МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. І. СІКОРСЬКОГО»

Комп’ютерний практикум №4

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

Виконав:
Студент групи ФБ-83
Сердюк Олександр
Перевірив:
Чорний О.М.

Київ
2020

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 p_1 , q_1 довжини щонайменше 256 біт. При цьому пари чисел беруться так, щоб $pq < p_1q_1$; p і q – прості числа для побудови ключів абонента A, p_1 і q_1 – абонента B.
3. Написати функцію генерації ключових пар для RSA. Після генерування функція повинна повертати та/або зберігати секретний ключ (d, p,q) та відкритий ключ (n,e) . За допомогою цієї функції побудувати схеми RSA для абонентів A і B – тобто, створити та зберегти для подальшого використання відкриті ключі (e,n) , (e_1,n_1) та секретні d і d_1 .
4. Написати програму шифрування, розшифрування і створення повідомлення з цифровим підписом для абонентів A і B. Кожна з операцій (шифрування, розшифрування, створення цифрового підпису, перевірка цифрового підпису) повинна бути реалізована окремою процедурою, на вхід до якої повинні подаватись лише ті ключові дані, які необхідні для її виконання. За допомогою датчика випадкових чисел вибрати відкрите повідомлення M і знайти криптограму для абонентів A и B, перевірити правильність розшифрування. Скласти для A і B повідомлення з цифровим підписом і перевірити його.
5. За допомогою раніше написаних на попередніх етапах програм організувати роботу протоколу конфіденційного розсилання ключів з підтвердженням справжності по відкритому каналу за допомогою алгоритму RSA. Протоколи роботи кожного учасника (відправника та приймаючого) повинні бути реалізовані у вигляді окремих процедур, на вхід до яких повинні подаватись лише ті ключові дані, які необхідні для виконання. Перевірити роботу програм для випадково обраного ключа $0 < k < n$.

Хід роботи:

Під час виконання роботи виникали труднощі із дотриманням синтаксису Python, визначенням сильно псевдопростих чисел, із занесенням даних до тестового середовища.

Відкинуті ключі:

2311103834992173627152801585216681200512306437060452302756222116006749293300 25
This p is divisible by 5
1820138012628147195121196363158932407126354035873589607988817327520919685212 53
This p is divisible by 3
2297743931738558263690203666976449063284578181393660842485350536587300356805 07
This p is divisible by 17
1868633720000161542361958903211096829458663832971286282930085333278368858481 21
This p is divisible by 29
1534882100704562603135090368671191338943288823978783344854578923387735409843 81
This p is divisible by 3
2097053622568657000628161110436119647035121953947940466498110051715393843267 57
counter < 15
1887770278129875314447482691630871633390666584273618352723321040279002397568 19
This p is divisible by 3
2211820130421296053200065732010022738921608755789659272848064297652290627875 11
counter < 15
2080473924535028860182863361022559718089979288788120028303528129956433655336 95
This p is divisible by 3
2125148645210821799208291496654142114285740915368880722020690573852802741859 19
counter < 15
2061148194053188124962038210828416418842216273947688034669789335303072649119 45
This p is divisible by 5
1340477314311630969460120601111965560937891275392749623351352477127561247412 71
This p is divisible by 3
1382680456316651467422234450387044067216532431573274076011394979521681913252 07
counter < 15
1275661161694430971565266480505155836243883062789976745541162265955860780886 71
This p is divisible by 7
1451105586783001702587572716513375921093637753696749553475702485460415578614 41
counter < 15
1507495311873144435490070610648176213020968466636821106630695039853453598593 17
This p is divisible by 3
1292454462280998833046180696207687533929170623466386130543590717086743495954 83
This p is divisible by 7
1728856452589769013382966876847390677230420043861490562254513697345555185995 81
This p is divisible by 7
1681941469290289947431863627879171023598256405671804038175297272308451096492 57
This p is divisible by 3
1914922125097690330336401475939921105353800097473423765474105538702577901983 79
counter < 15
2266260216835147553033464894870604469787966645862373129084278416975342282290 81
This p is divisible by 3
1774631551796323225115023737669382633737930108202281298731737559407168088297 77
This p is divisible by 37
2048609985780010234738743530861154872390156810044136377201063653398972359821 35
This p is divisible by 5
1285587371532119548215837330577041116149292925202751330674430945293232790606 51
This p is divisible by 3
1877472205087801262070586122924723499609609460160299506850965317711177802170 91
This p is divisible by 17
2008581142558273245985209931608817845625035730835395475624996896393493634950 09
This p is divisible by 47
1566066569351341657277923143136793504836101026059261698472404313368599347507 27
counter < 15
1574789800879764609536307473265292751919862281724769839616436954633141211700 61
This p is divisible by 3
1739806955646024370087585139260257471551786285558500036858122934658485535049 91
counter < 15
1412832167595441580922053411192421814112979518889934217332798129349280198499 35

This p is divisible by 3
120039832808454132904256993245088819479738217098021859189987249724567889859123
counter < 15
211605663291013053058862935789892799568773061167132596919591151331999347132415
This p is divisible by 5
177078009751988958353667501209411000814941192730944164110047540539522851871497
This p is divisible by 3
220986594734975268840151674953496317548652189665529020111725843199225976943139
counter < 15
188251700895814137823127190002067503755790988012374281583209673280262782677425
This p is divisible by 5
146255525806202747329046708789394137331090457089355912472240727986212829381583
This p is divisible by 3
148931326423645654545584242364041601854457599287337514199353070720241236965917
counter < 15
154983109067632817402828247118005074070638761003298326371616656517891361784781
This p is divisible by 7
148662908049652979223671369566357107427362316298255000597981946366097191366057
This p is divisible by 3
193634374999897670838479794528077250479468630213358907580699808905216282683049
This p is divisible by 3
180336393351963878244319420161552075109872379708655006591182428801168133664327
counter < 15
207576738027163271379646732030931627162071369827931625614563022104673514804545
This p is divisible by 5
213852388065674284867819205885011876288961576515204566084483896750133445842285
This p is divisible by 3
154782271449095775788586962285127967808213518493313983386327993785912435461091
This p is divisible by 3
185747659014405137327670103235521389610017337841749410123518034714009216867585
This p is divisible by 3
137084453781422002292777082207764200727358971339974644052162602296880406921371
This p is divisible by 3
138556953293571751805774521683967330037701794575647692532349556961671699531483
This p is divisible by 3
170896854785390790099575041821085106525666775368672883690915408006488272215091
counter < 15
152935602452822613816813143600941135665750685344729142693438240290034518441729
This p is divisible by 3
120689294684887192495955818355335289521913145614443987066828219850393135218433
This p is divisible by 11
149949857024142232776500217923586079665986240998515951371724372062361408851747
This p is divisible by 17
225167441062376072126651185853289279493366776638441040170448365984034532527375
This p is divisible by 3
144622277490033779750751174003526459025077931037141240175625333740637526145237
This p is divisible by 7
188480865645867482409366968863061145894975335497660002666127197027431703982933
counter < 15
192355978252211792579484876465736419326433132644251026758378831995861384000475
This p is divisible by 5
202602143459884648560499103704524736125348751609227234789796293908270838677493
This p is divisible by 3
221519747709270383512870780622471411626945345740275654792076377657183915335775
This p is divisible by 5
198689767361346984187063601890010556779780228743937278768660487482745976972847
counter < 15
177883349119864312000798086190487770999329661450847063089894399611475075522541
counter < 15
199620213063898449748127335292022417925614191232736034817054486096735403111181
This p is divisible by 13
210850751844243525093056697593095491066240193980855557774894422793360665093237
This p is divisible by 13
213809037175414379964744106052118121370260878824972997125378865932719726274921
counter < 15
142992102029003858886668319983056691324305055252422245738843334455026385110375
This p is divisible by 5
152571360302913350177628438577564882451573305601382674756271091031486772649225
This p is divisible by 5
193243788383164795039069703996690075112379086989624846313903444159141307157289

This p is divisible by 3
179182395381528129130336901838881180795429293152642807542012751828509031753841
This p is divisible by 17
188843723328907290772214381914543126318695529129565473763507885898843773278867
This p is divisible by 11
211608620537956025756028654269381258021978081415999882712327865165737846098433
This p is divisible by 11
149409649861781760671902308190305077681454967425767845954586086792072522371123
This p is divisible by 3
178574914179886016512724289944272921429340973806970642365863096064413166088803
This p is divisible by 41
228110954264003012148512876725824387976743985151896443930509872240919553664415
This p is divisible by 5
143116683037755148343345322601405812953535417599062998772871330017259291623759
counter < 15
212610037007499585211633990043154543657100626095803362676735271689428723114373
counter < 15
153387512828569699290131196844589055996830482051437145851008426679125894310745
This p is divisible by 5
125306234684525470324328181070915711149856069924993269508650049706618607433241
counter < 15
171995225561464302738771970630207204648432155618876506585413050465452010146691
This p is divisible by 3
138910756544559429086259782236379855048420196513697944904192830535404557807041
counter < 15
207846967021408897313326783684242052867790085527798635392239688133735740432883
This p is divisible by 37
134751878190889025335617354442083437933646904136667061192930949819018072596487
counter < 15
133638221274432509405447890550525752727352050819261729159138343977433551380627
This p is divisible by 41
177419569184915159920748875145617873262257496024155620724090783189655199643921
counter < 15
137209463285236999095735605390047183349299837948535955007659445590108533501153
counter < 15
140851757371716706210760663221352463511452462756984855287789007605427253791793
This p is divisible by 7
200822625029863314663089162774181228999105563906424931418306908765783473199947
This p is divisible by 3
161462537673998764256770821201446876369312955557534143105982028996212900810791
This p is divisible by 23
205175226803265985271608125388840522003328004571008740470275771599256225503799
This p is divisible by 3
128205344261209419456122451362686418502978020195299248698113087895457634553525
This p is divisible by 5
162111873717687288523054461766323836501661630778386871337915380170543277791153
This p is divisible by 3
224410986475732369587721888927444307329564712124460244514734183539854516720123
This p is divisible by 3
203920355399818444798144618631591022751258441475436625901226561787547085666553
counter < 15
136044773899520203478092201184809468740146855534778509270752016268415858827063
This p is divisible by 3
150351409463615772457455450736151066346708965549584642961224893911440115805193
counter < 15
147561154147244517370784136543645617528204909903002354308501203518204244670451
This p is divisible by 17
207043442460122721484378049366689096978503666585033681471751486321647076300861
counter < 15
150877232711633836054091697904670539003523605462874195922702739781664339616469
counter < 15
177354148728125964051383665509554914277470301352418516730556388608768401061635
This p is divisible by 5
136030465189552774187940765472230726173210342292391050018193382808487428034351
counter < 15
197466185309915701412672290550621461272122015725675286987924278292068801318707
This p is divisible by 3
229993814057637271372191302026431716565524162943448390523775974497033676171983
counter < 15
207195653283896573923622515970274773279090502878331195947089027603193839478219

…
This p is divisible by 13
19757169792189846971749338506633759857692861297306599553984005905415040077818 5
This p is divisible by 3
13554569633667574879228516664217509771835721138784395422742421812014237817110 7
13554569633667574879228516664217509771835721138784395422742421812014237817110 7 is pseudoprime!

Generating good p and q:
43231626083464863857844923523815031431549378215938610663775157224777863535265 5
This p is divisible by 5
86463252166929727715689847047630062863098756431877221327550314449555727070530 9
This p is divisible by 3
…
11456380912118188922328904733810983329360585227223731825900416664566133836845331 1

265 11456380912118188922328904733810983329360585227223731825900416664566133836845331 1

30151091988469950869999057196905920343523997163217180779397611503077157622615 9
counter < 15
60302183976939901739998114393811840687047994326434361558795223006154315245231 7
This p is divisible by 3
90453275965409852609997171590717761030571991489651542338192834509231472867847 5
…
This p is divisible by 13
21015311115963555756389342866243426479436226022762375003240135217644778862963212 7

697 21015311115963555756389342866243426479436226022762375003240135217644778862963212 7

42851970549361360398479231185704335087667243612772318910407354089920433040967 9
This p is divisible by 19
…
17055084278645821438594734011910325364891562957883382926342126927788332350305184 5
This p is divisible by 3
17097936249195182798993213243096029699979230201496155245252534281878252783346152 3

399 17097936249195182798993213243096029699979230201496155245252534281878252783346152 3

27109139267335149758457033328435019543671442277568790845484843624028475634221 5
This p is divisible by 3
…
20602945843174713816427345329610614853190296130952281042568481154261641482008265
This p is divisible by 3
20874037235848065314011915662894965048627010553727968951023329590501926238350479

77 20874037235848065314011915662894965048627010553727968951023329590501926238350479

p: 1145638091211818892232890473381098332936058522722373182590041666456613383684533111
q: 20874037235848065314011915662894965048627010553727968951023329590501926238350479
p1: 17097936249195182798993213243096029699979230201496155245252534281878252783346152 3
q1: 21015311115963555756389342866243426479436226022762375003240135217644778862963212 7

A has public key: [65537,
23914092174761409756113370899680952621674664871993127171823825412348273744197308229607725740069705193881766176500488249897370796610134415909000584789111659859 69]

A has private key:
72738073670093831282842354015936052849605988915927033132907538607160915027668205021715994337885219932139884697508923391787129977219901277118103962708238873823 3

B has public key: [65537,
359318449717747749775428913336752324682784772619375281355043303964655439361538661286668760627918347699224964515519118860466120899744941948360326666802044991494 21]

B has private key:
339262803455826678187188393249079101866823915420515480338873073317803896001535782625338554832067399033044274688713042454825236508628071748398600145207687532705 97

Checking of encrypting and decrypting:

M:
174358945183808502731412947590021318574185283159781813595114326911650063122499224341350626269790465023055054856354029768699075787870877445059372601205703133063 7
C:
205815091613080412600871695963757451366648063565021051873893939351744206471187965601922606299961164210378652080493301599042705454560404463665501126099010414644
Decrypted message:
174358945183808502731412947590021318574185283159781813595114326911650063122499224341350626269790465023055054856354029768699075787870877445059372601205703133063 7
A decrypts message from B successfully

M1:
246625047666450262898032997800602969336467779494511333756511634730739045567885313835007120622979740103541804064108546086549975306784944129867834342921585814363 14
C1:
243174770694564706912836921888386833637584138629664566855270650860832256086227486237449235620707738020639026921755186215955265864181959842103765644901817977969 63
Decrypted message:
246625047666450262898032997800602969336467779494511333756511634730739045567885313835007120622979740103541804064108546086549975306784944129867834342921585814363 14
B decrypts message from A successfully

Checking of signing and verifying:

S:
654414580709336550969498854386974419992933882355980704720399598575652720948228942223908108675907010790007920869812168388767262001535344814771372749666042938416
A was verified successfully

S1:
171214850299144763898158935833767868623886890778358053409809486614175808722770592112313586811434994114019615379352767963680199262112076128070619235306476518978 81
B was verified successfully

Using of protocol of key distribution:

A sended key:
[87212592658906421596653178021825276100198496743744144600479567905020589662322462213825328648478500040949984741936581906349453726420099503570962711361392669964 0,

122303248485669497945994936174636720422681724765635539357501111749986204140380618581552281041083451284423244415719003799475479506198430329389502475465404062285081]

k:
347813819360549337337368372707830933740620838903400817386817901136321078722158219773702845508063311631088571501441884159576232000506672585402431413572205170652

S:
832848273023487363758519804615368740194112900954021868125535083142259720217298488619487397948622238875434093109347689814633376455908421737032213439750231403227

Sign checking:
347813819360549337337368372707830933740620838903400817386817901136321078722158219773702845508063311631088571501441884159576232000506672585402431413572205170652
A was authenticated successfully

Висновки.

В ході роботи було досліджено алгоритм визначення сильно псевдовипадкових чисел, шифрування та розшифрування за допомогою криптосистеми RSA, обчислення відкритих та секретних ключів, створення та перевірка повідомлень з цифровим підписом, а також було організовано протокол конфіденційного розсилання ключів із підтвердженням справжності по відкритому каналу за допомогою алгоритму RSA.