 84822533305071433171853012736734282619531158821284076120441205803758550622291
Candidate 76553189740122330863769117575122883039976847506135389664116033449481590652705
Candidate 109531003752959141339882163007468867129919646170808237892114080741664533587675
Candidate 6115979809670250550944570586821260339831308795613964635358038935876273995263
Candidate 74458666285432397674269111589695184766318318460176970220195969278844284329515
Candidate 58069503491298152656244635481542654125477467335377115976000143280019086487627
Candidate 66239003386214935743505976331443807627935077097631128253451520526433006534509
Candidate 73473757760862236968190169677073933910145288474169466806625660945333400702989
Candidate 63962637963378083743683548135663376625557488489293819055790861847652394849589
Candidate 6411931700291540749959664151059775745867422858240344579783276137254599781375
Candidate 71146822243804213432852178442639295432100104145970164347011597788317712416935
Candidate 84287835097621940908803137462460501295964833304542059584932868762900330390999
Candidate 93792782807659629643230806562073545789719967974642115588748324629231884523101
Candidate 85195241958199411081848896442921503863098134978204149511138481471254697324341
Candidate 108697204290293636204415901295942701380208890995476727637386817740391849609917
Candidate 10802504896534616821998396275817172989678295331096620485756489054624232184027
Candidate 89825449933219519979217174492237859867126514154114683990904770564879613842249
Candidate 74915125261706341169106232838628110163853503712714903512019781550350321946033
Candidate 68597321382391413054315970201951897637234440047142093854764403934761640218353
Candidate 93511123131813646232591218653291424738370580252136173999062269360072944542527
Candidate 66212487805303706027112945197166650034293567362668515231021269566469299607871
Candidate 75115122881305632051715932664454384939904285408921243970174880688649818991967
Candidate 97690251890931422057059128830931040981541110921486807351015437285501713972233
Candidate 79480497287697681635676822312066912151768333116404539516254627944910247864947
Candidate 107442113232881225035006573282870310009871547044759973885450581896089908912421
Candidate 93210217975676512512184003316932602460945150605699692666374513710926547131557
Candidate 83184768609255234310879094942060891215618793213450123688259421163267843157931
Candidate 108414169955426960918537232431752815051699088700388460630272803151824300279903
Candidate 9410440922570109140498483696371719525705662710827809603057886650299457472371
Candidate 62695357247318864618212180731806501168918081098341256573593904286606328863367
Candidate 102179241980179014418592809401498408275168095915657703068227257652171887045961
Candidate 71663158638269363585044239022968006234260491334688964429061601495433021206001
Candidate 86256986976977575405157050633552059283724453906623219340374117911228890993633
Candidate 92180394800317335235084212554402281683465569976900993085449933080374683483535
Candidate 66256744728684142620477688984262336309321609035360769363538878030653647832707
Candidate 60904277567247517580202959753950683908192974541267934964592254660764572737179
Candidate 108776743717732464412962174099908111020192378305758663791536185959447681863539
Candidate 114011949334160359277915620899861246033902509168860587727642808125660335376643
Candidate 112798598462448784404849240189683184716093781193254643973316680500602053839555
Candidate 108140735542819869335989093093438538800821385447419610893055818597373937646199
Candidate 6757171687671590992432244529017195678261232424972927654721963185686708663281
Candidate 70686797268191559440252072020079029337639796056533569692822982865076574821843
Candidate 59893057090628357752579635559970231988671270093712332384753599969610284151687
Candidate 97142165259569979272523120590870105031105679223034521295301683621944615594855
Candidate 83241269272965054546111316120831524730589428578177037290502417546395135148693
Candidate 86381117668559627275147327271451493614955556423183893300730099610446349770981
Candidate 932722857677780224732392193390385873431261303024427227657477854643888407321
Candidate 68314350793320975286766803972157753237767614839543079614131110308401866249923
Candidate 98370182319207937627471161472331267432564053615290950320523829265843136904569
Candidate 77235200034156585336174086211942849123009387436757811622168221079784775695159

Candidate 72678973019298149174147464954243245411804789835185486129004692171009262731431
Candidate 73920460814471954999882984184104779382532047032660013964441112474412800542579
Candidate 61589304273728138868414716798846406209763331364341217032939151742814238916951
Candidate 110739768085890385030817179991099629234745087021620449664064331519869803441339
Candidate 100746570877911277259518750263065787951181494639486197399875845095615993674641
Candidate 110939938893135375011907928592514481278763815112613447608022066648818349822541
Candidate 84696944441987988369909511319760167050887956254064525426727330708788560156163
Candidate 79863629856851619235278238510948249531739586619649188461334676786850186642473
Candidate 74449383646779181428691711261692905857800670465092015318782477445404733385499
Candidate 59790259653539483077525150476605222603146572073530458504242023778963004959583
Candidate 82929802792615136467247234698716122733665499821824336882697405610739346859291
Candidate 74164351882869284855921751389937994786964686059069291465023652181725569085475
Candidate 110088310095330477237911018043504857999412392838356303171400349608759753968939
Candidate 103611656903240268698326623904592155374109406589862390017272845686723968216261
Candidate 70866994472588678875077246430020093126472551945287125390347387770217154390927
Candidate 103749318405082558529740694096529064159580406804081453381361885942676300167817
Candidate 73898238505994663723473997369790145120968932958704308449453427490224495316431
Candidate 105639212650768082666508946930864220898038180661828638228568185759661970677275
Candidate 61661864676361740188040424576077106339500396531639003454091975160065228219475
Candidate 112700111187487312972101073714169639888121217555328387815232037966989105730745
Candidate 59981851780968067335832662932340263929134849184384572298184313163223425726139
Candidate 86646281286006463284425642025175726355691690667466402006756671207759912199595
Candidate 63803178344252983906294052010708138166533851748743156944661819435155260009055
Candidate 110473796450643368115342096669421154327385493762768252382026423454647873553883
Candidate 74642141022609962156583621464109467671306776798718429252413398923501032444431
Candidate 10127276601836952249395762632256399506849889860066002401941346351436131734777
Candidate 110620589706407867674590185583292459215344852007526891622320392584511244707497
Candidate 85554030705936914460251634707212338217823371694854033879869826633830913808035
Candidate 66526720804395088692638475644976331928799602884241316957168566029203413062493
Candidate 101120043887980057470546476345528775439400306678798284553997887488137604501985
Candidate 81415582927257550815688997425769658804525489926004578572258541085788992542641
Candidate 97243642023262833037832963793350257090181806612947619996965310859090588711089
Candidate 87634177383218929471874773345281200933563015043691391217187775217097503824923
Candidate 107690988470191925696353461710637690129586749580194423762915940647426576900739
Candidate 72960488526128295741738392348826778826053948767470216571114929080738290834751
Candidate 58974982424105765349303829820778546029043429086919410124895187417104032154643
Candidate 113589225232335681418537430676121406190306046252963647749141235604552989050771
Candidate 66227796685347134648255442796378629377287531662804722848537168066438038853135
Candidate 76421138362379446071731069512296987031390964076689413377249874815300835884983
Candidate 99830261463990796461441432664679095803224912467037041895308997426003277215181
Candidate 113945836532331909598701337253478325015036147205078249258766724302442995911607
Candidate 100359249745521158196219282982898637144101212450801748666732677158108162496343
Candidate 83257649499608172411507747749734129560408232528498985800795303786498810906585
Candidate 87515314449962506740276685617259520662288022159049254307491257416502702637133
Candidate 101499600208933001101909332330846867161850354055049765690222137464754633581681
Candidate 115574588957613306203218453898792976305408362093458147915609428684685135767081
Candidate 61482883373009430498718089141392534670048694942177153833836582256578484096965
Candidate 102086367674115511813508811109490439543966935193504716627875648988219153182219
Candidate 10121126610743370426250623277944889136565491603315034200763011728208361010657
Candidate 78162728468867170731120265759350234866349110236672970207783809179032027421613
Candidate 108279495476416222481048439551470525987293729682686470835157208702005485867471
Candidate 74333958371852755874320733459860965430596278018094405749147070859653179524209
Candidate 83156989385130078846042278065979946346533007950780286397780128333456414005631
Candidate 10880203784861330791314703711274126974887732749552986336039342716795697214461
Candidate 107251207007220745133373324804071198165071797105487994514635258125360992172635
Candidate 9010870153035205971379226948469993274136963556527911004424823362582153167479
Candidate 72398768751646741857451156798549112266395719757744751366555990476937422943887
Candidate 108781506176545221396372827757885330531607568548169986403551752757815811378893
Candidate 94390903202134632329724590436624165056024665076215204436623763067217516458793
Candidate 97700337483552919049822979619202969798773693348050131868137591603699162234129
Candidate 1154433440445180088632713044610606980673908832737317278332752176422704561503979
Candidate 81256265321761731730711435155384400431460368139207383900035266106794648907665
Candidate 87506824265004481466115740891255453487512409273727987577718280702066179397493
Candidate 96208086170726042147317706215779249279537036067992546185342757570183598696101
Candidate 67177829271734228768437130086488125453972094762691105008986711654294647728675
Candidate 69368763437557816960874713462016705896695021388387465287079787331779116310123
Candidate 70230481424942830507961392051594757065109400914449177394236928646026857230207
Candidate 89011621859306636853050960104360464017046151706943161681186151851186252836359
Candidate 110603645529872475585336051472594716294841448794370637479409852316123931938563
Candidate 85350625547571205536568072485766963061587574302142764170865971428822221443703
Candidate 111113101652566682576207268974776083938386840730107110111589652447627015237473
Candidate 103367394435864907697061378574583820431907923611392405051972739322390184333559
Candidate 95031415339741824508006252087826810098088612195950966198124492997436121906797
Candidate 103442204813300865222484220882890028073229585827851121703072540821405602328707
Candidate 69693474478819445452042345982236394021058118698310117009430421397586255616631
Candidate 112010052263508562992301447821131817327319749664365738883392801564446701354025

Candidate 67645129136355533088667821447463674121587227845661929513365493648163300817281
Candidate 104104766655177784804196075581526224341881516024629932838326441436221963180667
Candidate 94606295553329333867782729962787270234256549592739114137364029512944225792453
Candidate 104679783337951089427911708473352015364462655632106329912514950594907182769663
Candidate 89580266040682231345121356954938140654414905406247470319949365870617537851783
Candidate 92449666795096186168853393977805332779231393972510978319180692034365332155901
Candidate 88776735433681283397343662348950332318192999784776318539664707482648877412737
Candidate 99301997054298156037234058255716369902156263197681460744887351900279961508877
Candidate 68375309393505070572546424124593374568308158678836390012938688286198861617365
Candidate 95137430080483315850618441412039005456755654312233918320136640168199793758677
Candidate 58610749349198002764677686946422081369624369392273946279686133249269985118199
Candidate 114441491799423814215156929099881781393996704190299297607768337079553840036333
Candidate 84898390586161030696225614287782501183510813448618356213533973927928701664451
Candidate 69965340229419965344445428029930554697316787585900465028285518461307630790381
Candidate 87390428411771082894360598173446332477220756158548352598418852846733182907947
Candidate 104090060152552498534318857866186419245030758326262347790892592461344872443323
Candidate 82753867385234186417422323415485074658275359624227725921508840344969216686561
Candidate 112054783405795824836895171420684758159890931766608540426812504707567876765979
Candidate 84376607453891774483235173555864028384786462725268239158080739202287930769465
Candidate 104613965496322782236665236198334445063628499339845743773347069949032653980885
Candidate 80496588357227973412208388536978016819266460879290729586507656548341310148301
Candidate 80047549667218835703973349054220705399600817980491035314361483371436345678995
Candidate 64346260948769770479995492839330347957282701599685708197800209468188342853583
Candidate 59919672107348273448964333108751497591476095936735269388890928503536207666665
Candidate 93379974931234852776751708728236442893531201223848263608232359313378549559165
Candidate 94124042188472171694659176211749255010840124717804424735720716554913448960481
Candidate 83654464105712044817378413692215455620124485671118439030577327558081502180773
Candidate 97118651088770631378946344892835842252181399116701686791760837273791530231037
Candidate 7050126308240075988204462549064481495152232058547131020598178662177353066439
Candidate 6795684423393100585633483885688224137416212410563019676608894934284802702731
Candidate 60549033063957918019058835136321209152245193955006983328865694742134622400481
Candidate 59662779060085826929583251010711651626617383874871884152570665078652380637771
Candidate 80104382356403275434226725625530848889020518762402702484464183932521774670033
Candidate 66022221189617056465111929210466900582334556325089289974129896008672638264051
Candidate 104059840719147281855019186586575189567269140641627625685063704033244033920683
Candidate 75225640363462733289917616057549424336412127091349290454860336225756491253615
Candidate 97175454940965350315559819210492490125611259744871233654825633005404937976143
Candidate 65132505350411755490480442780715522549851136638769963096857729684541751305325
Candidate 93445034729198936850065903404554766537179549405198621867425094679999099288139
Candidate 106145112307397259397826544314419651927556349772760183220767550858793895451549
Candidate 62834079553328683969124184086383960709457100676074576187861926513248404320973
Candidate 7490910517344900407819175234597973703365000245658817903759228493673703914535
Candidate 108843119055350177893656287648447715486534399277361679571587238013349969629105
Candidate 9710694719188277835644517674011706960174154171472695707248092185255939484815
Candidate 97754976575191214913232354365931104374706404778131023727426654024409681865747
Candidate 9348555231579548200160484598824251863369310262002901734833125156637824911129
Prime 78969642338192227974176951719975943471383148654196544002681475585533408709729
Candidate 4
Candidate 85216619805109262412994309898491966768772307049024689209235976845687150962741
Candidate 62031236588779423917313316515346662176548137388049436454192051035065354268303
Candidate 102329683751337524513857896713955767234430659889885659093207198303028547641635
Candidate 68241139351981021447638554500541453664914124309264472290282993698533245309877
Candidate 114889608202828087358657772909966515851197017560756963546034167426478592752351
Candidate 77355564334440031168680389536127360533850327045580776683808797022284352943311
Candidate 110331614502793498175343450549615097091719913389602233321545375966103363488929
Candidate 92105773655336119773233984098595009644239973986980152976796002506115348698561
Candidate 108655524851666791667162277135838073656936203695982839449912154991514032565449
Candidate 58208180725075425614816670845694909416297189490455274930804974004653293178907
Candidate 102164555384759520519304849740662646897725474251833834043084349493941860170797
Candidate 860257598562362369606895310072728618341453393312257819390070923892191932849
Candidate 107966312168251248924564081656961846089315554419135881378642918068741771449359
Candidate 70622758811597302481452069442228564468969722331447331638629990281134694961583
Candidate 73639776237681596627994312896300102373300030657331433591690202497397472928731
Candidate 115473597180823397639029842633710481087744405337074021952114966533409603070173
Candidate 76906385773371965921757842208516926848817058472147571736711123360339468228275
Candidate 65426201382780695910580935086945778180804419513256692189435211499009021556497
Candidate 98604977841140898751855336041402972557300060174723922345484158859693702803451
Candidate 61162887490536863335154556475084260357519159883358077265701817442359829416205
Candidate 80921401065148042387534946365561041116183670867869988005843452859478762453669
Candidate 69937503695747732209125171002742597814888379735563766338821777470085334145763
Candidate 58003725187359925163069285658466390010294428041806677667850813227794037851939
Candidate 111120429504438681842260558981383774318526077064402296686563169867658981055621
Candidate 1109791384743550769083911149196050513122869240221530303022698074960005156475
Candidate 110120374929603998112669674249382236448590426813446941382906159007756846260351
Candidate 85736896190291501490603790874800503675247713356818083675191208915587862718421
Candidate 111448098509665098862941852508692322164183363373121397890048972403254180365317

Candidate 114079398551088740602101314403073961853843930117108392793737284719100299214361
Candidate 106587497905985157862299350673831869852247896206611535144121598516343229029141
Candidate 70907815016623987693999864542067819898272667854485305107057883848518010700271
Candidate 63569207330096027276883987580303489112195373794191212857509307754486498852305
Candidate 8548032295714132342183497104563200387281809626642312623362114727647140538579
Candidate 107165781841370127047538336111819132508472990096422404889989000547327054070971
Candidate 77536713700044881804471810275347631001946968946888213400831732644479380160559
Candidate 63891751063545092832763541561882191470014013779666340741053743561449177474533
Candidate 71062330989856758304006114908508003010666042537926453512887088187338437858379
Candidate 90341511834631143341954620757556263669940110736580115172717283065004704145725
Candidate 68390591784153446209237467708656263287428113745942284016973659832259031596811
Candidate 103123642571120927580947642011726379414512179989807288867750319046518465131839
Candidate 103761622645280666704060287972460544212773235486137424206500644885646790419523
Candidate 74230337934008203140895570891899744099148161871098246745783145863923333320771
Candidate 72701843736089459035016264624539002472760536397353512693219378627368093477155
Candidate 77497693423733792467248824490119038794952218869127228776071451583496976211289
Candidate 8009140152013406187894092117632073325122396063851462510913112161661204046337
Candidate 111263837405880886038294805499103927629892477784175277169125261140141754215143
Candidate 109051305257346232265732132303669326266497341571765271410735691229207388433465
Candidate 96260539684978964688850164926466605709986035424301802306092829490377157965321
Candidate 78166319937147858367584942690285178823569246843283599431340266609189399957171
Candidate 62251817739976957510232638642016414392261761849258650561404127893529617873729
Candidate 77440696761150961264813340057683746913899049242148029499102550570898255289245
Candidate 69644167041257692348026678018301137314602397580782716533114686178124438272577
Candidate 65624050582884990743803481419659645709007062845478702004101387423665556333281
Candidate 105599580039479795083475236559663372356385042773681695775082023018615580814437
Candidate 107218208153439500232852927316846773864341533389073731102409991706226851388617
Candidate 83424214065417008487044842499103237696855754883492183135876258613367663906035
Candidate 81782993937915728844731248311740262702832871648993164871310414136719324479533
Candidate 85444982147083560394510488365758497286960700145128143788739855967008114306785
Candidate 61600680778101184023571242672642174130899812828615904626587665193168189591437
Candidate 107706001717268305698872145325772127712725340032461777854206844741569092691841
Candidate 105265667815205608023448442735102284608007755135116597148337316019271776811249
Candidate 87624659166554498049644183997354851898703121493254440821895438907288174636621
Candidate 69054057987672974570048878988199991895607343004722092979329841588015603249943
Candidate 8161628144066965103432538794808738574840514393929913791004303692459360364435
Candidate 88039286886262724323872016780345677264289990351974473248589131305167685397137
Candidate 73499988775697701843930272811250771816996122756892968498939060605093880298389
Candidate 85595126902358224996369763324176521781422195536514908633090377823172530268697
Candidate 104842124561872225134648943996148898277637980466295026853826060980787718198365
Candidate 114976412669243072521735900683871609948670803734348507657417436386233162814547
Candidate 113753300522544572056824278576369949487828215431320989912574575166229070916647
Candidate 114050385782867733514097419064054985037310271367358972101807715043827818404785
Candidate 89806852394638741271576604936356776467296468314706033931870604942820918051165
Candidate 69563830603775417780503835671733514031601092736563566978879533873014901218721
Candidate 87017645467838023368815666092178875851826864469679839988428304281718908119917
Candidate 65659349819632066812061008577156431859150914640803218811188209225282559988713
Candidate 11142297729444210849092985175457758709001004384485416118410288589969269987047
Candidate 6351042727890759686874264080133656210541998429944834653729690104760788244873
Candidate 62340962758868489870253363078974051150278884306634557133573856439647180724919
Candidate 82574985975284958120306607786475318039893787576880926946656732340037355241545
Candidate 65074759221917423963974140078086298847204260616103620425410481675231995437939
Candidate 69887939049039383432823627591114297927243113529978226978972174375589593498847
Candidate 95732539579647510318257669917744528253585111571338944653032821188777029553205
Candidate 107018291269649495205437250831907002816816538366578394888393103085697577077183
Candidate 98834469656336149966565086670946166097956886416087550528988054874470660230673
Candidate 106202965695088488130918797349826896985665466084081393778579173372258993283373
Candidate 90921315379281857991613066836818481003004499804348380721828636384577016010741
Candidate 82882730680377904337185616574245374376173479489753313094687468363206057444737
Candidate 68252239913077831740158562701584803269296075173771277927328525769993413340981
Candidate 6166205214718547977048198742979758383286833155787211790400867522274392516353
Candidate 98183281948010715001782104497580506495948258728323354685337203292369526049421
Candidate 95168291102012069594582843830574770006980197798968159083961437326559335975189
Candidate 96842580762019317461369099245732180406106112092242335176689106171728731439403
Candidate 101509517689074899936688720687074079566235721712187742899966197788881652966785
Candidate 60997821671968077598797550385233728683049791778321470861178839315114959990461
Candidate 10562715874254781156132278952862380795624793235488737686892563129212163124571
Prime 8782935655740055326075155671940645847323940975233481431485480142093688080439
Candidate 4
Candidate 82531200269337992972556768373781465176940657296380822973213817198978895103473
Candidate 91509742452611841482397075542646804277182565320656236381844293569034842868329
Candidate 67979045103096129904771226314954339770320038386399017817011584102072651416873
Candidate 75345904173517680310665727553498105931936687147840146697460194000708202737327
Candidate 703093145167530212527406757815122119788232416023795594655560523642493789111
Candidate 85119453287694770104269193764030978296573558287950595095944725706674530442039
Candidate 66321380289734960704985944214470681480273837360643281572704669721309531144309

Candidate 83304198751246394221756773512912550464232113844703848566846945424575595344597
Candidate 94897933548899908676518374734126153428383263425137346592993451075012135151997
Candidate 96052022073956331618665182194508522736824873749113655864323911127971872388955
Candidate 1097789613541458760898370976693337209693835973646309839304989601571458313907
Candidate 60565295173744946875623152280394618776111115264681333315696173812496714946263
Candidate 97385170620965371358253807122540342762856914524696165606040696002052289201111
Candidate 64532874913284184519733181918993835183908190144408574697589030188493662267229
Candidate 100097826309359656116372684707611373933915109495863073933157173962504183557975
Candidate 73586790950446919161631283348959503407778816796583234760443103728732446209725
Candidate 73462399836133638049261692453419095616096218420683803685433215926469988674533
Candidate 114582069202586984696864601453599430625138645686978911474180421144673349900107
Candidate 65950972184768636656218686699419670625853750970654411152889373071996600482599
Candidate 62445832244272798328632466501301653011400637863978138320759542231950820935407
Candidate 106462198500178641427758649674739424545136411374814369891204422166767615878031
Candidate 102699761943669156879247466609489749717444756874674463380138564207148740002981
Candidate 86600677400885083008122487484357901031456712837019948615096043159816525036971
Candidate 6363278032059003072852616003217652479297963441793958464560197571049902562175
Candidate 66046787072457344123000585368874276798000048181158460659925879313924201479053
Candidate 7080604383734139041546687790884079605828687372447735273283425424385193866711
Candidate 58090252472413606208382327077297451270579940011398319842872208297376222415539
Candidate 58301065275316752105856906134761174254805771571446997306625819695057038306799
Candidate 92371500753245972995075322833528548986500138349971503944823151185782290962293
Candidate 99040233987003292543801032844856020245945371717637956188272642957188225194641
Candidate 109597886470456060451394757964899234472699329185780024155987173401622888706155
Candidate 73664410962443272353069965271893359576032109161029049213586763215368067755059
Candidate 107391072079868959865155139918871896670334205103656478089228007646404719583469
Candidate 105989527050246722814501954979824869125745934326858723196775392337198366840051
Candidate 83638683854263549632257078258376948936029995727628037156839692786097530474541
Candidate 729669215958497378597786427375224064968284829494679055660559669137405609004491
Candidate 88845117654794952951580822104052916908705322109813684743905426447431081194401
Candidate 110430473207458035126596514758437350180655997673769972182564959791975310163601
Candidate 110558023826018863414158522100887601983466164669139625643625341025202101153877
Candidate 91685778094920029013311268414561250328478680814079772891804102294313619712597
Candidate 109960884280358954667186380833113729831080514191733358811014415589847287855993
Candidate 59362425426658469218570464502861726903378673048473181948473508658806936954069
Candidate 70559502400514301887008739732375476414586117296989410084632620504479845681887
Candidate 106324819404897805135201468774045209511223580093036306871274904662961488543743
Candidate 94337823680579022321908859770706491751526274142658225170522479380619826907117
Candidate 83661939302966324037513533137059896203658478491614332780284073500205163180721
Candidate 74543145397337269578984401629311024961830403826203451735119546430436780487639
Candidate 1097967036004085099400985823236607710782788922085700852283790590255621043535
Candidate 5810252079016109012413775439493025174634235275189418392016115730688349435759
Candidate 94636815356189353627581128179787299863958027655970882985601167337100853138879
Candidate 107750370092114787871508182430881409517439238147188288388559430658805808278851
Candidate 112812077754474989881488781160417442070071046089056024588972474701152977031029
Candidate 83576581197612375499804709774122139591455526679632209878156465597565297108319
Candidate 67962018884100728982256421369486172258495316373362415456199218669562511722421
Candidate 64750653996894015095538241655464642672852702306751254987904979993525920088281
Candidate 77569483121259881489202621518910617937240496947649102211817451250683855955595
Candidate 79223034693066127196415081592405375004674536630609697240341914888558319762907
Candidate 100207740217622386987919378528287036257272626466217235135595987395179115944419
Candidate 62201882344390015610966309161189982491286794980148314306099403726557513444451
Candidate 63160176109273063075183868625216228956173712823497837740825650659659030246251
Candidate 84374323000110851391029265261719397257419783301798456991078807231458186567089
Candidate 58965812235735426063575304691900331388086533378989978436081538070232439997957
Candidate 93249031143899251559528547677399505326576264071521295309921397976733875338221
Candidate 101469789738395008382203176116432703917186184610138058824456833477030219224347
Candidate 57967140817715574263496000988376377757204718994801514350965024596937438025285
Candidate 95040858974389086756698755305150399288756484058091359372413732137133906396143
Candidate 72764349926463876951661409391453384157901856505302164645788845967438213212957
Candidate 1081684092955404374464601789172601247687860538025335666715845168632166564072755
Candidate 104699424156640576776011639849818510480989597189824846022671167875155732664961
Candidate 88500348831551066442499980783298613016957540927487994487157041527961357604001
Candidate 84381740507692289625798588186934951181616344244341300448692524965279705061795
Candidate 105733369767654654999860746759197959841025146989033621616441691337589102459391
Candidate 63227475034607155125870206581903329427360534643299834098929564325728354784539
Candidate 7012493414077832703558375686297477832941474681148076820219870119213638615515
Candidate 75440731245287497068974891403525917892151382516177800872147751028595171344763
Candidate 85614358080563521416012813710634175620696316120327145149960489801437261403449
Candidate 110077265040095963381265209954834435094786063916753168858480498402180422494605
Candidate 83065412308158273020300200597430901382612872747736554420598951934353267798309
Candidate 99458421235942802094441408515295449770926192195289203168150507913348169902037
Candidate 64888128581716392020821107343437543059485594546099363720858747583050300257745
Candidate 115319704234160394306193144672461705271826052534335623372548086309998662147525
Candidate 59410346872071966232847558759601509047051098913084637656713209841140075479015
Candidate 8261188797940970080038271821553030542325305461022005090542435337618770056133

Candidate 85387985052089200868993476173055340657694322234246062917937108446467433420139
Candidate 86965005121019408633004716272067575495545750984470419156082503034438164328343
Candidate 9792261494023269934419287708101672638762565725725656660502681530070062899877
Candidate 7481867441370643797434197234306969760273626022429228836672536821660334655929
Candidate 106884709449093150539906532631455646948589586451270849744225771487887571168915
Candidate 76195968073708860244972521638299758090250252168573536618660004936302306215997
Candidate 100074805563269188785887212923379332706689261666374120100681675647577639788181
Candidate 88780306337967347320984094543830967711056485573244927300022747838273500676543
Candidate 70457514979908128145938945037713321897948255009534559576965522368668283731423
Candidate 86520312918811288436805816929370947431420906425358665818497616867238551011635
Candidate 91239177795335722549098826687836214865219608354954236806815630318638253991845
Candidate 103143807806611995189786452479416897128875257542815335350267263001810723925219
Candidate 71740284227475286611550081348743840666502720196215568947269004710359078879469
Candidate 62750220444011791248308755021318510009052646353475657018973528640714498651063
Candidate 108440565914574776613532906811397835987006295690470418157633476268444887595419
Candidate 9538914389660214668114260844096823708229310814571529752656646766136373809543
Candidate 11504829098508832641892046946475667430241058545852808686099936628213958565225
Candidate 74466309427468951410245664459490958297652701091199462683549014965224795590347
Candidate 110799054626885168469931720231616445668650382865794626509118568977933347559997
Candidate 92663432923607298408964975845329475346384713127896322042042135483345973073165
Candidate 104107533434984664396568070684750099491882801259023974552875092995492449692939
Candidate 88230864598231837723803607741169595109511783387495432572349553103630061492349
Candidate 8960254892874655082893328591818751424089313711083348801562149077015896840839
Candidate 93367326568278755634697793210587925616740553815729249710277324593941271665609
Candidate 110054446360728742654430579539243300843212650471580656270879080290606622571837
Candidate 76012654120258917813048559991572295202515515790779170493644095701705672486175
Candidate 112378596001172986838179322713566890209267049824527907604637859964679928698311
Candidate 89601495004080322139178810777605557320678638714565648165385643682192030448619
Candidate 67974209438004423654476017083055504286947242796121296751501834230616888365625
Candidate 8509758622200670662807857899953571599165276577760205344277467245115758268053
Candidate 112828546156913850898759758804182786202390261315095953674162766812413491351969
Candidate 81342139054572368315412727556502773982767405759014307426216586281161872293525
Candidate 103330676558906167659369538087538162960454850383109290500043564060359356456927
Candidate 8302637898077928198650664168138039083461997446942715744266711466385989880083
Candidate 99012383663196055108264236860723175830800162472255118220398622681691983250677
Candidate 106097315043483831267851958021786330111968161534758060949314159024562429482649
Candidate 102826607510060425958933844082008657584954329397733856314618310758605797515585
Candidate 60366091262423455138855504819014872883517167950693895918691987807031854839869
Candidate 105329486991633624903250751031338286170459262534246722634779489210325854228555
Candidate 101813152390880378451775218018098795640870521846685427674867095204447327330065
Candidate 77126665636074148507249883082880550914575149974743188768264130865742469559417
Candidate 72859703404524802063881489986977876990381844808572496825917575195893802879299
Candidate 61609840126531591459670755525176369421075632991051407265624666470006870874443
Candidate 89054863146931790494433400479159785907127907769688360112022216987847461457345
Candidate 75548377789957781655157615025068626344243105121841585924955000372616423301369
Candidate 58577543387023227383981791245393720400974261314789719190818469586929077993239
Candidate 88754061921209665490137768815282195647563311952056149701175189669878860389939
Candidate 111573405176705220054713193208960566582347842697999221308123024033255164037519
Candidate 85085862187301743540276813690149841423477074540373906249443096981499825549603
Candidate 90791594620174406419244672484863153883266528512023187095519183083512440541677
Candidate 109292108845682192158132997827278845177493568660439621967616491301930592389037
Candidate 58376396917619492266381555809561269303163261815950420983771212096855652880201
Candidate 98752729054722638696433697916746291480084327054150213445606300857066441825961
Candidate 93400134587838916095115068044794129616244070003927186204385447531581905194215
Candidate 75142150362331099485104291516166483723906519773189727696911580520957063407727
Candidate 101930134787450662607736734482331652343229117427594053486821845302849998157039
Candidate 111040106560880941672943259359353218984238199592380327842734037913064387063011
Candidate 81065007431528385271944021052891326253206926231015593435347730880683424974135
Candidate 62386414982174798647586359785528415163211992177231463499663884971490780764965
Candidate 108502812787525061635290205578448027285958633891210719122639045173690857316637
Candidate 111014058394941106932014765226721591561049711337896552942190647600364531852627
Candidate 64487925141997765961299989782937690552097302553028856012279338189977927496541
Candidate 82344669383949855027248131240495835122981316008867332234365927611843895246871
Candidate 67354398021962616040075462776341868338625659039479495587770014947158093360673
Candidate 72982806247334277607361370119195564166903732600490247601618322552470612906267
Candidate 82167917552814000699028214793848516868345899558656766738345431358919252014017
Candidate 73956757734160042479412051511809840958376950642193476405009257212065628307595
Candidate 100099575454691246033026232792867318805777320889059033953301154663515118007683
Candidate 89125055091868187702985305900260692855198370833340453687395336679825582249839
Candidate 86106499746645637932003821265384897657476210604096330054600954587339553032151
Candidate 66810888808552116212978088901199947392956683766181908241866553526446063989463
Candidate 90270688649689798068743128322079406464045590289149877041801258260285678134059
Candidate 89663324219992128176759061356707737659365125126936717466500204174236455528523
Candidate 110442504863007057877433574322496969515632694021826495261517376438096456935555
Candidate 66488259659831741877129073825643189178700899431055718679671331356440917393213
Candidate 93454921922802435528511762489794232582721493223085882557336236978478726415421

Candidate 94864040335559209634103637409534426724612624635545339811448262679380615988287
Prime 61956383508975613888915561873352308418051505765770090133435314036341650531649

Вибрані числа, що пройшли перевірку

pA	61956383508975613888915561873352308418051505765770090133435314036341650531649
qA	65620629053331790136688908026169806950420785748631833292836535063668149515787
pB	78969642338192227974176951719975943471383148654196544002681475585533408709729
qB	87829356557400553236075155671940645487232940975233481431485480142093688080439

Рівність $pA * qA \leq pB * qB$ при даних параметрах задовольняється

Параметри криптосистеми для двох абонентів

A	n	40656168597284517719806762601549963474377938989366807088543627291769997920082293613704 35107744675553541154412640414588026215336067792938032508650468642763
	e	99718667482075234398285743957600107955603810246476007163730442309056379183319783891995 266343800448302458955893487589706094541604507977892294213896467513
	d	23378991633346589019800671965129398581035722719629607197268691259596378031567116457496 350245570199060206920015368358641632400183907739258015972177375113
B	n	40656168597284517719806762601549963474377938989366807088543627291769997920082293613704 35107744675553541154412640414588026215336067792938032508650468642763
	e	31562068103163868075090293480971253823339811557115406856919922343939941217881467380123 46471947291586663186716061539253388526337809184658116076725511557023
	d	30434132824175692186853547435211822435702623726560949745308764099881495349067798711784 79432824908462944743759984945833498073868053487917242612704369244127

Чисельні Значення прикладів на яких будуть проводитися тести

BT	1234567890
ШТ	40504298285791715600554286615804609096056461205856667936816576743118949926128418716925 61401651035006985437466384065635972781928814435801339360931952393407
ПІД ПИС	99241745678707675487270965894732828050235777072637728757607584514800595582833676384609 0364163947320448449795032296661705159435391116719140099889186342967

Вивід програми:

<A> message 1234567890

<A> cryptogram
405042982857917156005542866158046090960564612058566679368165767431189499261284187169256140165
1035006985437466384065635972781928814435801339360931952393407

<A> decode cryptogram 1234567890

<A> sign message 1234567890 with cryptogram
992417456787076754872709658947328280502357770726377287576075845148005955828336763846090364163
947320448449795032296661705159435391116719140099889186342967

<A> verify message True

Протокол конфідційного розсилання ключів

1. Абонент А має повідомлення і цифровий підпис цього повідомлення

```
<A> send message 1234567890  
<A> cryptogram 4050429828579171560055428661580460909605646120585666793681657674311894992612841871692561401651035006985437466384065635972781928814435801339360931952393407
```

2. Абонент А формує повідомлення, які потім будуть відправлятися абоненту В

```
<A> generate k1 = 434884656101619600803659738013348361402385231316041247305095660917119152444625048566329501406906160937617364080971155529306248447053000886195960755168124
```

```
s1 = 2498356133692923985075349505745756516283709624087853805817346773550255514700911644916680055923791865256447489953265024866314081183116094917439317551021594
```

k1	434884656101619600803659738013348361402385231316041247305095660917119152444625048566329501406906160937617364080971155529306248447053000886195960755168124
s1	2498356133692923985075349505745756516283709624087853805817346773550255514700911644916680055923791865256447489953265024866314081183116094917439317551021594

3. Абонент В отримує значення повідомлення та цифрового підпису за допомогою секретного ключа

```
<B> receive k = 1234567890, s = 992417456787076754872709658947328280502357770726377287576075845148005955828336763846090364163947320448449795032296661705159435391116719140099889186342967
```


4. Абонент В за допомогою відкритого ключа абонента А перевіряє цифровий підпис

```
<B> check sign True
```

Results

Decryption using C,D,N

99241745678707675487270965894732828050235777
07263772875760758451480059558283367638460903
64163947320448449795032296661705159435391116
719140099889186342967



Купуй вже зараз

ASUS Zen AiO 24 (A5401)
Висока потужність. Сучасний стиль.
На базі процесора Intel® Core™ i7

RSA Cipher - dCode

RSA DECODER

Indicate known numbers, leave remaining cells empty.

★ VALUE OF THE CIPHER MESSAGE (INTEGER) C= 1234567890

★ PUBLIC KEY E (USUALLY E=65537) E= =9971866748207523439828574395760010795560381024647

★ PUBLIC KEY VALUE (INTEGER) N= 40656168597284517719806762601549963474377938989366

★ PRIVATE KEY VALUE (INTEGER) D= 23378991633346589019800671965129398581035722719629

★ FACTOR 1 (PRIME NUMBER) P=

★ FACTOR 2 (PRIME NUMBER) Q=

★ INTERMEDIATE VALUE PHI (INTEGER) Φ=

★ DISPLAY ☐ PLAINTEXT AS CHARACTER STRING
☐ COMPUTED VALUES (C,D,E,N,P,Q,...)
☒ PLAINTEXT AS INTEGER NUMBER
☐ PLAINTEXT AS HEXADECIMAL FORMAT

CALCULATE/DECRYPT

Висновки

Реалізували криптосистему з алгоритмом шифрування RSA та знаходження простого числа за допомогою тестів Рабіна-Міллера. Переконалися, що звичайний алгоритм перевірки числ на простоту не підходить для великих значення, оскільки виконується за $O(\sqrt{\text{розмір_числа}})$, що приблизно займає 5 - 7 хвилин для перевірки числа довжиною в 256 знаків.