Бердақ атындағы Қарақалпақ мәмлекетлик университети магистратура бөлими 5А130202 – «Әмелий математика ҳәм информациялық технологиялар» қәнигелиги магистранти Балтабаев Жахангир Елибаевичтың магистрлик академиялық дәрежесин алыў ушын жазылған «Мағлыўматлар ағымын шифрлаўда RSA алгоритмин қолланыў» диссертациясына

ПИКИР

Электрон түрдеги мағлыўматлардың қәўипсизлигин тәмийинлеў бүгинги күнде баслы мәселелердиң бири саналады. Бул мәселени шешиўдиң бирден-бир бағдары - мағлыўматларды криптографиялық усыллар жәрдеминде қорғаў болып табылады. Республикамызда бул бағдар тез пәт пенен раўажланып ҳәм оған болған қызығыўшылық күннен-күнге артып бармақта. Жаңадан жаңа криптографиялық системалар, алгоритмлер, стандартлар ислеп шығылды ҳәм ҳәр қыйлы тараўларда қолланылып атыр. Атап айтқанда, электрон таңбалы имза ҳаққында O'zDSt 1092:2005, хэшлеў тараўындағы O'zDSt 1106:2006 миллий стандартлардың ислеп шығылыўы буған айқын мысал бола алады.

Магистрлик диссертацияда информацияларды қорғаўдың кең тарқалған алгоритмлериниң бири болған RSA алгоритми қаралған. Алгоритмди толық тәрийплеў ушын оның тийкарында жатыўшы санлар теориясының тийкарғы теоремалырына тоқтап өтилген. Магистрлик диссертация темасы бойынша тийисли әдебиятлар үйрнилип, берилген тема бойынша сәйкес материаллар таңлап алынған ҳәм оларды шешиў алгоритмлери изертленген. Келтирилген теориялық мағлыўматларға бир неше әмелий мысаллар көрип шығылған. Алгоритм тийкарында мағлыўматларды шифрлаў ҳәм имзалаўды көрсетпели түрде әмелге асырыў мақсетинде жоқары басқышлы программаластырыў тили болған C++ орталығында программалық тәмийнаты ислеп шығылған.

Көп мийнет етиўиниң ҳәм тынбай излениўшилигиниң нәтийжесинде Ж. Балтабаев магистрлик жумысын табыслы жазып шықты. Жуўмағында ҳәзирги ўақыттағы криптографияда жаңа және актуал болған мәселени үйренип шығыўға еристи ҳәм алгоритмди әмелий реализациялаў мақсетинде программалық тәмийнат ислеп шықты.

Магистрант Жахангир Балтабаев тәрепинен таярланған « Мағлыўматлар ағмын шифрлаўда RSA алгоритмин қолланыў» темасындағы магистрлик диссертациясы қойылған барлық талапларға толық жуўап береди ҳәм оның авторы 5А130202 – «Әмелий математика ҳәм информациялық технологиялар» қәнигелиги бойынша магистр академиялық дәрежесине ылайық деп есаплайман.

Илимий басшы **доц. М. Бердимуратов**

Бердақ атындағы Қарақалпақ мәмлекетлик университети магистратура бөлими 5А130202 – «Әмелий математика ҳәм информациялық технологиялар» қәнигелиги магистранты Балтабаев Жахангир Елибаевичтың магистрлик академиялық дәрежесин алыў ушын жазылған «Мағлыўматлар ағымын шифрлаўда RSA алгоритмин қолланыў» диссертациясына

СЫН

Информациялық технологиялардың тез пәт пенен раўажланып барыўы жәмийетте ҳәр қыйлы информациялық хызметлердиң пайда болыўына алып келди. Бул тараўларда мағлыўматлардың алмасыўын тәмийнлеўде қәўипсизлик мәселелери айрықша болып есапланады. Мағлыўматлардың қәўипсизлигин тәмийнлеў ҳуқықый-норматив ҳүжжетлер, техникалық қураллар ҳәм криптографиялық алгоритмлер ҳәм де протоколлар тийкарында әмелге асырылады.

Магистрлик диссертация жумысы үш баптан ибарат болып мағлыўматларды қорғаўдың асимметриялы криптосистемаларының бири болған RSA алгоритми қаралған ҳәм әмелий жақтан мысаллар исленген. Жумыстың 1-бабында криптосистемалар ҳаққында улыўма түсиниклер берилген. Классикалық шифрлаў усыллары ҳаққында айтылып, олардың анализи қаралған. Асимметриялы системалардың тийкарында жатыўшы дискрет логарифмлеў мәселеси берилген. 2-бапта RSA алгоритми қаралып, оның жәрдеминде мағлыўматларды шифрлаў ҳәм дешифрлаў этаплары көрип шығылған. Алгоритм тийкарында электрон таңбалы имзаны жаратыў усыллары қарастырылған. Үшинши бапта болса алгоритмди әмелий жақтан реализациялаў мақсетинде оның программалық тәмийнаты исленген. Жоқары басқышлы программалыстырыў тили болған C++ орталығында алгоритмди пайдаланып шифрлаў/дешифрлаў ҳәм электрон имзаны жаратыў және оны тексериў программасы ислеп шығылған.

Жуўмақлаў бөлиминде программалық тәмийнатты ислеп шығыўда жазылған программа коды берилген. Программалық тәмийнатты қолланыў ушын түсиндирмелер кем берилген ҳәм пайдаланыўшы интерфейси әпиўайы етип ислеген. Улыўма айтқанда диссертация жумысында исленген мысаллар «Информацияларды қорғаў» пәни бойынша әмелий сабақлар өтиўде пайдаланыў мүмкин.

Жоқарыда айтып өтилгенлерди есапқа алсақ, Жахангир Балтабаевтың магистрлик диссертация жумысы магистратураның 5А130202 – «Әмелий математика ҳәм информациялық технологиялар» қәнигелиги бойынша қойылған барлық талапларға толық жуўап береди ҳәм Ж. Балтабаев магистр академиялық дәрежесине ылайық деп есаплайман.

Сын бериўши: **ф.-м.и.к. Қ. Елгондиев**

Бердақ атындағы Қарақалпақ мәмлекетлик университети магистратура бөлими 5А130202 – «Әмелий математика ҳәм информациялық технологиялар» қәнигелиги магистранты Балтабаев Жахангир Елибаевичтың магистрлик академиялық дәрежесин алыў ушын жазылған «Мағлыўматлар ағмын шифрлаўда RSA алгоритмин қолланыў» диссертациясына

СЫН

Ҳәзирги ўақытта мағлыўматлардың қәўипсизлигин тәмийинлеўде ең исенимли қураллардан бири мағлыўматларды криптографиялық қорғаў усыллары есапланады. Компьютер тармақлары ҳәм электрон ҳүжжетлер алмасыў технологияларының раўажланыўы: финанс, банк иси, саўда-сатыққа уқсас тараўларда қолланылыўы информацияны қорғаўдың криптографиялық усыллары улыўма жәмийетлик искерликтиң ҳәр қыйлы тараўларына кең түрде кирип барыўына себеп болды. Ҳақыйқаттан да байланыс тармақларында информацияны қорғаўды криптографиялық усылда тәмийинлеў жәмийеттиң раўажланыў басқышлары менен байланыслы болған узақ тарийхый дереклерге ийе.

Бул магистрлик диссертация жумысында асимметриялы криптосистемалардағы RSA шифрлаў ҳәм электрон таңбалы имза алгоритми қарастырылған. Диссертация жумысы кирисиў бөлими, үш баптан, жуўмақлаў бөлиминен ҳәм пайдаланылған әдебиятлар дизиминен ибарат.

Кирисиў бөлиминде жумыстың әҳмийетлилиги айтылып, оның жәмийеттеги тутқан орны ҳаққында баян етилген. 1-бапта криптографияның тийкарғы мәселелери айтылған. Ҳәзирги ўақытта ҳәрекет етип атырған криптосистемалардың еки класына тоқтап өтип, оларды анализлеген. Асимметриялы криптосистема усылларының идеясын мысаллар жәрдеминде түсинидириўге ҳәрекет еткен ҳәм олардың тийкарында жатыўшы мәселениң түрлери бойынша классификациялаған.

Шифрлаў ҳәм электрон таңбалы имзаны жаратыў стандартлары ҳаққында мағлыўмат берген. 2-бапта болса асимметриялы криптосистемалардың бири болған RSA шифрлаў ҳәм электрон таңбалы имза алгоритмлери қаралған ҳәм оның тийкарында мысал исленген. Алгоритмди тәрийплеўде зәрүрли болған санлар теориясының айырым анықлама ҳәм теоремалары дәлиллеўсиз берилген. 3-бапта болса екинши бапта сөз етилген алгоритмлерге программалық қурал жаратыў этаплары айтылып Visual Studio орталығында айналы интерфейс жаратлыған ҳәм программаның C++ тилиндеги кодын қосымша бөлиминде келтирип өткен.

Магистрлик диссертация жумысын жазыўда RSA алгоритмине программалық тәмийнат ислеп шыққан. Жумыста айырым орфографиялық қәтелерге жол қойылған ҳәм пайдаланылған әдебиятларға силтемелер кемирек берилген. Улыўма алғанда магистрлик диссертация жумысы жақсы жазылған ҳәм оны «Информацияларды қорғаў» пәнин өзлестириўши талабалар ушын методикалық қолланба ретинде пайдаланыў мүмкин.

Магистрант Балтабаев Жахангир тәрепинен таярланған «Мағлыўматлар ағмын шифрлаўда RSA алгоритмин қолланыў» темасындағы магистрлик диссертациясы қойылған барлық талапларға жуўап береди ҳәм оның авторы 5A130202 – «Әмелий математика ҳәм информациялық технологиялар» қәнигелиги бойынша магистр академиялық дәрежесине ылайық деп есаплайман.

Сын бериўши: ф-м.и.д Н. Утеулиев

ÓZBEKSTAN RESPUBLIKASÍ JOQARÍ HÁM ORTA ARNAWLÍ BILIMLENDIRIW MINISTRLIGI

BERDAQ ATINDAǴÍ QARAQALPAQ MÁMLEKETLIK UNIVERSITETI

Fakultet: Magistratura bólimi
Kafedra: Ámeliy matematika
Oqıw jılı: 2019-2020

Magistrant: J.E.Baltabaev
Ilimiy basshı:doc.M.K.Berdimuratov
Qánigeligi: Ámeliy matematika hám informatsiyalıq texnologiyalar

MAGISTRLIK DISSERTACIYA ANNOTACIYASÍ

Magistrlik dissertaciya temasınıń tiykarlanıwı hám aktuallıǵı.

Házirgi kúnde elektron hújjetlerdi almasıwda shifrlaw, ashıq kanallarda giltlerdi almasıw hám elektron imza algoritmleri áhmiyetli másele bolıp tabıladı. Bulardı ámelge asırıwda eksponencional turaqlılıqqa iye kriptoalgoritm hám subeksponencial turaqlılıqqa iye asimmetriyalı kriptoalgoritmler qollanıladı. Asimmetriyalı kriptoalgoritmlerdiń esaplaw sistemalarında salıstırmalı túrde tómen realizaciyalanıwınıń sebebinen jeke kompьyuterler ushın arnawlı esaplaǵıshlardı jaratıw zárúrligi payda boldı. Sonlıqtan informaciyalardı qayta islewde hám olardı programmalıq túrde realizaciyalawda joqarı tezlikti támiyinlewshi asimmetriyalı kriptosistemlardı jaratıw máselesi aktual bolıp tabıladı.

Bul jumıs birinshi asimmetriyalıq shifrlaw hám elektron tańbalı imza algoritmi bolǵan RSA kriptografiyalıq sistemacın úyreniwge arnalıp, bir qansha teoriyalıq hám ámeliy máseleler islep kórsetildi.

Izertlew obiekti hám predmeti. Izertlew obiekti - RSA kriptosistemasınıń matematikalıq modeli. Izertlew predmeti - sanlardı faktorizaciyalaw máselesine tikarlanǵan shifrlaw algoritmi.

Izertlewdiń maqseti hám wazıypaları. Bul magistrlik dissertaciya jumısın orınlawda kriptografiyalıq algoritmlerdmi izertlew, asimmetriyalı krpitosistemalardaǵ RSA shifrlaw hám elektron tańbalı imza algoritmin analizlew hám olardıń tiykarında programmalıq ónim islep shıǵıw.

Magistrlik dissertaciya jumısın orınlawda tómendegishe wazıypalar qoyıldı

- Sanlar teoriyasındaǵı tiykarǵı túsiniklerdi úyrenip shıǵıw hám olardı kriptogrfiyalıq maqsette qollanıw jolların anıqlaw.
- Sanlardı faktoriyazaciyalaw máselesine mısallar kórip onı analiz etiw.
- RSA algoritmi tiykarında maǵlıwmatlardı shifrlaw hám elektron imza algoritmnen úyreniw hám ónim islep shıǵıw

Izertlewdiń ilimiy jańalıǵı. Bul magistrlik dissertaciyasınıń nátiyjesinde RSA kriptosistemasınıń matematikalıq modeli tolıq uyreniledi hám maǵlıwmatlardı shifrlaw algoritmine programma dúzildi.

Máseleniń izertleniw dárejesi. Algoritmniń tiykarında sanlardı ápiwayı kóbeytiwshilerge jiklew máselesi jatadı. Bul oblasta tiykarınan D. Pollard, A. Lenstra, D , P Shoralardıń izertlew jumısları úlken áhmiyetke iye. Sanlar teoriyasındaǵı esaplawlar hám úlken sanlardı faktorizaciyalaw máselesin izzertlewshilerdi xoshametlew ushın 1991-jılı mart ayında RSA Laboratories iniciativası menen RSA Factoring Challenge konkursı járiyalandı. Konkursta usınılǵan sanlardıń ápiwayı kóbeytiwshilerin tabıw máselesi qoyıldı. Konkurs 2007-jılı juwmaqlanǵan bolsa da, qızıǵıwshılar házirgi waqıtqa shekem sol sanlardı kóbeytiwshilerge jiklew menen shuǵıllanbaqta. 2020-jıldaǵı maǵlıwmat boyınsha usınılǵan 54 sannıń ishinen 22 sanı ǵana jiklengen.

Izertlewdiń alıp barıw usılları. Visual studio ortalıǵınan paydalanıp asimmetriyalı kriptosistemalardı úyrenip RSA shifrlaw hám elektron tańbalı imza algorimine programma jaratıw.

Izertlewdiń ámeliy áhmiyeti hám ilimiy nátiyjelerdiń aprobaciyası. Dissertaciya jumısın orınlaw barısında alınǵan tiykarǵı nátiyjeler boyınsha programmalıq ónim islep shıǵıldı. Magistrlik dissertaciya jumısı boyınsha eki maqala baspadan shıqtı. Dissertaciya jumısı boyınsha islep shıǵılǵan programmalıq támiynattı informaciyalardı qorǵaw pániniń ámeliy jumıslarında máseleler sheshiw ushın paydalanıwǵa boladı.

Jumıstıń dúzilisi hám kólemi. Magistrlıq dissertaciya jumısı kirisiw bólimi, úsh bap, juwmaqlaw, paydanılǵan ádedibyatlar dizimi, hám qosımsha bólimlerinen ibarat hám kólemi 60 bet.

Ilimiy basshı: M.K.Berdimuratov

Magistrant: J.E.Baltabaev

ÓZBEKSTAN RESPUBLIKASÍ JOQARÍ HÁM ORTA ARNAWLÍ BILIMLENDIRIW MINISTRLIGI

BERDAQ ATINDAǴÍ QARAQALPAQ MÁMLEKETLIK UNIVERSITETI

Qol jazba huqıqı

UDK: 004.9

Baltabaev Jahangir Elibaevichtiń

Maǵlıwmatlar aǵımın shifrlawda RSA algoritmin qollanıw temasında

5A130202 – Ámeliy matematika hám informaciyalıq texnologiyalar

Magistr akademiyalıq dárejesin alıw ushın jazılǵan
DISSERTACIYA

MAK da jaqlawǵa ruxsat
Magistratura bólimi baslıǵı: **doc. A.Gulimov**

Kafedra baslıǵı: **doc. D.Utebaev**
Ilimiy basshı: **doc. M.Berdimuratov**

Nókis – 2020

MAZMUNI

KIRISIW

Házirgi waqıtta informaciyalardı qorǵaw qurallarına hám usıllarına bolǵan talap asıp barmaqta. Bul bolsa mámleketimizdegi elektron húJjet aylanısınıń artıwı menen tıǵız baylanısqan. Elektron tańbalı imzaǵa bolǵan itibar artpaqta. Autentifikaciyalaw sistemalarınıń isenimliligin arttırıw maqsetinde algebra hám algebralıq geometriya usıllarınıń eń sońǵı nátiyjeleri qollanıladı.

Bul magistrlik dissertaciya jumısında maǵlıwmatlardı shiflawdıń asimmetriyalı algoritmi haqqında tiykarǵı túsinikler berilip, onıń tiykarında jatırǵan RSA algoritm járdeminde maǵlıwmatlardı shifrlaw hám hám elektron tańbalı imzanı jaratıw qaraladı.

Dissertaciya temasınıń aktuallıǵı: Jámiyettiń turaqlı túrde informatizaciyalastırıwdıń ósiwi hám informaciya bahasınıń asıwı maǵlıwmatlardı qorǵaw quralların hám usılların elede jetilistiriw zárúrligin tuwdırdı. Qorǵalıp atırǵan informaciyalıq sistemaǵa bir qatar talaplar qoyıldı. Mısalı, konfedenciallıqtı támiyinlew, huqıqlardı shegaralaw, maǵlıǵlıwmatlardıń pútinligi hám haqıyqıylıǵı, paydalanıwshını identifikaciyalaw h.t.b. Bul talaplar sistemanı paydalanıwda sistemanı buzıwshınıń xáreketleri berilgen model ushın anıq bar shártlerde orınlanıwı kerek. Informaciyalıq sistemanıń qorǵanǵanlıǵı onıń qanday da bir qorǵanıw sapasına tásir etiwshi eń jaqsı algoritm menen ólshenedi.

Qaǵıyda boyınsha joqarıda kórsetilgen funkciyalar kriptografiyalıq qurallar járdeminde ámelge asırıladı. Egerde jaqın aralıqqa shekem kriptografiya kópshilik ushın belgisiz bolıp kelgen bolsa, búgin yamas jaqın arada onıń menen hár kim dus keliwi múmkin. Bir qatar mámleketlerde elektron saylaw hám elektron aqsha sistemaların jaratıw boyınsha bir qansha jumıslar alıp barılmaqta. Ózbekistan respublikasında da bul másele aktul másele esaplanadı. Mámleketimizde 2003-jılı “Elektron tańbalı imza haqqında”, 2004-jılı “Elektron húJjet aylanısı haqqında”, 2005-jılı “Elektron tólemler haqqında”, 2007-jılı “Informaciyalardı kriptografiyalıq qorǵawdı shólkemlestiriw ilajları haqqında” qabıl etilgen nızam hám qararları buǵan ayqın mısal boladı.

Házirgi kúnde elektron hújjetlerdi almasıwda shifrlaw, ashıq kanallarda giltlerdi almasıw hám elektron imza algoritmleri áhmiyetli másele bolıp tabıladı. Bulardı ámelge asırıwda eksponencional turaqlılıqqa iye kriptoalgoritm hám subeksponencial turaqlılıqqa iye asimmetriyalı kriptoalgoritmler qollanıladı. Asimmetriyalı kriptoalgoritmlerdiń esaplaw sistemalarında salıstırmalı túrde tómen realizaciyalanıwınıń sebebinen jeke kompьyuterler ushın arnawlı esaplaǵıshlardı jaratıw zárúrligi payda boldı. Sonlıqtan informaciyalardı qayta islewde hám olardı programmalıq túrde realizaciyalawda joqarı tezlikti támiyinlewshi asimmetriyalı kriptosistemlardı jaratıw máselesi aktual bolıp tabıladı.

Bul jumıs birinshi asimmetriyalıq shifrlaw hám elektron tańbalı imza algoritmi bolǵan RSA kriptografiyalıq sistemacın úyreniwge arnalıp, bir qansha teoriyalıq hám ámeliy máseleler islep kórsetildi.

Máseleniń izertleniw dárejesi. Algoritmniń tiykarında sanlardı ápiwayı kóbeytiwshilerge jiklew máselesi jatadı. Bul oblasta tiykarınan D. Pollard, A. Lenstra, D , P Shoralardıń izertlew jumısları úlken áhmiyetke iye. Sanlar teoriyasındaǵı esaplawlar hám úlken sanlardı faktorizaciyalaw máselesin izzertlewshilerdi xoshametlew ushın 1991-jılı mart ayında RSA Laboratories iniciativası menen RSA Factoring Challenge konkursı járiyalandı. Konkursta usınılǵan sanlardıń ápiwayı kóbeytiwshilerin tabıw máselesi qoyıldı. Konkurs 2007-jılı juwmaqlanǵan bolsa da, qızıǵıwshılar házirgi waqıtqa shekem sol sanlardı kóbeytiwshilerge jiklew menen shuǵıllanbaqta. 2020-jıldaǵı maǵlıwmat boyınsha usınılǵan 54 sannıń ishinen 22 sanı ǵana jiklengen.

Izertlew obekti hám predmeti. Izertlew obekti - RSA kriptosistemasınıń matematikalıq modeli. Izertlew predmeti - sanlardı faktorizaciyalaw máselesine tikarlanǵan shifrlaw algoritmi.

Izertlewdiń maqseti hám wazıypaları. Bul magistrlik dissertaciya jumısın orınlawda kriptografiyalıq algoritmlerdmi izertlew, asimmetriyalı krpitosistemalardaǵ RSA shifrlaw hám elektron tańbalı imza algoritmin analizlew hám olardıń tiykarında programmalıq ónim islep shıǵıw.

Magistrlik dissertaciya jumısın orınlawda tómendegishe wazıypalar qoyıldı

- Sanlar teoriyasındağı tiykarǵı túsiniklerdi úyrenip shıǵıw hám olardı kriptogrfiyalıq maqsette qollanıw jolların anıqlaw.
- Sanlardı faktoriyazaciyalaw máselesine mısallar kórip onı analiz etiw.
- RSA algoritmi tiykarında maǵlıwmatlardı shifrlaw hám elektron imza algoritmnen úyreniw hám ónim islep shıǵıw

Izertlewdiń alıp barıw usılları. Visual studio ortalığınan paydalanıp asimmetriyalı kriptosistemalardı úyrenip RSA shifrlaw hám elektron tańbalı imza algorimine programma jaratıw.

Izertlewdiń ilimiy jańalığı. Bul magistrlik dissertaciyasınıń nátiyjesinde RSA kriptosistemasınıń matematikalıq modeli tolıq uyreniledi hám maǵlıwmatlardı shifrlaw algoritmine programma dúzildi.

Izertlewdiń ámeliy áhmiyeti hám ilimiy nátiyjelerdiń aprobaciyası. Dissertaciya jumısın orınlaw barısında alınǵan tiykarǵı nátiyjeler boyınsha programmalıq ónim islep shıǵıldı. Magistrlik dissertaciya jumısı boyınsha eki maqala baspadan shıqtı. Dissertaciya jumısı boyınsha islep shıǵılǵan programmalıq támiynattı informaciyalardı qorǵaw pániniń ámeliy jumıslarında máseleler sheshiw ushın paydalanıwǵa boladı.

Jumıstıń dúzilisi hám kólemi. Magistrlıq dissertaciya jumısı kirisiw bólimi, úsh bap, juwmaqlaw, paydanılǵan ádedibyatlar dizimi, hám qosımsha bólimlerinen ibarat hám kólemi 60 bet.

I BAP. KRIPTOGRAFIYALIQ SISTEMALAR

1-§. Kriptografiyanıń tiykarǵı maseleleri

Informaciyalardı qorǵaw mashqalaları adamzattı bir neshe waqıtlardan baslap táshwishke salıp kelmekte. Informaciyanı qorǵaw zárúrligi áskeriy hám diplomatiyalıq xabarlardı jasırın uzatıw talabınan kelip shıqtı. Máselen, antikalıq dáwirdegi spartakshılar ózleriniń áskeriy xabarların shifrlaǵan, qıtaylılarda xabardıń ieroglifler járdeminde ápiwayı jazılıwı, onı basqa mámleketler ushın sırlı etip qoyǵan.

Kriptografiya mıń jıldan aslam tariyxı dawamında, shifrlaw hám shifrdan ashıwdıń qatań sır saqlanıwshı, turaqlı jańalanıp hám jetilistirilip barıwshı texnikalıq usıllar jıyındısı bolıp kelmekte.

Kriptologiyanıń áyyem zamanlardan baslap XX-ásirdiń ortalarına shekemgi rawajlanıw dáwirin ilimge shekemgi kriptologiya erası dep ataw qabıl etilgen. Sebebi sol waqıtqa shekemgi jetiskenlikler intuiciyaǵa tiykarlanǵan bolıp, dálillewler menen bekkemlenbegen edi. Ol waqıtlarda kriptologiya menen ilim sıpatında emes, al tek ǵana iskusstvo sıpatında shuǵıllanǵan. Álbette, kriptologiya táriyxı sol waqıtlarda hesh qanday qızıǵıwshılıq oyatpadı degendi bildirmeydi. Bunnan 2000 jıllardan aldın Yuliy Cezar hám Ciceronlar ózinińRimdegi doslarına shifrdı paydalanıp xatlar jazǵan. Tek ǵana ekinshi dúnya júzlik urıstıń baslanıwı menen áskeriy derjavalardıń kriptologiyalıq xızmetleri, kriptologiyanıń rawajlanıwına matematikler úlken úles qosıwı múmkin ekenligin túsinip jetti.

Kriptográfiya (áyyemgi grek. κρυπτός — jasırın hám γράφω — jazıw) — bul informaciyanıń konfidenciallıǵı (informaciyanıń basqa shaxslar tárepinen oqılmawı) hám durıslıǵın (pútinlik hám avtordıń haqıyqıylıǵı, sonday-aq avtorlıqtan waz keshe almawı) támiynlew usılları haqqındaǵı ilim.

Kriptoanaliz — shifrlanǵan informaciyanı onıń giltin bilmey turıp shifrdan ashıw, onı deshifrlaw usılları haqqındaǵı ilim.

Gilt — kriptografiyalıq algoritmde maǵlıwmatlardı shifrlawda (deshifrlawda) qollanılatuǵın sırlı informaciya.

Kriptoanaliz usıllarınan paydalanıp shifrdı ashıwǵa urınıwdı bul shifrǵa jasalǵan kriptografiyalıq húJim dep ataydı.

Kriptoanaliz hám kriptografiyanı biriktiretuǵın ilim tarawı kriptologiya dep atalaıp, ol grekshede «kripto» — sırlı hám «logus» — so'z degen mánisti ańlatadı.

Kriptografiyanıń wazıypası xabarlardıń sırlılıǵın hám haqıyqıylıǵın támiynlewden ibarat bolsa, kriptoanalizdiń wazıypası kriptograflar tárepinen islep shıǵılǵan qorǵanıw sistemasın buzıwdan ibarat.

Házirgi waqıtta kompyuterler menen basqarılatuǵın keń tarqalǵan baylanıs tarmaǵın xalıq xızmetinde paydalanıwda, maǵlıwmatlardıń kriptografiyalıq qurallar menen arnawlı qorǵalıwın talap etedi. Bunıń ushın kriptologiya ilimine sanlar teoriyası hám algebra elementleri kiritilgen bolıp, bunday matematikalastırıw tek ǵana kriptologiya tarawı qánigelerin emes, al dáslep kriptologiyadan uzaqta bolǵan birneshe matematiklerdi de qızıqtırıp qoydı. Zamanagóy kriptografiya matematika hám informatikanıń shegarasında bólek ilimiy baǵdardı dúzedi hámde matematikanıń (sanlar teoriyası, sızıqlı algebra hám algebralıq strukturalar) ayırım ayrıqsha oblastlarına tiykarlanadı.

Ulıwma aytqanda, házirgi kriptosistemalar tiykarında sanlar teoriyasına tiykarlanǵan quramalı matematikalıq mashqalalar (úlken sandı ápiwayı kóbeytiwshilerge jiklew, sanlardı ápiwayılıqqa tekseriw, sanlardı qaldıqlı bóliw, pútin bóliw, modulli arifmetikada dárejege kóteriw hám t.b.) jasırınǵan bolıp, bul máselelerdi sheshiw kriptografiyanıń aktual mashqalalarınan esaplanadı.

Kriptografiya informaciyanı ruxsatsız kiriwden qorǵap, onıń sırlılıǵın támiynleydi. Ulıwma aytqanda kompyuter tarmaǵına ruxsatsız kiriwdiń tolıq aldın alıw múmkin emes, biraq olardı anıqlaw múmkin. Informaciyanıń pútinligin tekseriwdiń bunday procesi, kóp jaǵdaylarda informaciyanıń haqıyqıylıǵın támiynlew delinedi.

Házirgi zaman kriptografiyasi tómendegi tort bólimdi óz ishine aladı:

- Simmetriyalı, bir giltli (sırlı giltli);
- Asimmetriyalı, eki giltli (ashıq giltli);
- Elektron tańbalı imza;
- Giltlerdi generaciyalaw hám olardı bo'listiriw.

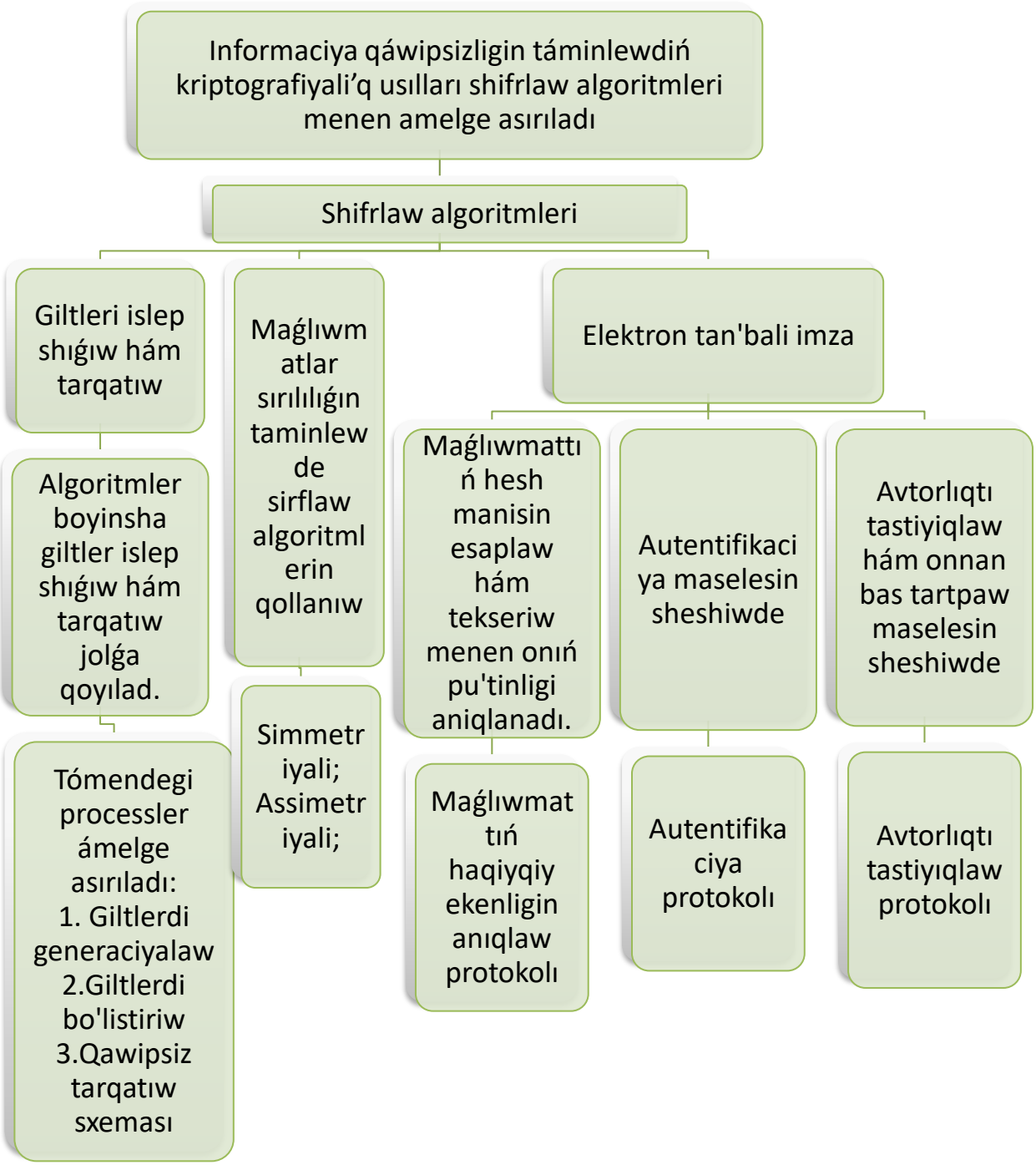
Kriptografiyalıq usıllardan paydalanıwdıń tiykarǵı baǵdarı: jasırın maǵlıwmatlardı ashıq baylanıs kanalı boyınsha qorǵalǵan túrde jo'netiw, olardıń haqiyqıylıǵın táminlew, informaciyalardı (elektron hújjetlerdi, elektron maǵlıwmatlar jıynaǵin) kompyuter sisteması yadında shifrlanǵan túrde saqlaw hám usı siyaqlı maseleler sheshimin óz ishine aladı.

Informaciyalıq sistemalardıń qáwipsizliginiń zamanagóy kriptografiyalıq usıllarına tómendegi ulıwma talaplar qóyıladı :

- shifrlangan maǵlıwmattıń túp nusqasına iyelik etiw múmkinshiligi tek deshifrlaw gilti belgili bolǵanda ǵana múmkin bolsın;
- paydalanılgan shifrlaw giltin shifrteksttiń qandayda bir anıq bólegi boyınsha yamasa oǵan sáykes keliwshi ashıq bólegi boyınsha anıqlaw ushın orınlanıwı zárúr bolǵan ámeller sanı - giltti anıq tabıw ushın orınlanıwı kerek bolǵan barlıq ámeller sanınan kem bolmawı kerek, yaǵnıy gilt tańlap alınıwı kerek bolǵan ko'plik elementleriniń sanınan kem bolmawı kerek;
- shifrlaw algoritmınıń ashıqlıǵı onıń turaqlılıǵına keri tásir etpewi kerek;
- gilttiń hár qanday dárejedegi ózgeriwleri shifrlanǵan maǵlıwmattıń sezilerli túrde ózgeriwine alıp keliwi kerek;
- shifrlaw algoritmı quramındaǵı elementler turaqlı bolıwı kerek;
- shifrlaw processi dawamında maǵlıwmatlarǵa kiritiletuǵın qosımsha bitler (elementler) shifrlanǵan tekstte (maǵlıwmatta) tolıq hám isenimli túrde jasırınǵan bolıwı kerek;
- shifrlanǵan teksttiń uzıńıǵı baslanǵish teksttiń uzıńıǵına teń bolıw kerek;

- shifrlaw processinde izbe-iz qollanılatuǵın giltler arasında ápiwayı hám ańsatlıq penen ornatılatuǵın baylanıslar bolmawı kerek;
- giltlerdiń mumkin bolǵan ko'pliginen alınǵan qálegen gilt informaciyanıń isenimli qorgálıwın támiyinlewi kerek;
- kriptoalgoritm programmalıq hámde texnikalıq jaqtan qollanıwǵa qolaylı bolıp, gilttiń uzınlıǵınıń ózgeriwi shifrlaw algoritmınıń sapasına tásir etpewi kerek.

Maǵlıwmatlardı qorǵawdı kriptografiyaliq usıllar menen támiyinlew qurallarının' tiykarın shifrlaw algoritmleri quraydı (1.1-súwret)



1.1-súwret

Shifrlaw algoritmleri sırlı parametrlerge tiykarlanǵan - simmetriyalı giltli hám qollanıw protokolı menen anıqlanıwshı, sırlı hámde ashıq parametrlerge tiykarlanǵan - asimmetriyalı shifirlaw kriptoalgoritmlerinen ibarat.

Informaciyalıq-kommunikaciya tarmaqlarında informaciya qáwipsizligin támiyinlewdiń kriptografiyaliq quralları: kriptografiyaliq algoritmlerdıń

programmalıq támiynatı hám apparatlı-programmalıq qurallardan ibarat boladı. Salıstırmalı túrde ápiwayı, biraq kriptoturaqlı bolǵan algoritmlerdiń apparatli-texnikalıq qurılmaları nátiyjeli qollanıladı.

K.Shennonnıń 1949-jılǵı "Sırlı sistemalarda baylanıs teoriyası" atlı publikaciyası jasırın giltli ilimiy kriptologiyanıń jańa erasınıń baslanıwına tiykar boldı. Óziniń bul ájayıp jumısında kriptografiyanı informaciya teoriyası menen baylanıstırdı.

K. Shennon tárepinen jaratılǵan bunday túrdegi jańalıq, álbette, onıń elektrotexnika hám matematika boyınsha teren' bilimleri hám bunnan bir jıl aldın ol jaratqan informaciya teoriyası páni sebepli júzege kelgen edi. Ol tek ǵana Vernamnın' tosınanlı shifrın buzıw múmkin emesligin jánede qorǵalǵan kanal arqalı uzatılatuǵın jasırın gilt o'lsheminin' (bitler sanın) shegaraların da anıq kórsetip berdi. Ol shegaralanbaǵan resurslarǵa iye bolǵan kriptotanalitik qandayda bir «tosınanlı shifr»dı ashıwında jasırın giltti tabıwı ushın zárúr bolǵan shifrlanǵan teksttegi simvollar sanı S tómendegishe ańlatatuǵınlıgın kórsetdi:

$$S = \frac{H(k)}{r \log n}$$

bul jerde: $H(k)$ – gilt entropiyası, yaǵniy gilttiń harbir simvolına sáykes keletuǵın informaciya muǵdarı, r – maǵlıwmattı saqlaw hám jo'netiwde qollanılatuǵn informaciya o'lsheminin' asıp ketiw parametri, n – alfavit o'lshemi.

Keltirilgen ańlatpa ulıwma jaǵdayda tastıyıqlanbaǵan bolsada ayırım jaǵdaylar ushın orınlı boladı. Bunnan tómendegishe juwmaq kelip shıǵadı: kriptoanalitiktın' jumısın tek ǵana kriptosistemanı tolıq jetilistiriw arqalı emes, al shifrlanatuǵın teksttegi r di nolge shekem kemeytiw arqalıda quramalastırıw múmkin. Demek, shifrlawdan aldın informaciyanı statistikalıq kodlaw (tıǵızlastırıw, arxivlew) kerek. Bunda informaciyanıń kólemi hám informaciyanın' artıwı (r) azayadı, entropiyası bolsa o'sedi. Sebebi, ıqshamlasqan tekstte tákrarlanıwshı sózler hám háripler azayıp shifrdı buzip ashıw qıyınlasadı.

Házirgi zaman kriptografiyasında simmetriyalı bloklı shifrlaw algoritmleri óziniń keń qollanılıwı menen ajralıp turadı. Bunday kriptografiyaliq sistemalarda giltti uzatıw mashqalası bar bolsada, shifrlawdağı tezligi hám isenimligi menen úlken kólemdegi maǵlıwmatlardı shifrlaw imkaniyatın beredi.

Uzatılatuǵın informaciyanıń mazmunın jasırıw ushın eki túrli ózgertiwler qollanadı: kodlaw hám shifrlaw.

Kodlaw ushın tez-tez isletiletuǵın simvollar kópligin óz ishine alıwshı kitap yaki tablicalardan paydalanadı. Bul simvollardıń hár birine kópshilik jaǵdaylarda cifralar kópligi menen beriletuǵın qálegen tańlanǵan kodlı sóz sa'ykes keledi. Informaciyanı kodlaw ushın mine usınday kitap yaki tablica talap etiledi. Kodlastırıwshı kitap yaki tablica qálegen kriptografiyalıq ózgertiwge mısal boladı. Kodlastırıwdıń informaciyalıq texnologiyasına sáykes talaplar, bul - qatarlı maǵlıwmatlardı sanlı maǵlıwmatlarǵa aylandırıw hám keri ámeldi orınlay alıwı. Kodlaw kitabın tez hám sırtqı yad qurılmalarında ámelge asırıw múmkin, lekin bunday tez hám isenimli kriptografiyalıq sistemanı áwmetli dep esaplawǵa bolmaydı. Eger bul kitaptan bir márte ruxsatsız paydalanılsa, onda kodlardıń jańa kitabın jaratıw hám onı hámme paydalanıwshılarǵa tarqatıw zárúrligi payda boladı.

Kriptografiyalıq ózgertiwlerdiń ekinshi túri shifrlaw óz ishine baslanǵısh tekst belgilerin ańlap alıw múmkin bolmaǵan formaǵa ózgertiw algoritmlerin qamtıp aladı. Bul jerde algoritmdi qorǵaw áhmiyetli orın tutadı. Kriptografiyalıq giltti qollap, shifrlaw algoritminiń ózinde qorǵawǵa bolǵan talaplardı kemeytiw múmkin. Endi qorǵaw obekti sıpatında tek ǵana gilt xızmet etedi. Eger giltten nusqa alınatuǵın bolsa, onda onı almastırıw múmkin hám bul kodlastırıwshı kitap yaki tablicanı almastırıwdan jeńil. Sonıń ushında kodlaw emes, al shifrlaw informaciyalıq-kommunikaciyalıq texnologiyalarda keń kólemde qollanbaqta.

Kriptografiyalıq sistemalar eki klasqa bólinedi:

- simmetriyalı (jasırın giltli, bir giltli)
- asimmetriyalı (ashıq giltli, eki giltli)

Simmetriyalı kriptosistemalardıń ilimiy teoriyasının' jaratılıwına hám ámeliy rawajlanıwına K. Shennon, O. Kerxgoff, Sh. Bebbij, Ol. Fridman, G. Vernam, E. Xebern hám basqalar úlken úles qostı.

2-§. Simmetriyalı kriptosistemalar

Kriptografiyalıq kóz-qarastan shifrlaw algoritmi – bul ashıq tekstti qanday da bir sırlı gilt járdeminde shifrlanǵan tekstke aylandırıw bolıp tabıladı. Bul process shifrlaw dep ataladı.

Shifrlaw processi tómendegishe teńleme arqalı ańlatıladı:

(1.1)

$$C = E_k(P)$$

bunda P - ashıq tekst, E - shifrlawshı funkciya, k - sırlı gilt, C - shifrlanǵan tekst. Keri processti deshifrlaw dep atap ol

$$P = D_k(C) \qquad (1.2)$$

formulası menen ańlatıladı, bunda D - deshifrlaw funkciyası. Bul processte shifrlawshı hám deshifrlawshı algoritmler hámmege málim bolıp, berilgen P tekstiniń qupıyalılıǵı onı shifrlawda qollanılıp atırǵan k giltiniń sır saqlanıwınan ǵárezli boladı. Processtiń eki tárepinde de bir gilt qollanılıp atırǵanlıǵı ushın bul algoritmdi biz simmetriyalı kriptosistema yamasa sırlı giltli kriptosistemalar dep ataymız.

Eń dáslepki kriptosistemalardan biri bolǵan orın almastırıw shifrında dáslepki berilgen tekst simvolları sol teksttiń belgili bir bólekleri menen arnawlı qaǵıydalar járdeminde orınları almastırıladı.

Bul usıl eń dáslep payda bolǵan bolıp tariyxta onı Yuliy Cezar qollanǵan degen maǵlıwmatlar bar. Sonlıqtan onı Cezar shifrı dep ataydı.

Dáslep maǵlıwmatlardı jazıwda qollanılatuǵın alfavit simvolların sanlar menen belgileymiz. Meyli latın alfaviti ushın $A-Z$ háriplerdi sáykes $0-25$ ke shekemgi sanlar menen belgileyik. Bunnan soń shifrlanıw kerek bolǵan maǵlıwmattaǵı háriplerdi sanlarǵa ózgertip, sanlar izbe-izligine iye bolamız. Shifrlawda qollanatuǵın k giltimiz pútin sandı ańlatıp, ol tekstte orın almasıw

poziciyasına teń boladı, yaǵnıy k nı teksttegi simvollardıń san mánisine 26 moduli boyınsha qosıp shıǵıw kerek. Bul jerde giltler sanı 25 ke teń 0 teksttiń mazmunın ózgertpeydi), sonlıqtan onı tabıw úlken qıyınshılıq tuwdırmaydı. Bul shifrdı buzıwda jiyilik analizi úlken áhmiyetke iye.

Orın almastırıw usılınan ózgeshe usıl bul almastırıw shifrı bolıp, onıń ózgesheligi berilgen teksttiń simvolları paydalanılıp atırǵan yamasa basqa bir alfavittiń simvolları menen almastırıladı.

Bul usılda gilt jaratıwda dáslep alfavit tártip boyınsha jazıladı, al onnan soń sol alfavit orınları ózgertilip berilgen alfavit astına qayta jazıp shıǵıladı. Mısalı

1.1- tablica

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
G	O	Y	D	S	I	P	E	L	U	A	V	C	R	J	W	X	Z	N	H	B	Q	F	T	M	K

Bunday etip jazıw ashıq tekst simvolları shifrlaw processinde qanday simvollar menen almasıwı kerek ekenligin ańlatadı, yaǵnıy hár bir simvol tómengi qatardıń sáykes simvolı menen almasadı. Mısalı *hello* sózin shifrlaǵanda ol *ESVVJ* túrinde boladı.

Bul usılda múmkin bolǵan giltlerdiń sanı

$$26! \approx 4,03 * 10^{26} \approx 2^{88}.$$

Sonlıqtan biz zamanagóy hám tezligi joqarı bolǵan kompyuter járdeminde bul giltlerdi teremen degenshe konkret xabardı deshifrlaw máselesi aktual emes bolıp qaladı. Biraqta shifrlawda qollanılıp atırǵan tildiń statistikasına súyene otırıp bul shifrdı da buzıw múmkin.

Egerde biz orın almastırıw shifrın aǵımlı shifr dep esaplasaq, onda almastırıw shifrı zamanagóy bloklı shifrǵa uqsas boladı. Onda blok bir inglis tiliniń háribinen turadı. Shifrotekst blokı ashıq tekstke bazı bir giltti qollanıw nátiyjesinde alınadı.

Orın almastırıw hám almastırıw shifrlarınıń tiykarǵı kemshiligi: olarda ashıq teksttiń hár bir háribi barlıq waqıtta fiksirlengen bir simvolǵa almastırıladı.

Sonlıqtan bunday shifrdı buzıwda qollanılıp atırǵan tildiń statistikası úlken rol oynaydı.

Almastırıw shifrı monoalfavitli almastırıw shifrına tiyisli boladı. Onda standart alfavitti almastırıwshı tek ǵana bir tártiplengen simvollar jıynaǵı qollanıladı. Bunday kemshilikti saplastırıw maqsetinde standart alfavit ornına bir neshe tártiplengen simvollar jıynaǵın qollanıp, ashıq teksttiń háribin anıq bir izbe-izlik boyınsha hár qıylı jıyın simvolları menen almastırıw jumısın orınlaw kerek. Bunday túrdegi shifrlar polialfavitli almastırıw shifrları dep ataladı.

Mısalı,

1.2-tablica

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
T	M	K	G	O	Y	D	S	I	P	E	L	U	A	V	C	R	J	W	X	Z	N	H	B	Q	F
D	C	B	A	H	G	F	E	M	L	K	J	I	Z	Y	X	W	V	U	T	S	R	Q	P	O	N

Bul jerde birinshi qatarda inglis tili alfaviti, al ekinshi hám úshinshi qatarlar bolsa shifroteksttiń 1-shi hám 2-shi alfavitleri boladı. Bul jaǵdayda ashıq teksttiń taq poziciyadaǵı háripleri 1-shi, al jup poziciyadaǵı háripleri bolsa 2-shi qatar háripleri menen almastırıladı. Sonda *hello* sózi endi *SHLJV* túrinde shifrlanadı. Itibarǵa alatuǵın bolsaq: ashıq tekstte 2 márte ushırasıtuǵın bir háribi hár qıylı eki simvol menen almastı. Bunıń járdeminde biz shifrǵa statistikalıq usıllardı qollanıp húјim jasawdı qıyınlastırdıq.

Bul qaralǵan mısalda bir waqıtta eki háripti shifrladıq, al bul bolsa bloklı shifrlawdı ańlatadı. Ámeliyatta giltler keńisligin keńeytiriw ushın shifroteksttiń 5 ke shekemgi hár qıylı alfavitlerin qollanıw múmkin. Haqıyqattan da, egerde biz simvollardı bes almastırıwshı jıyınlardan alsaq, onda múmkin bolǵan giltler sanı $(26!)^5 \approx 2^{441}$ ge teń. Bul jaǵdayda gilt $26*5=130$ háripler izbe-izliginen turatuǵınlıǵın umıtpawı kerek. Al onı eslep qalıw paydalanıwshı ushın úlken qıyınshılıq tuwdırdı. Giltti eslep qalıw qıyın bolmaǵan polialfavitli almastırıw shifrınıń bir túri Vijner shifrı bolıp tabıladı.

Bloklı shifrlawǵa uqsas Vijner algoritminde almastırıwshı jıynlar kópligi standart alfavittiń 26 cikllik orın almasıwlar menen sheklengen. Egerde, mısalı onda 5 almastırıwshı alfavit qollanılsa, onda giltler keńisligi $26^5 \approx 22^3$ shamasınan ibarat bolıwı, al gilt sıpatında $0-25$ aralıǵındaǵı 5 sandı eslep qalıw múmkin.

Shifrlawda sırlı gilt - qayta-qayta tákraralanıp giltler aǵımın payda etiwshi qısqa háripler (lozung) izbe-izligi boladı. Mısalı, egerde gilt $sesame$ sózi bolsa, onda

t	h	i	s	i	s	a	t	e	s	t	m	e	S	s	A	g	e
									+								
s	e	s	a	m	e	s	e	s	a	m	e	s	E	s	A	m	e
									=								
L	L	A	S	U	W	S	X	W	S	F	Q	W	W	K	A	S	I

Bul jerde ashıq teksttegi a háribi qay jerde turıwınan ǵárezsiz hár qıylı háripler menen almasadı.

Vijner shifrında gilt sóziniń uzınlıǵı anıqlanǵannan soń, shifrlawda paydalanıp atırǵan tildiń statistikasına tiykarlanıp onı buzıw qıyınshılıq tuwdırmaydı.

Endi joqarıda qaralǵan orın almastırıw usılınıń bazı bir jetilistirlgen túrlerin matematikalıq formulalar járdeminde ańlatıp, ámeliyatta paydalanıwdı qarastıramız. Dáslep onıń ushın ashıq hám shifrlanǵan tekst elementar xabarlarǵa ajıratıladı. Element sıpatında bir hárip, jup hárip, úsh hárip yamasa 50 háripten turatuǵın pútin bir blok bolıwı múmkin. Shifrlawshı túrlendiriw funkciya bolıp tabıladı, ol ashıq tekst elementlerin shifrlanǵan tekst elemntlerine túrlendiredi. Basqasha etip aytqanda, ashıq teksttiń elemntler kópligi P nı shifrlanǵan tekst elementler kópligi C ǵa sáwlelendiriwshi f sáwlelendiriwi boladı. Barlıq waqıtta bul sáwlelendiriw bir mánisli dep qabıl etemiz, yaǵnıy shifrlanǵan teksttiń bir elementi ushın ashıq teksttiń tek ǵana bir elementi bar boladı. Deshifrlawshı sáwlelendiriw keri baǵıtta bolıp, ol shifrlanǵan tekst

boyınsha ashıq tekstti tiklewshi f^{-1} funkciyasına aytıladı. Bunıń sxeması qısqasha

$$P^f \rightarrow C^{f^{-1}} \rightarrow P$$

túrinde boladı. Bunday túrdegi qálegen konstrukciya kriptosistema dep ataladı.

Ótken dáwirdegi kriptografiyanıń mánisi – xabardı jasırın giltti paydalanıp shifrlaw hám shifrdan ashıwdan - ibarat bolǵan bolsa, házirgi kúnde ol úsh hár qıylı mexanizmniń jıynaǵı menen anıqlanadı.

Simmetriyalı giltli kriptografiyada tiykarǵı hám shifrlanǵan tekstler simvollar kombinaciyası bolıp esaplanadı. Bunda shifrlaw hám shifrdan ashıw - simvollardı qayta orın almastırıw yamasa bir simvoldı basqası menen almastırıw bolıp esaplanadı.

Kópshilik ellerde milliy shifrlaw standartları qabıl etilgen. AQSh ta DES (Data Encryption Standart), AES simmetriyalı shifrlaw standartları qabıl etildi. Rossiya Federaciyasında 256 bit gilt uzınlıǵına iye bloklı shifrlaw algoritmi ГОСТ 28147 – 89 standartı, sonday-aq ГОСТ Р 34.10 – 2001 elektron imza algoritmi hárekette. Biziń respublikamızda maǵlıwmatlardı shifrlawdıń O'z Dst 1105:2009 hám elektron imza standartı bolǵan O'z Dst 1092:2009 qabıl etilgen.

DES (Data Encryption Standart) 1978-jılı Amerika milliy standartlastırıw institutı (American National Standarts Institute, ANSI) tárepinen qabıl etilip, ol maǵlıwmatlardı shifrlaw algoritmi (Data Encryption Algorithm, DEA) dep ataldı.

DES - bloklı shifrlaw algoritmi bolıp, ol 64 bitli maǵlıwmatlardı shifrlaydı. Algoritmniń kiriwinde berilgen 64 bitli ashıq tekst, shıǵıwda 64 bitli shifrlanǵan tekstke ózgeredi. DES simmetriyalı algoritm bolıp, onda shifrlaw hám deshifrlaw ushın birdey algoritm hám gilt paydalanıladı.

Algoritmde gilt uzınlıǵı 56 bitke teń (gilt ádette 64 bitke teń, biraq hár bir segizinshi bit juplıqtı tekseriw ushın qollanıladı hám ol alınbaydı). Qálegen 56 bitli san bolıwı múmkin bolǵan giltti, qálegen waqıt momentinde ózgertiw múmkin. Algoritmniń qáwpsizligin tolıǵı menen gilt anıqlaydı.

Algoritmniń ápiwayı bóleginde shifrlawdıń tiykarǵı eki usılı bolǵan: aralastırıw hám diffuziya qaraladı. DES tiń fundamental dúziwshi blokı tekstke giltten ǵárezli bolǵan usı usıllardıń bir mártelik kombinaciyasın qollanıw bolıp tabıladı (ornına qoyıw, sońınan orın almastırıw). Bunday blok etap dep ataladı. DES algoritmi 16 etaptan turadı, yaǵnıy usıllardıń birdey kombinaciyası ashıq tekstke 16 márte qollanıladı.

DES ashıq teksttiń 64 bitli blokı menen jumıs isleydi. Dáslepki orın almastırıwdan soń blok 32 bitten turıwshı oń hám shep bóleklerge ajıratıladı. Sońınan maǵlıwmatlardı gilt penen biriktiretuǵın f funkciyası 16 etapta da orınlanadı. 16 etaptan keyin oń hám shep yarım bólekler qosıladı hám algoritm aqırǵı orın almastırıwdı orınlaydı (dáslepkige qarata keri).

Hár bir etapta gilttiń bitleri jıljıydı hám sońınan 56 bitli giltten 48 bit alınadı. Oń bólektegi maǵlıwmatlar keńeytirilgen orın almastırıw járdeminde 48 bitke shekem jetkerilip, ol 48 bitli gilt penen XOR ámeli járdeminde biriktiriledi, sońınan segiz $S-$bloktan ótip jańa 32 bitti dúzedi hám jáne orınları almastırıladı. Bul tórt ámel f funkciyası járdeminde orınlanadı. Alınǵan f funkciyasınıń nátiyjesi shep yarım bólek penen XOR ámeli járdeminde biriktiriledi. Bul ámellerdi orınlaw nátiyjesinde jańa oń yarım bólek payda boladı, al eski oń yarım bólek jańa shep yarım bólekke ózgeredi. Bul ámeller 16 márte orınlanadı.

Egerde i-shı iteraciyanıń nátiyjesi B_i bolsa, onda R_i hám L_i lar B_i dıń oń hám shep yarım bólekleri, K_i – bolsa i-shı etap ushın 48 bitli gilt, al f - gilt penen XOR hám barlıq orın almastırıw ámellerin orınlawshı funkciya bolsa, onda bul etaptı tómendegishe kórsetiwge boladı:

$$\mathrm{L_i} = R_{i-1}$$

$$R_\mathrm{i} = L_{i-1} \oplus f(R_{i-1}, K_i)$$

ГОСТ algoritmde bloktıń uzınlıǵı 64 bit hám gilttiń uzınlıǵı 256 bitten ibarat. Algoritmniń islew processi 32 etaptan turadı. Bul etaplarda izbe-iz túrde shifrlawdıń ápiwayı algoritmi orınlanadı.

ГОСТ hám DES algoritmleriniń bir-birinen ózgesheligi to'mendegishe:

- DES giltten úles giltlerdi genraciyalaw ushın quramalı proceduranı paydalanadı, al ГОСТ ta bul procedura júdá ápiwayı.
- DES te gilt uzınlıǵı 56 bit, al ГОСТ ta ol 256 bitke teń. Egerde S – bloklardıń sırlı orın almastırıwların qossaq, onda ГОСТ tıń sırlı informaciyasınıń tolıq kólemi shama menen 610 bitti quraydı.
- DES tiń S – bloklarında kiriw 6 bit hám shıǵıw 4 bit, al ГОСТ ta bolsa kiriw de shıǵıw da 4 bitten turadı. Eki algoritmde de S – bloklar sanı teń, biraq ГОСТ ta onıń ólshemi DES tiń S – blokı ólsheminiń tórtten birine teń.
- DES te P-blok dep atalıwshı regulyar emes orın almastırıwdı paydalanadı, al ГОСТ bolsa shepke 11 bitli cikllıq jıljıwdan paydalanadı.
- DES te 16 etap, al ГОСТ ta 32 etap.

ГОСТ algoritmin qopal kúsh jumsap buzıw júdá qıyın. Sonlıqtan ol júdá qáwpsiz algoritm sanaladı. Algoritm 256 bitli giltti paydalanadı, egerde sırlı S – bloklardı da esapqa alsaq, onda onıń uzınlıǵı elede ósedi. Ol DES ke qaraǵanda differencial hám sızıqlı kriptoanalizge qarata turaqlıraq. Biraqta ГОСТ tıń tosınnanlı S – blokları DES tiń fiksirlengen S – bloklarınan da kúshsiz bolıwı múmkin. Olardıń sırlılıǵı ГОСТ tıń differencial hám sızıqlı kriptoanalizge qarsı turaqlı bolıwın arttıradı. Ashıwdıń bul usıllarına etaplar sanı tásir etedi, yaǵnıy etap qanshelli kóp bolsa, shifrdı ashıw sonshelli qıyın sanaladı. ГОСТ algoritminde etaplar sanı DES ke qaraǵanda eki ese kóp, sonlıqtan kriptoanalizdiń bul usılların qollanıp onı ashıw jolın joqqa shıǵaradı.

ГОСТ tıń ayırım etapları hálsiz sanaladı. Ol DES algoritminde qollanılatuǵın keńeytirilgen orın almastırwdan paydalanbaydı. Bunday ámeldiń joqlıǵı algoritmdi hálsiretedi.

Eń úlken ayırmashılıq, bul ГОСТ ta orın almastırıw ornına cikllıq jıljıwdı qollanadı. DES tegi orın almastırıw sel effektin kúsheytiredi. ГОСТ algoritminde bir kiriwshi bittiń ózgerisi bir etaptıń bir S – blokına tásir etedi hám sonnan soń kelesi etaptıń eki S – blokına tásir etedi h.t.b. ГОСТ ta kiriwshi

bir bittiń ózgerisi nátiyjeniń hár bir bitine tásir etiw ushın 8 etap talap etiledi, al DES te bunıń ushın tek ǵana 5 etap kerek. Bul algoritmniń hálsiz jeri. Biraqta ГОСТ 32, al DES tek ǵana 16 etaptan turatuǵınlıǵın umıtpawımız kerek.

3-§. Asimmetriyali kriptosistemalar

Asimmetriyalı shifrlaw usılı Uitfild Diffi hám Martin Xellmannıń 1976-jılı járiyalanǵan «Zamanagóy kriptografiyanıń jańa baǵdarları» jumısında kórsetildi. Ashıq giltti tarqatıw haqqında Ralf Merkldiń jumısları tásirinde, olar ashıq kanaldı paydalanıp jasırın giltti alıw jolın usındı. Bul sxema 1970-jıllarda Malkolm Vilyamson tárepinen islep shıǵılǵan edi, biraq 1977-jılǵa shekem sır saqlandı. Ashıq giltti tarqatıw boyınsha Merkl usılı 1974-jılı jaratıldı hám ol 1978-jılı járiyalandı, onı jánede Merkl jumbaǵı depte ataydı.

Diffi-Xellman algoritmi jaratılǵannan soń, onıń tiykarında 1977-jılı Massachusets Texnologiya Institutı (MIT) alımları Ronald Rivest, Adi Shamir hám Leonard Adleman tárepinen kóbeytiwshilerge jiklew máselesine tiykarlanǵan shifrlaw algoritmi islep shıǵıldı. Ol qorǵalmaǵan kanal boyınsha informaciya almasıw máselesin sheshetuǵın birinshi asimmetriyalı shifrlaw algoritmi boldı. Sistema olardıń familiyalarınıń birinshi háriplerinen ibarat bolıp RSA (Rivest, Shamir, Adleman) dep ataldı. Bul sistema 1973-jılı húkimetlik baylanıs orayında islewshi Klifford Koks tárepinen ashılǵan edi, biraq bul jumıs oraydıń ishki hújjetlerinde ǵana saqlandı. Sonlıqtan ol 1977-jılǵa shekem belgisiz bolıp qaldı. RSA – shifrlaw hám elektron tańbalı imza ushın paydalanatuǵın birinshi algoritm boldı.

Ulıwma aytqanda, belgili asimmetriyalı kriptosistemalar tiykarında bir táreplemeli funkciyalar hám funkciya-lazeykalardı dúziwge baylanıslı quramalı matematikalıq máseleler jasırınǵan.

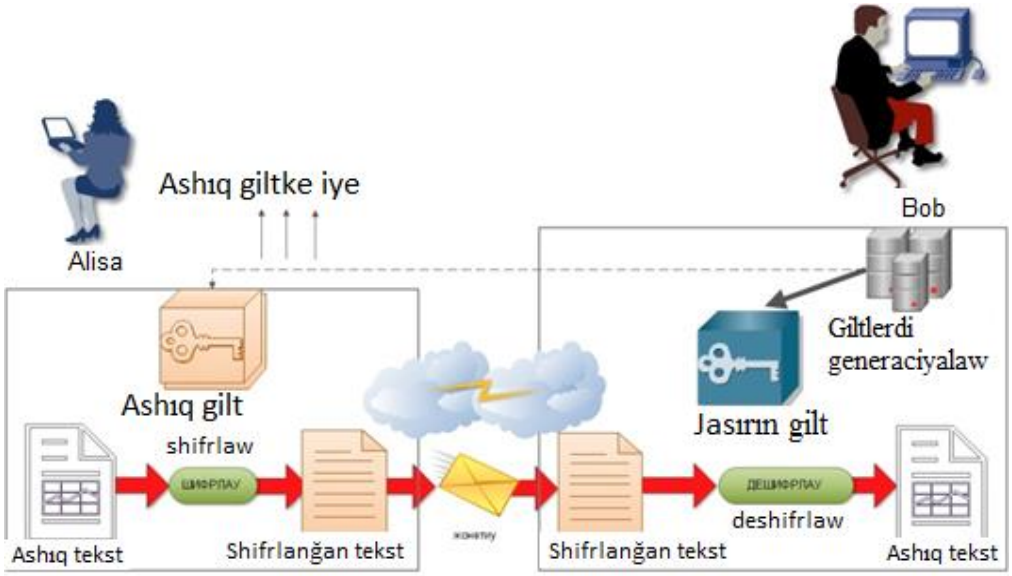
Asimmetriyalı giltli kriptografiya sanlar teoriyasınıń máseleleri menen tıǵız baylanıslı. Házirgi waqıtta paydalanatuǵın barlıq ashıq giltli kriptosistemalar tómendegishe túrdegi máselelerge tiykarlanǵan boladı:

1. Úlken sandı ápiwayı kóbeytiwshilerge jiklew (RSA algoritmi);

2. Logarifmdi yamasa dárejege kóteriwdi esaplaw (Diffi-Hellman algoritmi);
3. Algebralıq teńlemelerdiń korenlerin esaplaw;

Keri esaplanıwı qıyın bolǵan funkciyalarǵa ápiwayı mısal keltireyik. Máselen, yadtan eki ápiwayı 11 hám 13 sanlarınıń kóbeymesin tabıw ańsat. Biraq yadtan, kóbeymesi 437 ge teń bolǵan eki ápiwayı sandı tez tabıwǵa háreket etip kóriń?. Júdá úlken sandı ápiwayı kóbeytiwshilerge ajıratıw ushın esaplaw texnikasın paydalanǵanda da úlken qıyınshılıqlardı keltirip shıǵaradı (bul másele sheshiliwi múmkin, biraq kóp waqıt talap etiledi).

RSA kriptosisteması shifrlaw hám shifrdan ashıw ushın júdá úlken sanlardı paydalanadı. Tilekke qarsı kópshilik kompyuter tilleri, ásirese júdá úlken san ushın dárejeni effektiv esaplaw operatorlarına iye emes. Bul ámeldi esaplawda jaqsı nátiyjege erisiw ushın bizge effektiv algoritmler zárúr boladı.



1.2-súwret. Asimmetriyalı giltli kriptosistemanıń ulıwma ideyası.

Asimmetriyalı kriptosistemalarda eki hár qıylı gilt qollanadı: K_b – A uzatıwshınıń ashıq gilti; k_b – B qabıl etiwshiniń jasırın gilti. Giltler generatorın B qabıl etiwshi tárepte jaylastırǵan maqsetke muwapıq (k_b jasırın giltti qorǵalmaǵan kanal boyınsha uzatpaw ushın). K_b hám k_b giltleri mánisleri giltler generatorınıń dáslepki jaǵdayınan ǵárezli.

K_b ashıq gilti boyınsha k_b jasırın giltti anıqlaw esaplaw jolları járdeminde sheshilmeytuǵın másele bolıwı kerek.

Asimmetriyalı kriptoalgoritmlerdi:

- informaciyalardı qorǵaw ushın óz betinshe ortalıq sıpatında;
- giltlerdi bólistiriw ortalıǵı sıpatında. (ádette asimmetriyalı kriptosistemalar járdeminde kólemi boyınsha kishi giltlerdi bólistiredi, al úlken informaciyalıq aǵımlardı uzatıw ushın basqa algoritmdi paydalanadı);
- paydalanıwshılar autentifikaciyası sıpatında

paydalanıw múmkin.

Tómende keltirilgen asimmetriyalı kriptosistemalar keń tarqalǵan sanaladı:

- RSA (Rivest-Shamir-Adleman)
- DSA(Digital Signature Algorithm)
- El-Gamal (El-Gamal sisteması)
- Diffie-Hellman (Diffi — Xelman giltlerdi almasıw algoritmi)
- ECDSA (Elliptic Curve Digital Signature Algorithm) — elliptikalıq iymekliklerdegi elektron tańbalı imza algoritmi.
- ГОСТ Р 34.10-2001 hám t.b.

Asimmetriyalı kriptografiya usılları ideyası menen júdá jaqınnan tanısıwda bizge tómendegishe 3 másele járdem beredi.

1-másele – kompyuterde sırlı sózdi (paroldı) saqlaw. Tarmaqtaǵı hár bir paydalanıwshı óziniń sırlı sózine iye boladı. Tarmaqqa kirgende ol óziniń atın, sońınan sırlı sózin kiritedi. Egerde bul sóz kompyuterde saqlansa, onda onı nızamsız túrde ózge shaxs alıp, basqa maqsetlerde de paydalanıwı múmkin. Sonlıqtan bunday xadiyseler júz bermewi ushın kompyuterdegi saqlanǵan maǵlıwmattı «buzıw»ǵa jol qoymaw máselesin sheshiw bolıp esaplanadı.

2-másele bul - radiolakator hám hawa húјiminen qorǵanıw sistemalarınıń payda bolıwı menen baylanıslı. Samolet shegaranı kesip ótip atırǵanda radiolakator onnan sırlı sózdi soraydı, egerde ol ras bolsa, onda samolet ózimizdiki, keri jaǵdayda dushpan samoleti dep esaplanadı. Bul jerde másele

ashıq kanallar járdeminde sırlı sóz qalayınsha jetkerip beriw máselesi bolıp tabıladı. Sebebi dushpan tárep barlıq sóylesiwlerdi esitiwi hám sırlı sózdi bilip onı óz mápinde isletiwi múmkin.

3-másele de dáslepkige uqsas, biraq ol tarmaqta bir-birinen uzaqta jaylasqan kompyuterler arasında, yaǵnıy bank hám klient arasında bolıwı múmkin.

Házirgi waqıtta bunday máseleler kriptografiyalıq usıllar járdeminde sheshiledi. Bul máseleni sheshiw bir tárepleme funkciya túsinigine tiykarlanadı.

Anıqlama. Meyli X ($x \in X$) shekli kópliginde anıqlanǵan

$$y = f(x) \tag{1.3}$$

funkciyası berilsin hám onıń

$$x = f^{-1}(y) \tag{1.4}$$

túrindegi keri funkciyası bar bolsın. Egerde (1.3) funkciyanı esaplaw ańsat, al (1.4) keri funkciyanı esaplaw qıyın másele bolsa, onda bunday funkciyanı bir tárepleme funkciya dep ataymız.

Atap aytqanda keri máseleni zamanagóy super kompyuterlerde sheshiwde shama menen $10^6 - 10^{10}$ mashina waqtın talap etiwi múmkin.

Mısal sıpatında bunday funkciyaǵa

$$y = a^x \pmod p \tag{1.5}$$

qarastırayıq, bunda p bazı bir ápiwayı san, al x sanı - $\{1,2,...p-1\}$ kópliginen alınǵan pútin san. Keri funkciya

$$x = \log_a y \pmod p \tag{1.6}$$

túrinde belgilenip onı biz diskret logarifm dep ataymız.

Házirgi waqıtta eń jaqsı zamanagoy kompyuterlerden paydalanıp (1.6) esaplawdı qıyınlastırıw ushın ólshemi 512 bitten úlken bolǵan sanlar qollanıladı. Ámeliyatta ayrım waqıtları bir tárepleme funkciyanıń basqasha túrleri de qollanıladı (mısalı, qısqa 60-120 bitli tártiptegi sanlarǵa súyenetuǵın xesh-funkciya dep atalıwshı funkciyalardan paydalanamız).

Dáslep biz (1.5) esaplaw jetkilikli dárejede tez orınlanatuǵının qarastıramız. Mısalı $a^{16} \bmod p$ sanın esaplawda

$$a^{16} \bmod p = (((a^2)^2)^2) \bmod p$$

dep jazamız, yaǵnıy berilgen mısalda 15 márte kóbeytiwdiń ornına tek ǵana 4 kóbeytiw ámelin orınlaw kerek boladı.

Algoritmdi táriyplew ushın $\log_2 x$ pútin bólegi bolǵan $t = \lfloor \log_2 x \rfloor$ shamasın kiritemiz. Tómendegishe sanlar qatarın esaplaymız

$$a, a^2, a^4, a^8, \ldots a^{2^t} \pmod p \tag{1.7}$$

(1.7) qatarındaǵı hár bir san $p-$moduli boyınsha dáslepki sandı óz-ózine kóbeytiw jolı arqalı alınadı. x dáreje kórsetkishin ekilik sanaq sistemasında jazamız:

$$x = (x_t x_{t-1} \ldots x_1 x_0)_2$$

Onda $y = a^x \pmod p$ sanı

$$y = \prod_{i=0}^{t} a^{x_i 2^i} \pmod p \tag{1.8}$$

túrinde esaplanıwı múmkin. Mısal sıpatında $3^{100} \pmod 7$ qarastırayıq.

$t = \lfloor \log_2 100 \rfloor = \lfloor 6,643856 \rfloor = 6$ tabamız hám (1.7) tiykarında

$$\begin{array}{ccccccc} a & a^2 & a^4 & a^8 & a^{16} & a^{32} & a^{64} \\ 3 & 2 & 4 & 2 & 4 & 2 & 4 \end{array} \tag{1.9}$$

esaplaymız. Dáreje kórsetkishti ekilik sanaq sistemasına ótkeremiz

$100 = = (1100100)_2$ hám (1.8) formula boyınsha:

$$\begin{array}{cccccccc} a^{64} & a^{32} & & & a^4 & & & \\ 4* & 2* & 1* & 1* & 4* & 1* & 1 & = 4 \end{array} \tag{1.10}$$

iye bolamız. Biz bul jerde barlıǵı bolıp 8 kóbeytiw ámelin orınladıq ((1.9) ushın 6 hám (1.10) ushın 2 ámel).

Ulıwma jaǵdayda tómendegi tastıyqlaw orınlı boladı.

Tastıyqlaw. ((1.5) esaplaw quramalılıǵı haqqında). (1.5) kórsetilgen usıl boyınsha esaplaǵanda kóbeytiw ámelleriniń san $2\log_2 x$ tan asıp ketpeydi.

Dálilleniwi. (1.7) qatardaǵı sanlardı esaplaw ushın t kóbeytiw talap etiledi, al y tı (1.8) boyınsha esaplaw ushın kóbeytiw t dan artıp ketpeydi. $t=\lceil \log_2 x \rceil$ shártinen $\lceil \log_2 x \rceil \le \log_2 x$ boladı. Dálillendi.

Eskertiw. p moduli boyınsha dárejege kótergende dáreje kórsetkish $x < p$ túrinde bolıwı kerek. Bul jaǵdayda (1.5) esaplawda kóbeytiw ámelleriniń sanı $2\log_2 x$ tan asıp ketpeydi dep ayta alamız.

(1.5) úlken p lar ushın haqıyqattan da bir tárepleme funkciya boladı. Egerde biz keri funkciyanı esaplawda kelesi paragraflarda qarastırılatuǵın «kishi adım, úlken adım» usılın paydalansaq, onda tómendegi nátiyjeni alamız:

1-tablica

p nıń jazılıwındaǵı onlıq tańbalar sanı	(1.5) in esaplaw ($2\log_2 x$ kóbeytiw)	(1.6) in esaplaw ($2\sqrt{p}$ kóbeytiw)
12	$2\cdot 40 = 80$	$2\cdot 106$
60	$2\cdot 200 = 400$	$2\cdot 1030$
90	$2\cdot 300 = 600$	$2\cdot 1045$

Biz bul jerede, egerde modullar 50-100 onlıq tańbadan turıwshı sanlar bolsa, onda «tuwrı» funkciya tez esaplanadı, al keri funkciyanı esaplaw ámeliy jaqtan múmkin emes ekenligin kóremiz. Mısal sıpatında 90 tańbalı eki sandı 10^{-14} sekundta kóbeyte alatuǵın superkompyuterge (1.5) esaplaw ushın

$$T_{tuwri\ funk\ esap} = 600\cdot 10^{-14} = 6\cdot 10^{-12}\ sek$$

al (1.6) esaplaw ushın

$$T_{keri\ funk\ esap} = 10^{45}\cdot 10^{-14} = 10^{31}\ sek$$

waqıt talap etedi, yaǵnıy ol shama menen 10^{22} jılǵa teń. Bunday uzınlıqtaǵı sanlar ushın keri funkciyanı esaplaw hátteki kompyuter tarmaǵında parallel esaplawlar júrgizgenimiz benen de ámeliy jaqtan ulıwma múmkin emes.

Qarastırılǵan mısalda biz keri funkciya $2\sqrt{p}$ ámelde esaplanadı dep aldıq. Házirgi waqıtta diskret logarifmdi esaplawdıń júdá «tez» algoritmleri de bar. Biraqta báribir olarda da talap etiletuǵın ámeller sanı $2\log_2 p$ dan kóp. Bunnan biz (1.5) funkciya haqıyqattan da bir tárepleme dep uyǵarıwımız múmkin, biraqta hesh kim (1.6) keri funkciyasın «tuwrı» funkciyaǵa uqsas tez esaplanatuǵınlıǵın házirge shekem dálillep kórsetpegen.

(1.5) bir tárepleme funkciyasın joqarıda aytılıp ótken barlıq úsh másele ushın da qollanamız.

Ámeldegi asimmetriyalı kriptosistemalar turaqlılıgın támiyinlewge tiykar bolǵan quramalı másele túri boyınsha tómendegishe klassifikaciyalanadı:

- faktorlizaciyalaw máselesine tiykarlanǵan kriptosistemalar;
- diskret logarifmlew máselesin esaplaw quramalılıǵına tiykarlanǵan kriptosistemalar;
- elliptikalıq iymekliklerdegi diskret logarifmlew máselesine tiykarlanǵan kriptosistemalar;
- basqa máselelerge tiykarlanǵan kriptosistemalar.

Ámeliyatta asimmetriyalı kriptoalgoritmler arasında xalıqaralıq aralıq hám mámleketlik standartlarǵa iye bolǵan elektron tan'balı imza algoritmleriniń kópshiligi faktorlizaciyalaw (RSA, ESIGN), diskret logarifmlew (DSA, ГОСТ Р 34. 10-94), elliptikaliq iymekliklerdegi diskret logarifmlew (ГОСТ Р 34.10-2001, EC-DSA-2000, EC-KCDSA, EC-DSA hám ДСТУ 4145-2002) hám modul boyınsha dárejege ko'teriw (ÓzDSt 1092-2005, ÓzDSt 1092-2009) máselelerine tiykarlanǵan algoritmler bolıp tabıladı.

I-bapqa juwmaq

Bul bapta úyrenilgen matematikalıq tiykarlamalar bizge kriptografiyalıq sistemadan paydalanıwǵa múmkinshilik beredi. Biz ulıwma kriptografiyalıq sistemalardı qarap shıqtıq hám temanıń tiykarǵı izertlew obekti bolǵan RSA algoritmi algoritminiń tiykarında jatırǵan bir tárepleme funkciya haqqında ulıwma túsinik berip óttik.

II-BAP. FAKTORIZACIYALAW MA'SELESINE TIYKARLANǴAN KRIPTOGRAFIYALI' SISTEMALAR

1-§. RSA shifrlaw algoritmi

Diffi hám Xellman bir tárepli funkciyanıń anıqlamasına tıykarlanıp, jasırın baylanıs sistemasının' paydalanıwshıları ushın, ózleriniń ashıq giltli kriptosistemasın usınıs etdi. Bul sistema jasırın kanal járdeminde jónetiletuǵın sırlı giltlerdi qollanbay aq, maǵlıwmatlardı qorǵawǵa múmkinshilik beretuǵın birinshi sistema bolıp tabıladı.

Egerde N paydalanıwshıdan turatuǵın baylanıs kanalı bar bolǵanda eki abonent arasında sırlı giltlerdi almasıw ushın $C_N^2 = \frac{N(N-1)}{2} \approx \frac{N^2}{2}$ gilt zárúr bolar edi. Egerde abonentler sanı 100 bolsa, onda 5000 gilt, al egerde abonentler 10^4 bolsa, onda giltler sanı $5 \cdot 10^7$ bolıwı kerek. Bul jerde biz sonshelli giltlerdi bólistiriw qanday qıyın hám kóp shıǵın talap etetuǵının kóremiz.

Diffi hám Xellman giltlerdi esaplap olardı ashıqtan ashıq bólistiriw esabınan bul máseleni sheshti.

Meyli A, B, C abonentleri arasında baylanıs sisteması dúzilsin. Hár bir abonent óziniń sırlı hám ashıq informaciyasına iye. Bul sistemanı shólkemlestiriw ushın bazı bir p úlken ápiwayı sanı hám $1 < g < p-1$ aralıqtan g sanı saylap alınadı. Bul sanlar barlıq abonentlerge málim.

Abonentler bazı bir X_A, X_B, X_C úlken sanların saylap alıp olardı sır saqlaydı (ádette olar tosınnan saylap alınadı). Sońınan hár bir abonent tómendegi ámellerdi orınlaydı:

$$\begin{cases} Y_A = g^{X_A (\mathrm{mod}\, p)} \\ Y_B = g^{X_B (\mathrm{mod}\, p)} \\ Y_C = g^{X_C (\mathrm{mod}\, p)} \end{cases} \qquad (2.1)$$

hám olar ashıq túrde basqa abonentlerge jetkerip beriledi. Nátiyjede tómendegishe tablicaǵa iye bolamız: Y_A, Y_B, Y_C ashıq gilt

A abonent B abonenti menen baylanıs jasamaqshı bolsın, bul jaǵdayda joqarıdaǵı maǵlıwmatlar eki abonentkede belgili. A abonenti B ǵa ashıq kanal arqalı xabar jibermekshi ekenligin xabarlaydı. Sońınan ol

$$Z_{AB} = (Y_B)^{X_A} (\mathrm{mod}\ p) \tag{2.2}$$

esaplaydı. Óz gezeginde B abonenti de

$$Z_{BA} = (Y_A)^{X_B} (\mathrm{mod}\ p) \tag{2.3}$$

ámelin orınlaydı.

Tastıyıqlaw.

$$Z_{AB} = Z_{BA} \tag{3.17}$$

Dálilleniwi.

$$Z_{AB} = (Y_B)^{X_A} (\mathrm{mod}\ p) = (g^{X_B})^{X_A} (\mathrm{mod}\ p) =$$
$$= g^{X_A X_B} (\mathrm{mod}\ p) = (Y_A)^{X_B} (\mathrm{mod}\ p) = Z_{BA}$$

Sistemanıń tiykarǵı qásiyeti:

1. A hám B abonentleri baylanıstıń ashıq kanalında jiberilmegen birdey $Z = Z_{AB} = Z_{BA}$ sanına iye boldı.

2. Sistemaǵa xújim etiwshi X_A, X_B sırlı sanların bilmeydi, sonlıqtan ol Z_{AB} sanın esaplay almaydı. Ulıwma aytqanda ol Y_A boyınsha sırlı san bolǵan X_A nı esaplawǵa urınıwı múmkin, biraqta bul úlken p lar ushın ámeliy jaqtan múmkin emes (millionlaǵan jıl kerek).

A hám B abonentleri Z_{AB} sanın sırlı gilt sıpatında qollanıp maǵlıwmatlardı shifrlaw hám deshifrlaw ushın paydalanıwı múmkin. Usınday jol menen qálegen eki abonent tek ózlerine belgili bolǵan sırlı giltti esaplawı múmkin.

Sistemada g sanın saylap alıw bir qansha qıyınshılıq tuwdıradı. Qarastırılǵan sistemanıń joqarı turaqlılıǵın támiyinlew ushın $p-1$ sanı úlken

ápiwayı kóbeytiwshige iye bolıw kerek degen talap qoyıladı. Sonlıqtan p ápiwayı sanı

$$p = 2q + 1$$

teńligi orınlanatuǵınday etip saylap alanadı, bunda q - ápiwayı san. Onda g sıpatında tómendegi shártti qanaatlandıratuǵın qálegen sandı alıwımızǵa boladı.

$$1 < g < p - 1$$

$$g^q \bmod p \neq 1$$

Bul sisemani 1976-jılda Diffi hám Xellman ózleriniń «Kriptologiyada jańa bag'dar» ilimiy jumısıda bayan etken edi. 1978-jılda bolsa, Massachusets texnologiya institutınıń ilimpazları R. L. Rivest, A. Shamir, L. Adleman, ózleriniń ilimiy maqalasında birinshi bolıp sırlı hám haqıyqattan da bir tárepleme bolǵan funkciyanı usınıs etedi. Bul maqala «Tańbalı imzalardı du'ziw usılları hám ashıq giltli kriptosistemalar» dep atalıp, kóbirek autentifikaciya máselelerine qaratılǵan. Házirgi kúnde, bul joqarıda atları keltirilgen ilimpazlar usınıs etken algoritm, sol ilimpazlardıń húrmetine RSA algoritm dep ataladı. Bul algoritmdi u'yreniw ushın sanlar teoriyasınan to'mendegishe ayırım maǵlıwmatlardı biliw talab etiledi.

Anıqlama 1. Egerde bizge p pútin oń sanı berilip, ol tek ǵana ózine hám birge bólinse, onda ol ápiwayı san dep ataladı.

Mısalı, 11, 23 sanları ápiwayı, al 27, 33 sanları quramalı, sebebi 27 sanı 3 ke hám 9 ǵa, 33 bolsa 3 ke hám 11 ge bólinedi.

Teorema. (Arifmetikanıń tiykarǵı teoreması). Qálegen pútin oń sandı ápiwayı sanlardıń kóbeymesi túrinde kórsetiw múmkin hám ol jalǵız boladı.

Mısalı, $27 = 3 \cdot 3 \cdot 3,\ 33 = 3 \cdot 11$

Anıqlama 2. Egerde a hám b sanları berilip $EUUB(a,b) = 1$ bolsa, onda olar óz-ara ápiwayı sanlar dep ataladı.

Mısalı, 27 hám 28 sanları óz ara ápiwayı, sebebi $EUUB(27,28) = 1,$ al 27 hám 33 bolsa óz-ara ápiwıyı emes, sebebi $EUUB(27,33) = 3$

Anıqlama 3. (Eyler funkciyası). Meyli $n \geq 1$ pútin sanı berilsin. Onda $\varphi(n)$ Eyler funkciyası $1,2,3,...n-1$ sanlar qatarında n sanı menen óz-ara ápiwayı bolǵan sanlardıń sanına teń boladı.

Mısalı: a) $\varphi(10) = ?$

1.3-tablica

n	1	2	3	4	5	6	7	8	9
$\varphi(n)$	1	0	1	0	0	0	1	0	1

Demek $\varphi(10) = 4$

b) $\varphi(12) = ?$

1.4-tablica

n	1	2	3	4	5	6	7	8	9	10	11
$\varphi(n)$	1	0	0	0	1	0	1	0	0	0	1

Demek $\varphi(12) = 4$

Eskertiw. Bul jerde óz-ara ápiwayı bolatuǵın sanlar astına 1 jazılǵan.

Tastıyıqlaw . Egerde p ápiwayı san bolsa, onda

$$\varphi(p) = p - 1 \tag{2.4}$$

Tastıyıqlaw (*). Meyli p hám q ápiwayı sanlar bolsın $(p \neq q)$, onda

$$\varphi(pq) = (p-1)(q-1) \tag{2.5}$$

Dálilleniwi. $1,2,3,...,pq-1$ sanlar qatarında pq sanı menen óz-ara ápiwayı emes sanlar

$$p, 2p, 3p, ..., (q-1)p$$

$$q, 2q, 3q, ..., (p-1)q$$

Bunday sanlardıń sanı $(q-1)+(p-1)$. Sonlıqtan pq sanı menen óz-ara ápiwayı bolatuǵın sanlardıń sanı

$$pq - 1 - (p-1) - (q-1) = pq - q - p + 1 = (p-1)(q-1).$$

Teorema (Ferma). Meyli p ápiwayı san hám $0 < a < p$ bolsın, onda

$$a^{p-1} \bmod p = 1 \tag{2.6}$$

Mısalı, $p = 13, a = 2$

$$2^{12} \bmod 13 = (2^2)^2 \cdot ((2^2)^2)^2 \bmod 13 = 3 \cdot 9 \bmod 13 = 1$$

$$10^{10} \bmod 11 = 10^2 \cdot ((10^2)^2)^2 \bmod 11 = 1 \cdot 1 = 1$$

Teorema (Eyler). Meyli a hám b óz-ara ápiwayı sanlar bolsın, onda

$$a^{\varphi(n)} \bmod b = 1 \tag{2.7}$$

Ferma teoreması b sanı ápiwayı bolǵanda Eyler teoremasınıń dara jaǵdayı bolıp tabıladı.

Mısalı,

$$\varphi(12) = 4$$

$$5^4 \bmod 12 = (5^2)^2 \bmod 12 = (1^2)^2 \bmod 12 = 1$$

$$\varphi(21) = 2 \cdot 6$$

$$2^{12} \bmod 21 = 2^4 (2^4)^2 \bmod 21 = 16 \cdot 4 \bmod 21 = 1$$

Teorema(**). Egerde p hám q ápiwayı sanlar bolıp, $p \neq q$ hám $k \in Z$ bolsa, onda tómendegishe teńlik orınlı boladı:

$$a^{k\varphi(pq)+1} \bmod (pq) = a \tag{2.8}$$

Mısalı, $p = 5, q = 7$. Onda $pq = 35$, al $\varphi(pq) = \varphi(35) = 4 \cdot 6 = 24$. Meyli $k = 2$ bolsın, onda $2 \cdot 24 + 1 = 49$. Bunnan

$$9^{49} \bmod 35 = 9,\ 23^{49} \bmod 35 = 23$$

Bul orınlı boladı, sebebi 9 hám 233 sanları 35 moduli boyınsha óz-ara ápiwayı sanlar hám Eyler teoreması boyınsha

$$9^{24} \bmod 35 = 1,\ 23^{24} \bmod 35 = 1$$

Biraqta **3.13** tómendegi sanlar ushın da orınlı boladı, al Eyler teoremasın bolsa, olar ushın qollana almaymız (sebebi 10 hám 25 sanlarınıń hár biri 35 moduli menen óz-ara ápiwayı emes), yaǵnıy:

$$10^{49} \bmod 35 = 10,\ 28^{49} \bmod 35 = 28$$

Anıqlama. Meyli a hám b oń pútin sanlar bolsın, onda a hám b sanlarınıń eń úlken bóliwshisi dep a hám b sanların bóletuǵın eń úlken c sanına aytamız, yaǵnıy

$$c = EUUB(a,b)$$

Algoritmniń isenimliligi úlken sanlardı faktorizaciyalaw hám diskret logarifmlerdi esaplaw máselesine tiykarlanadı.

Kriptografiddıq sistemalar ushın evklidtiń ulıwmalastırılǵan algoritmi áhmiyetli bolıp tabıladı.

Teorema (Evklid). Meyli a hám b teris emes pútin sanları berilgen bolsın. Onda x hám y pútin sanları bar bolıp olar ushın

$$ax + by = E\bar{U}UB(a,b)$$

teńligi orınlıboladı.

Házirgi rawajlanǵan jámiyette informaciya kommunikaciya tarmaqlarında elektron maǵlıwmat almasıwdıń keń tarqalıwı maǵlıwmatlardıń sırlılıg'ın, haqıyqıylıǵın hám avtorlıqtı ornatıw máselelerin sheshiwdi talap etedi. Mısalı, almasıp atırǵan elektron maǵlıwmatlar tiykarında qandayda bir ózgeriwler, bul maǵlıwmatlardin' avtorı máplerine qarsı kelip, ol elektron maǵlıwmat avtorı ekenliginen bas tartıwı múmkin. Sonday jaǵdaylardıń aldın alıw mexanizmı maǵlıwmat avtorın ózine ǵana belgili bolǵan qandayda bir sanlı parametr (jasırın gilt) menen baylanıslı tu'rde alınatug'in sanlar izbe-izliginen ibarat bolǵan elektron tańbalı imza (ETI) esaplanadı.

ETI da a'dettegi imzag'a uqsas tómendegish ush qa'siyett qanaatlandırıwı kerek:

• Hu'jjetke imzanı tek g'ana onın' "haqıyqıy" iyesi qoyıwı mu'mkin;

• elektron hújjetke imza qoyǵan subiekt avtorlıqtan bas tarta almaydı;

• kelispewshilik kelip shıqqan jag'dayda imzanın' haqıyqıylıg'ın tekseriw ushın u'shinshi ta'rep (mısalı, sud) qatnasıwı mu'mkin.

Qa'legen ETI algoritmi eki bo'lekten ibarat boladı:

• imza qoyıw;

• imzani tekseriw;

Imzalaw avtor tárepinen, tek oǵan belgili bolǵan jasırın gilt penen ámelge asırıladı. Imzanın' haqıyqıylıǵın tekseriw bolsa qálegen shaxs tárepinen, imza avtorınıń ashıq gilti menen ámelge asırılıwı múmkin.

RSA algoritmi sanlar teoriyasındaǵı tómendegishe eki faktqa tiykarlanadı:

1) Sandı ápiwayılılıqqa tekseriw salıstırmalı túrde ańsat;

2) egerde biz tek ǵana n sanın bilip, al p hám q úlken sanlar bolsa, onda $n = pq$ túrindegi sanlardı ápiwayı kóbeytiwshilerge jiklew júdá qıyıyn másele boladı (faktorizaciya máselesi).

Meyli sistemada $A, B, C, \ldots$ abonentleri bar bolsın. Hár bir abonent tosınnanlı túrde eki úlken ápiwayı p hám q sanların saylaydı. Sońınan

$$n = pq \qquad (2.9)$$

sanın esaplaydı. Bunnan keyin abonent Eyler funkciyasın esaplaydı, yaǵnıy $\varphi(n) = (pq) = (p-1)(q-1)$ hám $\varphi(n)$ nen kishi bolǵan d sanın saylap aladı. Bul ámellerdi orınlap bolǵannan soń Evklidtiń ulıwmalastırılǵan algoritmi boyınsha e sanın tabamız hám ol tómendegishe teńlikti qanaatlandıradı:

$$ed(\mathrm{mod}\,\varphi(n)) = 1 \qquad (2.10)$$

Esaplaw nátiyjesinde alınǵan d, n parametrleri sistemada ashıq gilt, al e sırlı gilt wazıypasın atqaradı.

Meyli A abonenti m xabarın B abonentine jibermekshi bolsın. m xabarı san sıpatında qarastıramız hám ol $m < n$ teńsizligin qanaatlandırdı. Bul processti RSA algoritmi járdeminde tómendegishe ámelge asırıw múmkin:

1. A abonenti xabardı B abonentiniń ashıq parametrlerin paydalanıp

$$c = m^{d_B}(\mathrm{mod}\, n_B) \qquad (2.11)$$

formulası járdeminde shifrlaydı hám ashıq kanal boylap c nı jónetedi.

2. Shifrlanǵan xabardı alǵan B abonenti

$$m' = c^{e_B}(\mathrm{mod}\, n_B) \qquad (2.12)$$

esaplaydı.

Tastıyıqlaw. Qarastırılǵn algoritm ushın $m' = m$, yaǵnıy B abonenti A dan kelgen maǵlıwmattı aladı.

Dálilleniwi.

$$m' = c^{e_B} (\mathrm{mod}\, n_B) = m^{d_B e_B} (\mathrm{mod}\, n_B)$$

(2.10) teńlikten bazı bir k ushın

$$e_B d_B = k\varphi(n_B) + 1$$

Tastıyıqlaw (*) ǵa muwapıq

$$\varphi(n_B) = (p_B - 1)(q_B - 1)$$

Teorema (**) dan

$$m' = m^{k\varphi(n_B)+1} (\mathrm{mod}\, n_B) = m$$

ekenligi kelip shıǵadı.

Tastıyıqlaw (RSA algoritminiń qásyeti).

1) Algoritm maǵlıwmatlardı korret túrde shifrlaydı hám deshifrlaydı;

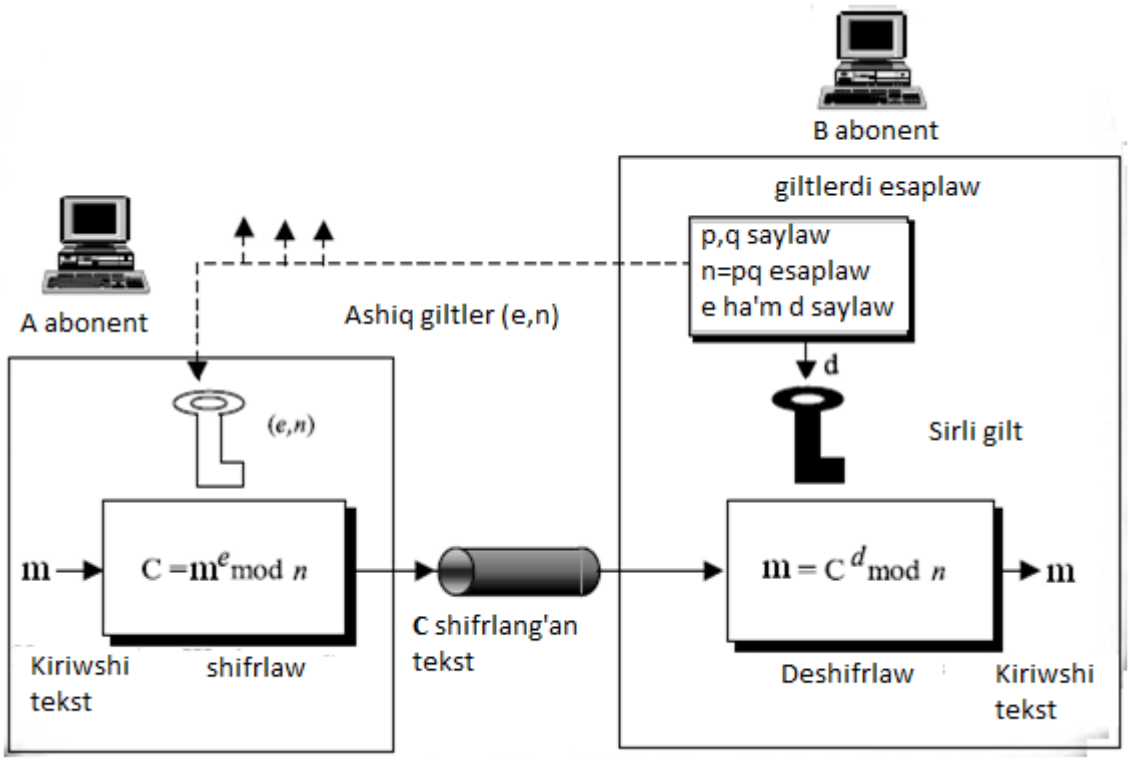
2) Barlıq xabarǵa iyelik etken hám ashıq maǵlıwmatlardan xabardar bolǵan shaxs baslanǵash xabardı taba almaydı (jetkilikli úlken p hám q ushın).

Dálilleniwi. Birinshi qásiyet 2.12 tastıyıqlawdan kelip shıǵadı. Ekinshi tastıyıqlawdı dálillewde buzǵınshı tek ǵana ashıq parametrlerdi biledi dep esaplaymız. Ol e ni tabıw ushın $\varphi(n_B)$ mánisin biliwi kerek, al onıń ushın bolsa onnan óz gezeginde p hám q lardı biliw talap etiledi. Ulıwma aytqanda ol p hám q lardı n sanın ápiwayı kóbeytiwshilerge jiklep tabıwı da múmkin. Biraqta bul júdá qıyın másele.

RSA sistemasında qollanılıp atırǵan $y = x^d (\mathrm{mod}\, n)$ bir tárepleme funkciyası, egerde n sanınıń ápiwayı kóbeytiwshileri málim bolǵanda $x = \sqrt[d]{y} (\mathrm{mod}\, n)$ keri funkciyanı ańsat esaplawǵa múmkinshilik beretuǵın «lazeykaǵa» iye. Egerde p hám q belgisiz bolsa, onda keri funkciyanı esaplaw ámeliy jaqtan múmkin emes, al p hám q lardı n boyınsha tabıw qıyın, yaǵnıy p hám q lar «lazeyka» yamasa «jasırın jol». Bunday qásiyetke iye bir

tárepleme funkciyalar kriptografiyanıń basqa bólimlerinde de óz qollanıwların tapqan.

RSA algoritmi ushın hár bir abonent óziniń jeke p hám q ápiwayı sanların saylap alıwı úlken áhmiyetke iye, yağnıy barlıq $n_A, n_B, n_C, \ldots$ modulleri hár qıylı bolıwı kerek (keri jağdayda abonentleri basqa bir abonentke arnalğan xabarlardı da oqıwı múmkin). Biraqta d ashıq parametrine bunday talap qoyılmaydı. d parametri barlıq abonentlerde birdey bolıwı múmkin.



___-su'wret

Mısal. A abonenti $m=15$ xabarın B ğa jibermekshi bolsın. B abonentiniń ashıq parametrleri tómendegishe:

$$p_B = 3, q_B = 11, n_B = 33, d_B = 3$$

e_B parmetrin Evklidtiń ulıwmalastırılğan algoritmi járdeminde tabamız, ol 7 teń.

m xabardı (2.11) járdeminde shifrlaymız:

$$c = 15^3 (\mathrm{mod}\, 33) = 15^2 \cdot 15 (\mathrm{mod}\, 33) = 27 \cdot 15 (\mathrm{mod}\, 33) = 9$$

9 sanı B abonentine baylanıstıń ashıq kanalı boyınsha jiberedi. Tek ǵana B abonentine $e_B = 7$ ekenligi málim, sonlıqtan ol alınǵan xabardı (2.12) formula járdeminde deshifrlaydı:

$$m' = 9^7 (\mathrm{mod}\, 33) = (9^2)^2 \cdot 9^2 \cdot 9 (\mathrm{mod}\, 33) = 15^2 \cdot 15 \cdot 9 (\mathrm{mod}\, 33) = 15.$$

Qarastırlǵan sistema p hám q lar úlken sanlar bolǵanda ashılmaydı, biraqta tómendegishe kemshilikke iye: A abonenti Bǵa onıń ashıq informaciyasınan (d_B, n_B) paydalanıp xabar jónetedi. Buzǵınshı B ushın arnalǵan xabardı oqıy almaydı, biraqta ol Bǵa A abonentiniń atınan xabar jiberiwi múmkin. Bunday jaǵdaydı boldırmaw ushın tómendegishe daslepkige qaraǵanda quramalıraq proceduradan paydalanamız.

Meyli A abonenti B ǵa m xabarın jibermekshi bolsın. Onıń ushın A dáslep $c = m^{e_A} (\mathrm{mod}\, n_A)$ sanın eaplaydı. Buzǵınshı bunı isley almaydı, sebebi ol sırlı e_A parametin bilmeydi. Sońınan A abonenti $f = c^{d_B} (\mathrm{mod}\, n_B)$ eaplaydı hám onı B ǵa jiberedi. B abonenti bul f tı aladı hám izbe-iz túrde $u = f^{e_B} (\mathrm{mod}\, n_B)$ hám $w = u^{d_A} (\mathrm{mod}\, n_A)$ esaplaydı.

Nátiyjede B abonenti $w = u$ xabarına iye boladı. Joqarıda qarastırǵanımızday bul jerde de buzǵınshı jiberilip atırǵan xabardı oqıy almaydı hám odan ózgesheligi buzǵınshı A abonentiniń atınan xabar jibere almaydı.

Bul jerde biz jańa túrdgi jaǵdayǵa dus kelemiz. Babonenti xabar A dan kelgenligin biledi, yaǵnıy A oziniń sırlı e_A parameti menen shifrlap onı «imzaladı». Bul qarastırılǵan mısal elektron tańbalı imza dep ataladı. Onı biz kelesi paragafta kórip shıǵamız.

2-§. RSA algoritmina tiykarlanǵan elektron tańbalı imza algoritmi

Egerde A abonenti hújjetti imzalawdı jobalastırǵan bolsın. Onda ol dáslep RSA parametrlerin dál aldınǵı paragrafta kórsetilgendey etip saylap alıwı kerek. Bul isti ámelge asırıw ushın A abonenti eki úlken p hám q ápiwayı sanların saylap alıp $n = pq$ hám $\varphi(n)$ di esaplaydı. Sońınan $\varphi(n)$ menen óz-ara piwayı

bolǵan d sanın saylap alıp $e = d^{-1}(\varphi(n))$ tabadı. Sońında bul n, d sanaların járiyalaydı, al e ni sır saqlaydı. Endi A abonenti elektron túrdegi xújjetlerge hám xabarlarǵa óz imzasın qoyıwǵa tayar boldı.

Meyli A abonenti $\bar{m} = m_1, m_2, ..., m_n$ xabarın imzalaw kerek bolsın. Onda ol dáslep $\bar{m}$ xabarına sáykes keliwshi y sanın tómendegishe esaplaydı hám onı xesh-funkciya dep ataymız, yaǵnıy:

$$y = h(m_1, m_2, ..., m_n)$$

y tı ózgertpey turıp $m_1, m_2, ..., m_n$ tiykarǵı teksti ózgeritiw ámeliy jaqtan múmkin emes. Sonlıqtan kelesi adımda A abonentin tek ǵana y sanın imzalaw jetkilikli hám bul imza barlıq $\bar{m}$ xabarına tiyisli boladı.

A abonentin

$$s = y^e (\mathrm{mod}\, n) \qquad (2.13)$$

sanın esaplaydı, yaǵnıy y sanın óziniń sırlı parametri menen dárejege kóteredi. Alınǵan s sanı elektron imza bolıp tabıladı. Ol $\bar{m}$ xabarına qosılıp

$$(\bar{m}, s) \qquad (2.14)$$

imzalanǵan xabardı qáliplestiredi.

A abonentininiń ashıq parametrlerin bilwshi hár bir abonent onıń imzasınıń haqıyıqıylıǵın tekserip eoriwi múmkin. Onıń ushın imzalanǵan (6) xabardı alıp, $h(\bar{m})$ xesh-funkciyanınıń mánisin hám

$$w = s^d (\mathrm{mod}\, n) \qquad (2.15)$$

esaplap, $w = h(\bar{m})$ teńliginiń orınlı bolatuǵınlıǵın tekseriw zárúr.

Eń ápiwayı xesh-funkciyanı «2 modulı boyınsha qosıw» ámeli járdeminde tómendegishe dúziw múmkin: kiriw qatar alınadı, onıń barlıq baytların 2 moduli boyınsha qosıp shıǵamız hám alınǵan nátiyje xesh-funkciyanıń mánisi sıpatında alıamız. Bul jaǵdayda xesh-funkciya mánisiniń uzınlıǵı kiriwshi xabardıń ólsheminen ǵárezsiz barlıq waqıtta 8 bitke teń boldı. Mısalı, tańbalı túrge keltirilgen kiriwshi maǵlıwmat (16 lıq formatta) 3E 54 A0

1F B4 túrinde bolsın. Onı ekilik túrge ótkerip, baytlardı bir birniń astına baǵana boyınsha jazıp 2 moduli boyınsha qosamız, sonda

0011 1110

0101 0100

1010 0000

0001 1111

1101 0100

0110 0101

Nátiyje (0110 $0101_{(2)}$ yamasa $65_{(16)}$) berilgen xabardıń xesh-funkciyasınıń mánisi boladı.

Tastıyıqlaw. Egerde imza haqıyqıy bolsa, onda $w = h(\overline{m})$

Dálilleniwi. (2.15), (2.13) hám RSA sxemasınıń qásiyetinen

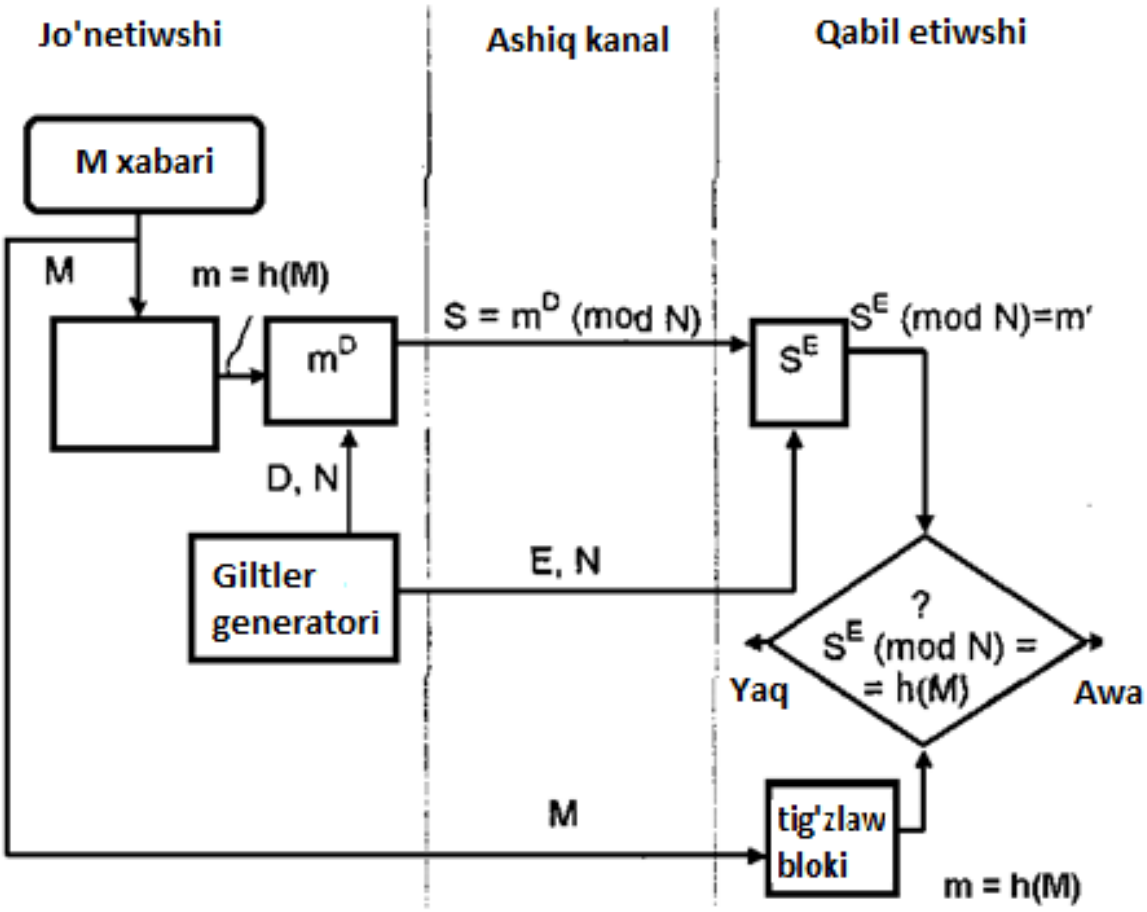
$$w = s^d (\mathrm{mod}\, n) = e^{ed} (\mathrm{mod}\, n) = y = h(\overline{m})$$

Tastıyıqlaw. Qarastırılǵan elektron imza oǵan qoyılǵan barlıq talaplardı qanaatlan,dıradı.

Dálilleniwi. Imzanıń birinshi qásiyetin tekseremiz. n sanın hesh kim ápiwayı kóbeytiwshilerge jikley almaydı. Sonlıqtan n, d bile otırıp e taba almaydı. Haqıyqattan da $e = d^{-1} (\mathrm{mod}\, \varphi(n))$ esaplawǵa $\varphi(n)$ biliw kerek, al onıń ushın ápiwayı kóbeytiwshiler bolǵan p hám q kerek.

Ekinshi qásiyet birinshiden kelip shıǵadı. Imzanıń avtorı imzadan bas tarıtıwı múkin emes, sebebi onıń atınan basqa hesh kim izanı jasawı múmkin emes.

Úshinshi qásiyette egerde kelispewshilik bolg'an jag'dayda sudta barlıq esaplawlardı tekserip ha'm haqıyqatlıqtı anıqlaw mu'kin.



__-su'wret

Mısalı. Meyli $p=5, q=11$, onda $n=5\cdot 11=55$, $\varphi(n)=40$. 40 sanı menen óz-ara ápiwayı bolǵan sandı $d=3$ dep saylap alayıq. Evklidtiń ulıwmalastırılǵan algorimti járdemiinde $e=3^{-1}(\mathrm{mod}\,40)=27$ tabamız.

$\bar{m}=abbbaa$ xabarı beillgen bolıp, onıń xesh-funkciyası 13 ke teń bolsın, yaǵnıy

$$y=h(abbbaa)=13$$

Bul jaǵdayda (5) boyınsha

$$s=13^{27}(\mathrm{mod}\,55)=7$$

esaplaydı hám $(abbbaa,7)$ imzanı dúzedi.

$(n,d)=(55,3)$ ashıq giltlerin bilgenler imzanıń haqıyılıǵın tekserip kóriwi múmikn. Imzalanǵan xabar alınǵannan soń tárarıy túrde xesh-funkciyanıń

mánisi esplanadı (egerde xabardıń mazmunı ózgermegen bolsa, onda xesh-funkciyanıń mánisi dáslepki mánis penen birdey boladı) hám (2.15) járdeminde

$$w = 7^3 (\mathrm{mod}\, 55) = 13$$

Demek mánisler bir-birine teń, onda imza haqıyqıy.

II-bapqa juwmaq

Bul bapta ashıq giltli shifrlaw bir tárepleme funciyalarǵa tiykarlanatuǵınlıǵı qarastırıldı. Mısal sıpatında sanlardı faktorizaciyalaw, diskret logarifmlew hám Diffi-Xelman máselesi keltirip ótildi. Bul máseleler arasında baylanıslar bar bolıp bir túrdegi máseleni ekinshi túrdegi máselege alıp keliw múmkin. RSA sisteması ashıq giltli kriptosistemalarınıń ishindegi eń keń tarqalǵanı bolıp, onıń esaplawǵa qarata qorǵanǵalıǵı RSA máselesiniń sheshiw qıyınshılıǵına tiykarlanadı. Al ol másele bolsa faktorizaciya máselesine uqsas bolıp, biraqta oǵan teń emes.

Elektron imza qısqa yamasa uzaq múddetke autentifikaciyanı támiyinleydi. Ol eki túrdegi sxema kórinisinde qollanıladı: imzalaw hám imzanı tekseriw. RSA shifrlaw algoritmin keri baǵıtta paydalanıp ashıq giltli imzalaw sxemasın alıwımız múmkin, biraqta bul algoritmdi xesh-funkciya menen birgelikte ámelge asırıw zárúr. Bunday etiw, imzalanıp atırǵan qısqa yamasa uzın xabarlardıń birdey turaqlılıǵın támiyinleydi.

III-BAP. Faktorizaciyalaw ma’selesine tiykarlanǵan kriptosistemalardıń programmalıq támiynatın jaratıw

1-§. RSA shifrlaw algoritminin’ programması

Usı programmalıq támiynattı jaratıwda zamanagóy programmalıq qurallarından paydalanıp jaratıw, olardıń múmkinshiliklerinen paydalanıw hám programmalıq qurallardıń universallıǵı, ápiwayılıǵı hám tarmaqta isley alatuǵın tárepleri úyrenilgen.

Microsoft Visual Studio 2010 programması Microsoft korporaciyasi tárepinen islep shıǵılǵan bolıp, ol programistler ushın arnalg’an. Bul programma járdeminde tómendegi programmalastırıw tillerinde programmalastırıwdı ámelge asırıw múmkin:

- Visual Basic .NET
- Visual C# .NET
- Visual C++ .NET
- Visual J# .NET

Microsoft Visual Studio 2010 programması járdeminde Windows ortalıǵı ushın, telefonlar ushın, tarmaqlar ushın, Web programmalardı jaratıw múmkin. Microsoft Visual Studio 2010 ortalıǵında Visual C#, Visual Basic, Visual J# tilleri járdeminde Web programmalardı hám Visual C#, Visual Basic, Visual J#, Visual C++ tilleri járdeminde Windows ortalıǵı ushın programmalar jaratıw múmkin.

Visual Basic. NET - Microsoft Visual Studio 2010 quramındaǵı eń natiyjeliligi joqarı programmalastırıw tillerden biri bolıp, bul programmalastırıw tilin tolıq obiektge bag’darlang’an programmalastırıw tili dep aytıwımız múmkin. Visual Basic. NET programmalastırıw tili járdeminde Windows programmaların hám Web programmaların jaratıw múmkin.

Visual C#. NET - Microsoft korporaciyasi tárepinen islep shıǵılǵan bolıp, bul programmalastırıw tili tiykarınan NET platformasi ushın islep shıǵılǵan. Visual C#. NET programmalastırıw tili múmkinshilikleri basqa obiektka

bag’darlang’an programmalastırıw tilleri (C, C++, Java hám Delphi) nen bir qansha keń bolıp, bul programmalastırıw tilinde Visual Basic. NET sıyaqlı Windows programmalar hám Web programmalar jaratıw múmkin.

Visual C++. NET programmalastırıw tili tómen dárejedegi programmist ushın programmalardı basqarıwda talap etiledi. .NET platformasınıń Visual C++ programmalastırıw tili basqa programmalastırıw tillerinen usı o’zgesheligi menen parıq etedi, bul programmalastırıw tili NET platformasining kodlı modeli hám Windows kodlı modelin qollap quwatlaydı.

Visual J#. NET - Microsoft. NET platformasi ushın Web-servis hám programmalar jaratıwshı Java-programmistleri isletiwi múmkin. Visual J#. NET programmalastırıw tili.

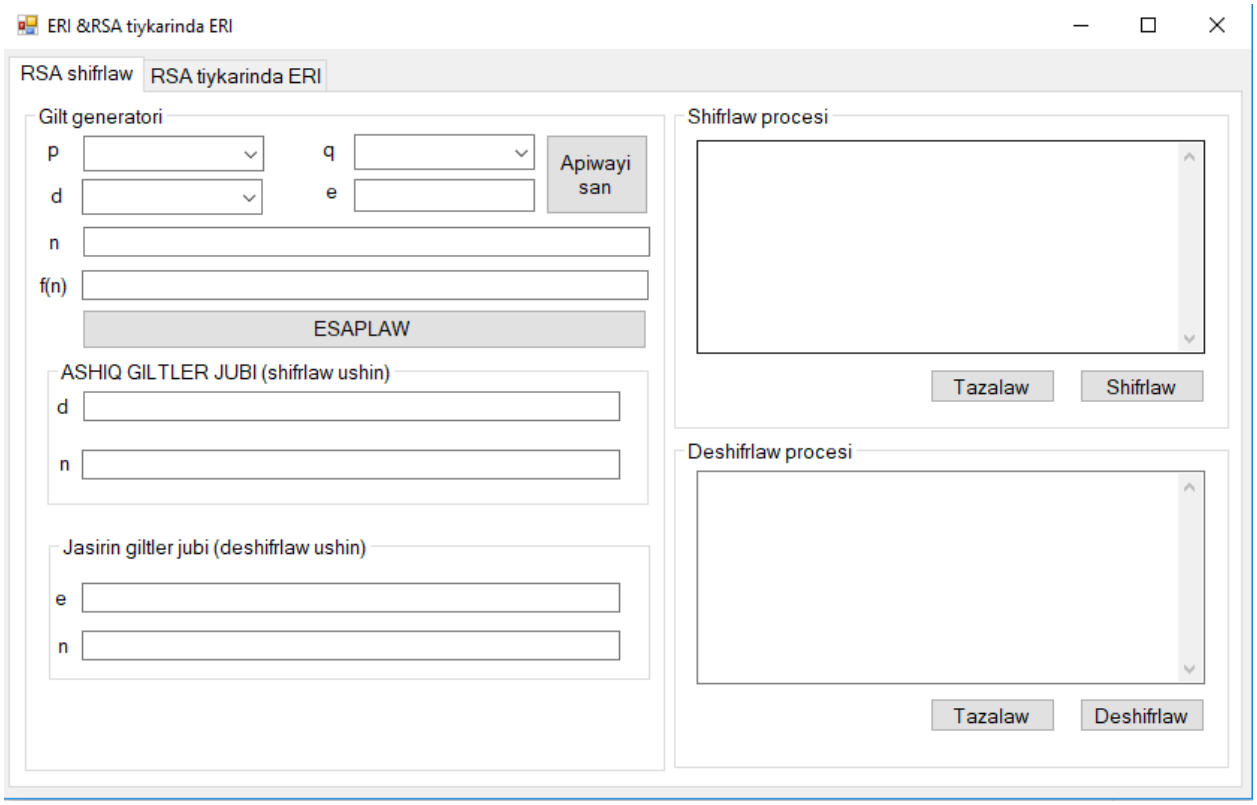
C# programmalastırıw tiliniń artıqmashılıq tárepleri sonnan ibarat, bul programmalastırıw tilinde júdá kóplep bibliotekalar bar. Bul bibliotekalar programmist ushın qolaylıq tuwdırıp qaymastan, soni’n’ menen birge olarg’a kem qáte islewge alıp keledi. C# programmalastırıw. NET Freamwork bibliotekalari’ menen isleydi.

Biz programmani’ dúziwde C# programmalastırıw tilinen paydalandıq. Bul programma Visual Studio ulıwmalıq paketine kiredi hámde Microsoft firması tárepinen islep shıǵılǵan. Sonıń menen bul programma tek Microsoft, Macintosh operacion ortalıqlarında isleydi. Bul programma islewi ushın bir qansha qosımsha programmalar kerek boladı. Mısalı eń: NET Freamwork programmasısız isley almaydı. Biz bul programmanıń aynalı (Windows Application) bóliminde dúzdik. C# programmalastırıw tili C klasi’ programmalarına kiredi. Sol sebepli onı C programmalastırıw tilin bilgen programmistke ol onsha qıyınshılıq tuwdi’rmaydi’. C# programmalastırıw tili C++ programmalastırıw tiliniń ıqshamlanǵan, paydalanıwshıǵa qolay kórinisinde shıǵarıldı. C++ programmalastırıw tilinde qolda jazılatuǵın programma bólimleri C# programmalastırıw tilinde avtomatik tárizde arnawlı buyrıqlar arqalı kirgizetuǵın boldı.

Islep shıǵılǵan programmalıq qural eki bólekten ibarat bolıp, olar tómendegishe:

- RSA shifrlaw algoritmı ;
- RSA algoritmi tiykarında ETI algoritmı.

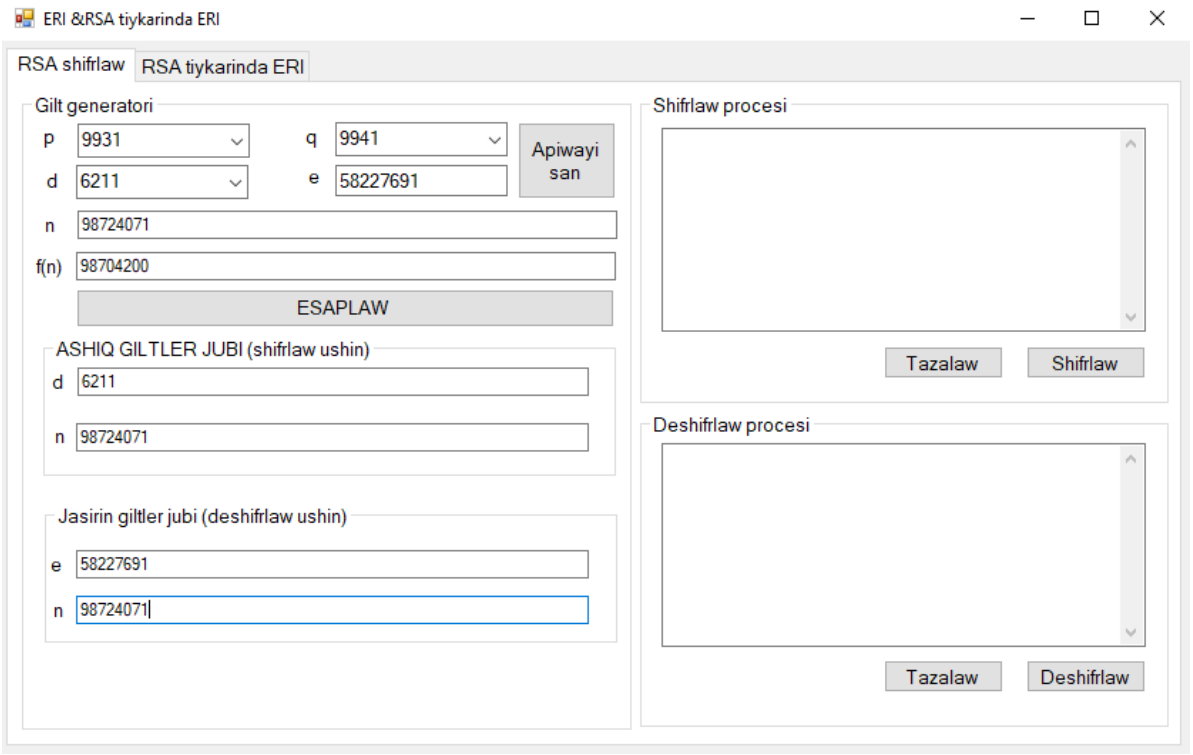
RSA shifrlaw algoritmı programması. Usı bólimde faktorizaciyalaw ma'selesine tiykarlanǵan hám házirde keń paydalanılıp atırǵan RSA ashıq giltli shifrlaw algoritminin' programmalıq quralı islep shıǵılǵan. Programmanıń ulıwma kórinisi tómendegishe:



3.1-súwret. Programmanıń ulıwma kórinisi

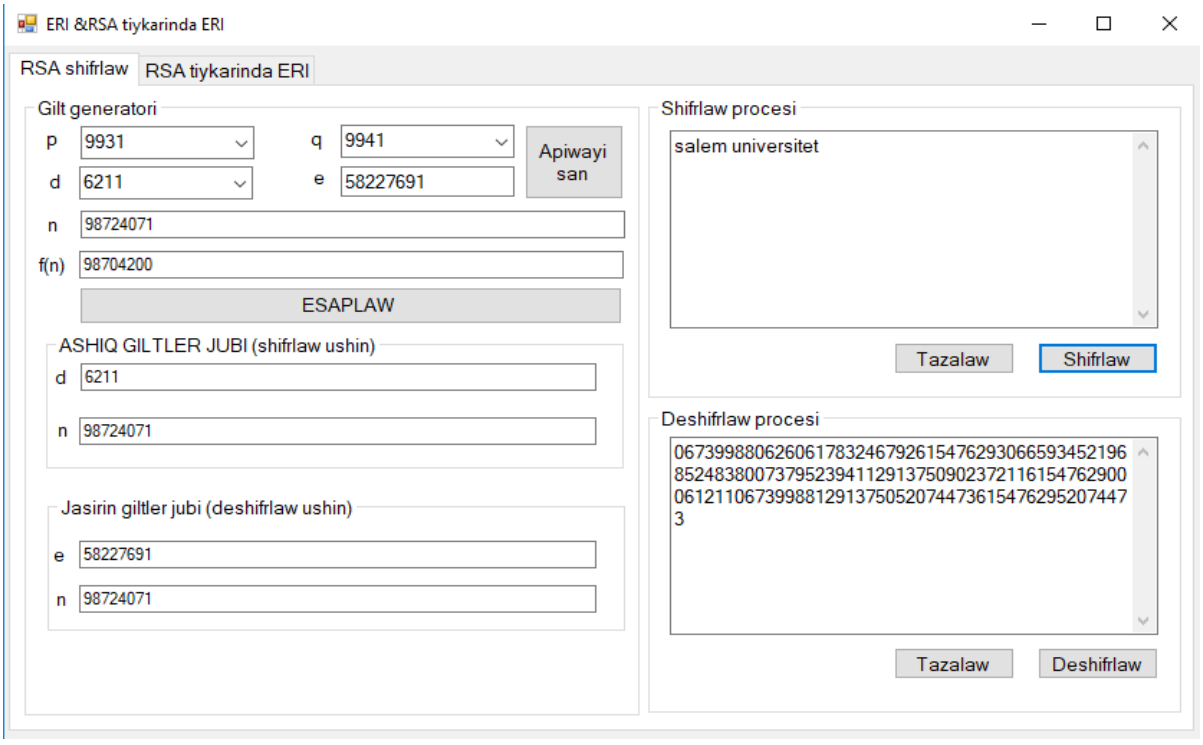
Programma tómendegi bo'limilerden ibarat :

1. *Gilt generatori bo'limi.* Usı bándte RSA shifrlaw algoritmi ushın kerekli bolǵan p,d hám d giltler avtomatik túrde payda etiledi. Onıń ushın "APIWAYI SAN" tuymesi basıladı. Nátiyjede hár birinde 6000-10000 arasındaǵı ápiwayi sanlar payda boladı. Usı sanlar tiykarında keyingi e,n hám $\varphi(n)$ shamaları esaplanadı. Bul ámel bolsa "ESAPLAW" tuymesin basıw arqalı ámelge asırıladı. Sonnan keyin "*Ashıq giltler jubı*" hám "*Jasırın giltler jubı*" punkti' sa'ykes túrde ashıq hám jasırın giltler jupli'gi'n payda etiledi.



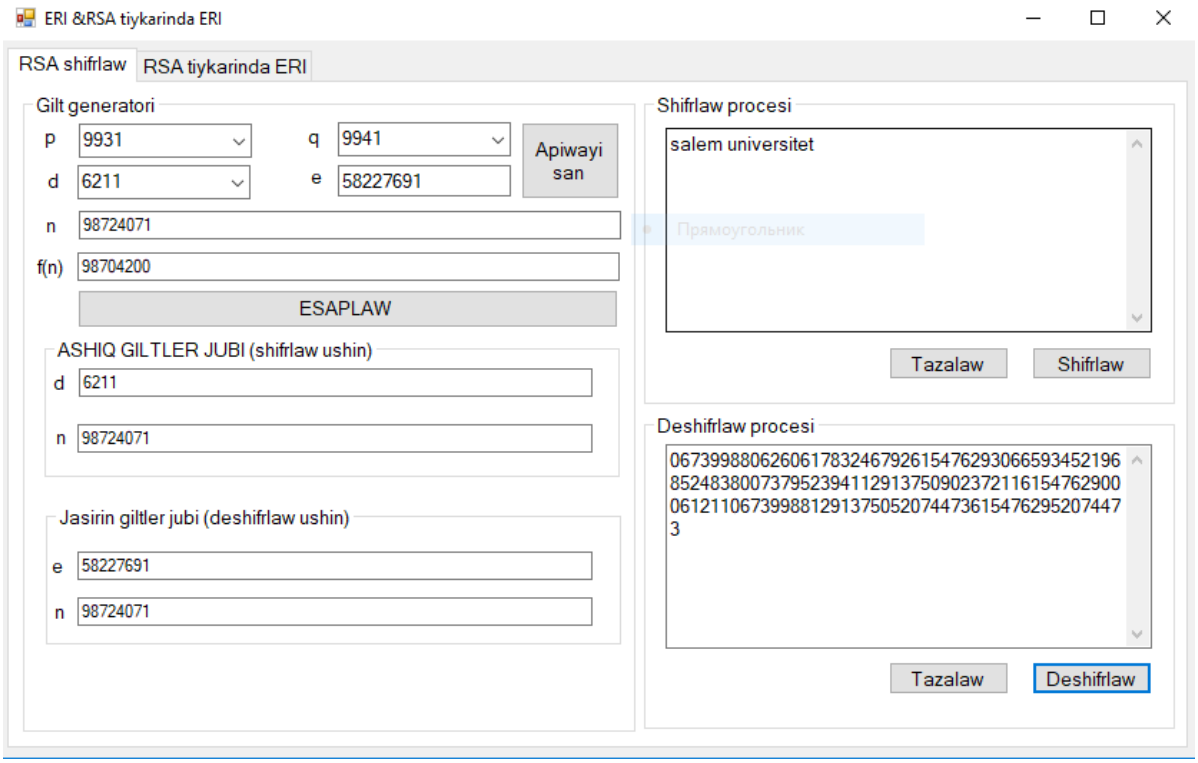
3.2-súwret Gilt generaciyası

2. *Shifrlaw procesi bo'limi*. Usı bo'limide jaratılǵan giltler tiykarında kiritilgen tekstti shifrlaw kórip ótiledi. Mısal ushın jaratılǵan gilt penen "sálem universitet" tekstin shifrlap kóremiz. Payda bolǵan shifr tekst bolsa deshifrlaw procesi bo'limi aynasında payda boladı.



3.3-súwret. Shifrlaw procesi

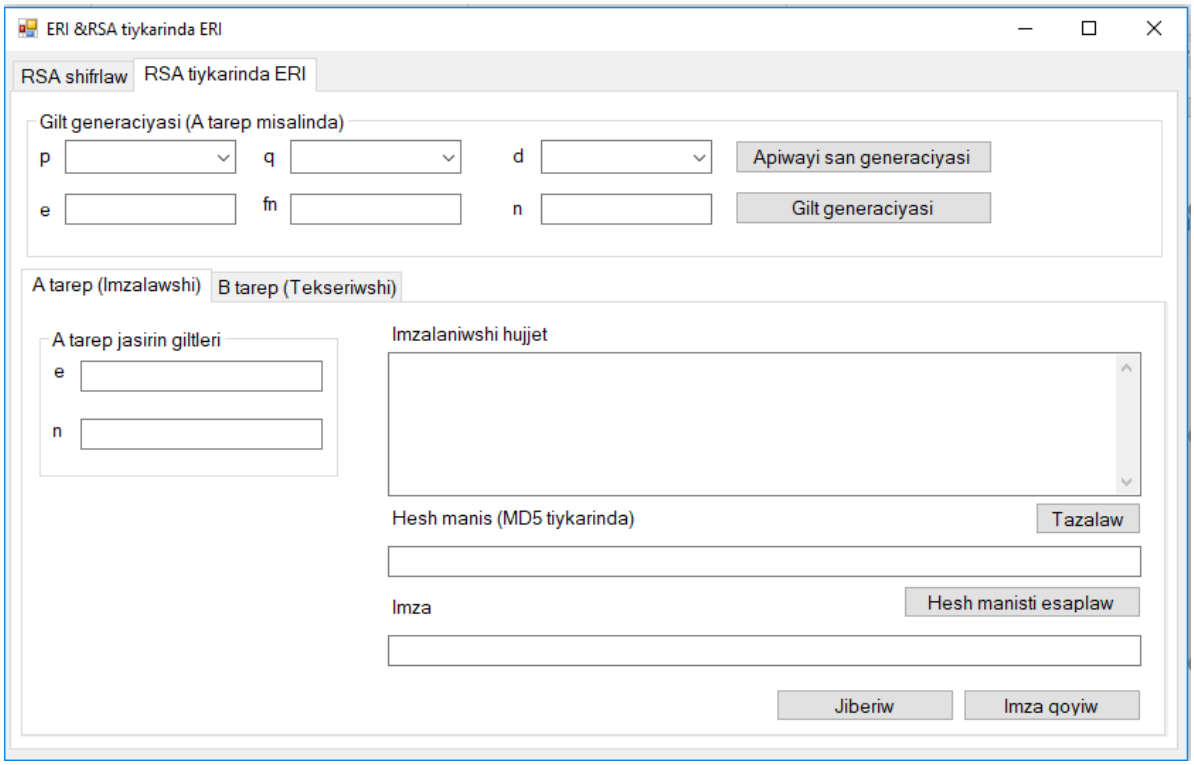
3. *Deshifrlaw procesi bo'limi*. Usı bo'limde payda etilgen shifr tekstti ashıq tekstke aylandırıw máselesi kórip shıǵıladı. Onıń ushın "Shifrlaw procesi" bo'limi aynası tazalanadı. Onıń ushın "Tazalaw " tuymesi basıladı hám "Deshifrlaw procesi" bo'limi ndegi "Deshifrlaw" tuymesi basıladı hám "Shifrlaw procesi" bo'limi aynasıda ashıq tekst payda boladı.



3. 4-súwret. Deshifrlaw procesi

2-§. RSA algoritmine tiykarlanǵan ETI algoritmi programması

Programmanıń ekinshi bólegi RSA shifrlaw algoritmi tiykarında islep shıǵılǵan ETI algoritmi bolıp tabıladı. RSA tiykarında ETI algoritmi shifrlawdan tek giltler menen parıq etedi. Yaǵniy, imza qoyıwda jasırın gilt hám imzani' tekseriwde ashıq giltten paydalanıladı. Programmanıń ulıwma kórinisi tómendegishe:

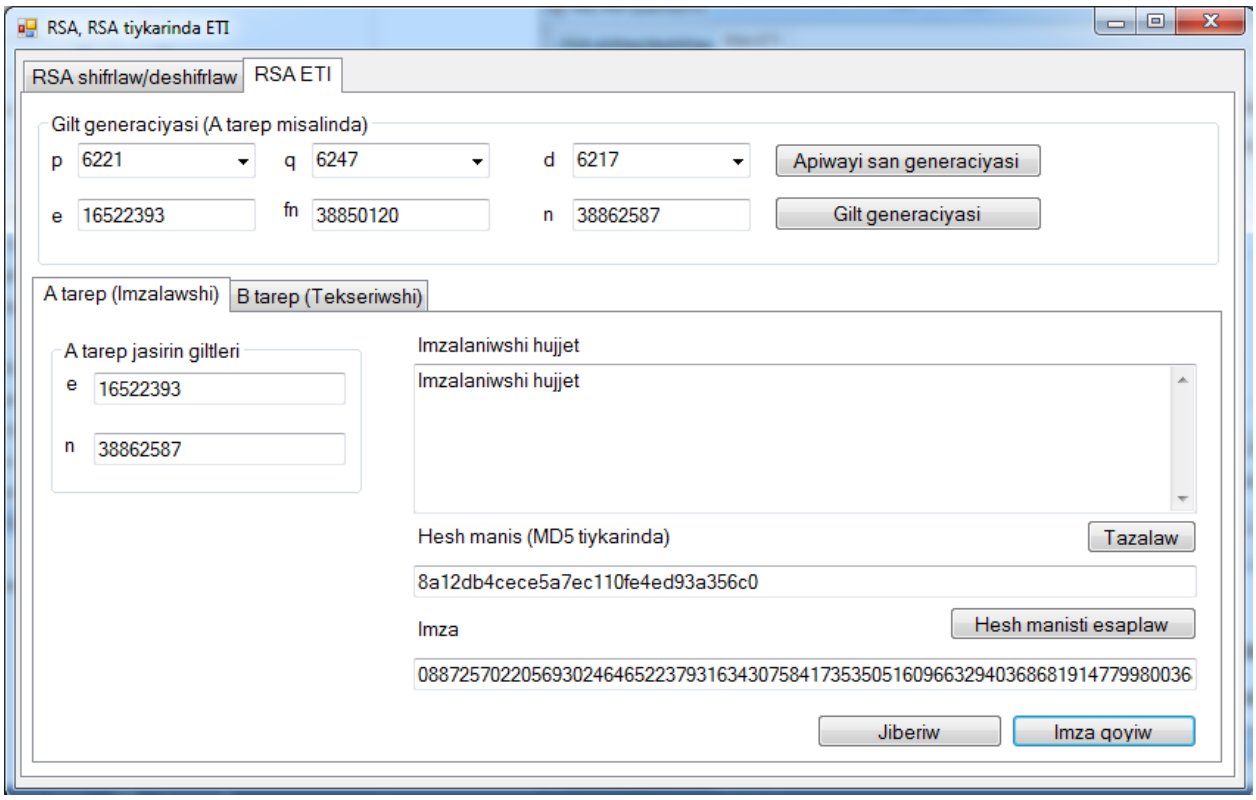


3. 5-súwret. ETI imza algoritmi

ETI imza algoritmleri tómendegi bo'limlerden ibarat :

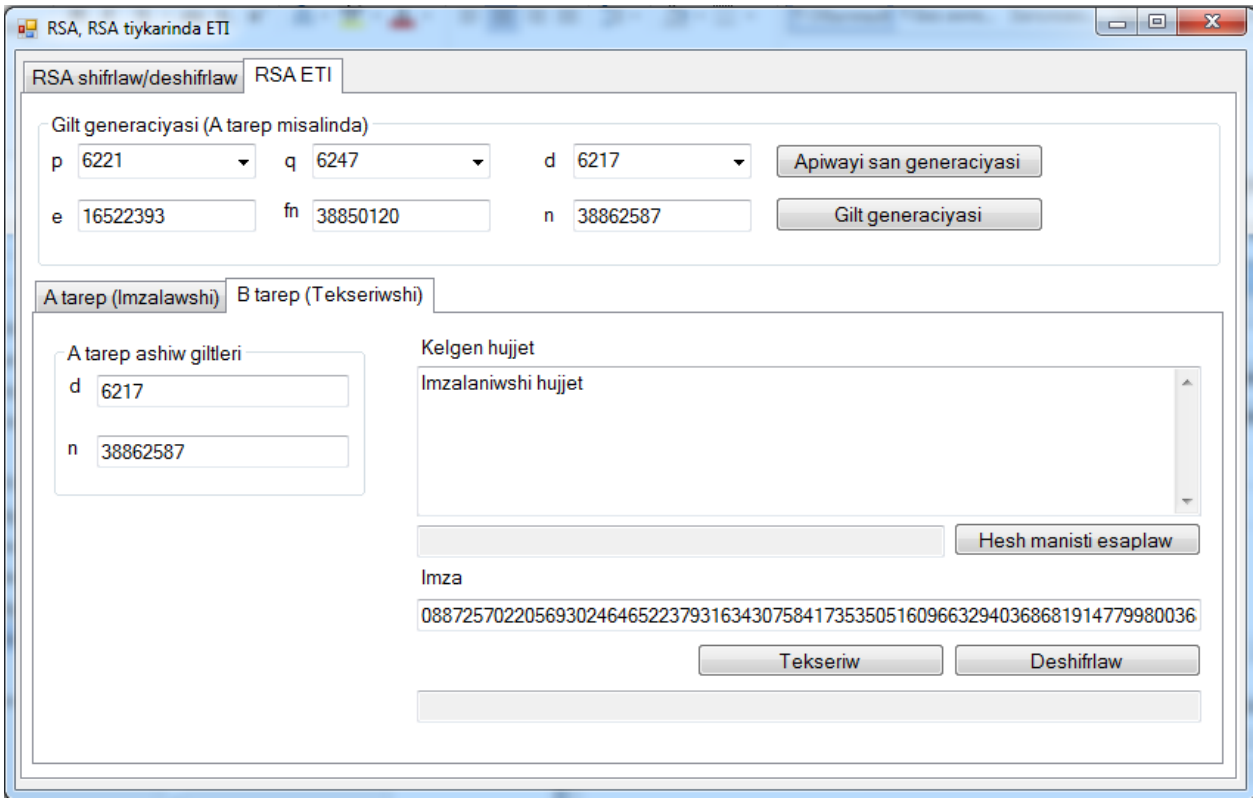
1. *Giltler generaciyasi bo'lim*. Usı bo'lim shifrlaw programması bo'lim menen birdey bolıp, ol jaǵdayda gilt generaciyasi ámeli atqarıladı.

2. *A abonent (imzalawshi).* Usı bo'limde jaratılǵan jasırın gilt penen avtor tárepinen hújjet imzalanadi. Onıń ushın "Imzalanıwshi hújjet" bo'limine imzalanıwshi tekstti kirgiziw jáne onıń xesh ma`nisin alıw shárt. Xesh ma`nisin esaplawda MD5 xesh algoritminen paydalanıladı. Bul algoritm ótken ásirdiń 90-jıllırındı MD4 xesh-funkciyasın jetilistiriw nátiyjesigde payda bolıp, olardıń avtorı R. Rivest bolıp abıladı. Xabarǵa MD5 ti qollanıw nátiyjesinde 128 bitli xesh-mánis alınadı. Algoritmde elementar logikalıq ámeller (inversiya, konyunkciya, 2 moduli boyınsha qosıw, cikllıq jıljıw h.t.b), jánede ápiwayı arifmetikalıq qosıw ámeli qollanıladı. Alınǵan xesh-mánistiń hár bir bitı hár bir kiriwshi bitten alınǵan funkciya boadı. 128-bitli xesh-mánislerdi alıw ushın MD5 ti júdá kúshli xesh-funkciya dep esaplaydı. Sondan keyin "*Imza qoyıw* " tuymesi basıladı hám B abonentke jiberiw ushın "*Jiberiw*" tuymesi basıladı. Tómende giltlerdi jaratıw hám imza qoyıw processleri keltirilgen.



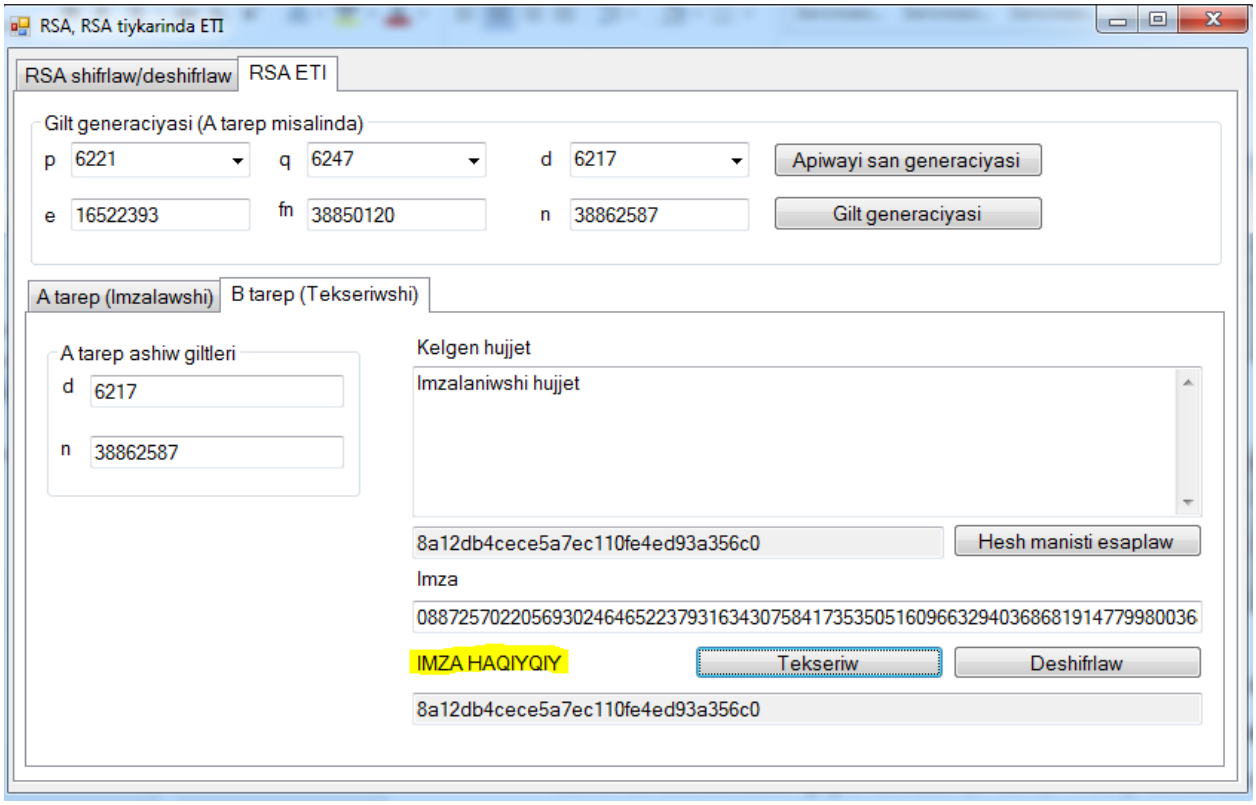
3.6 -súwret. Imza qoyıw procesi

3. *B abonent (Tekseriwshi).* Usı ayna B abonent tárepinen ámelge asırıladı hám ol jaǵdayda kelgen maǵlıwmatlar tómendegilerden ibarat boladı.



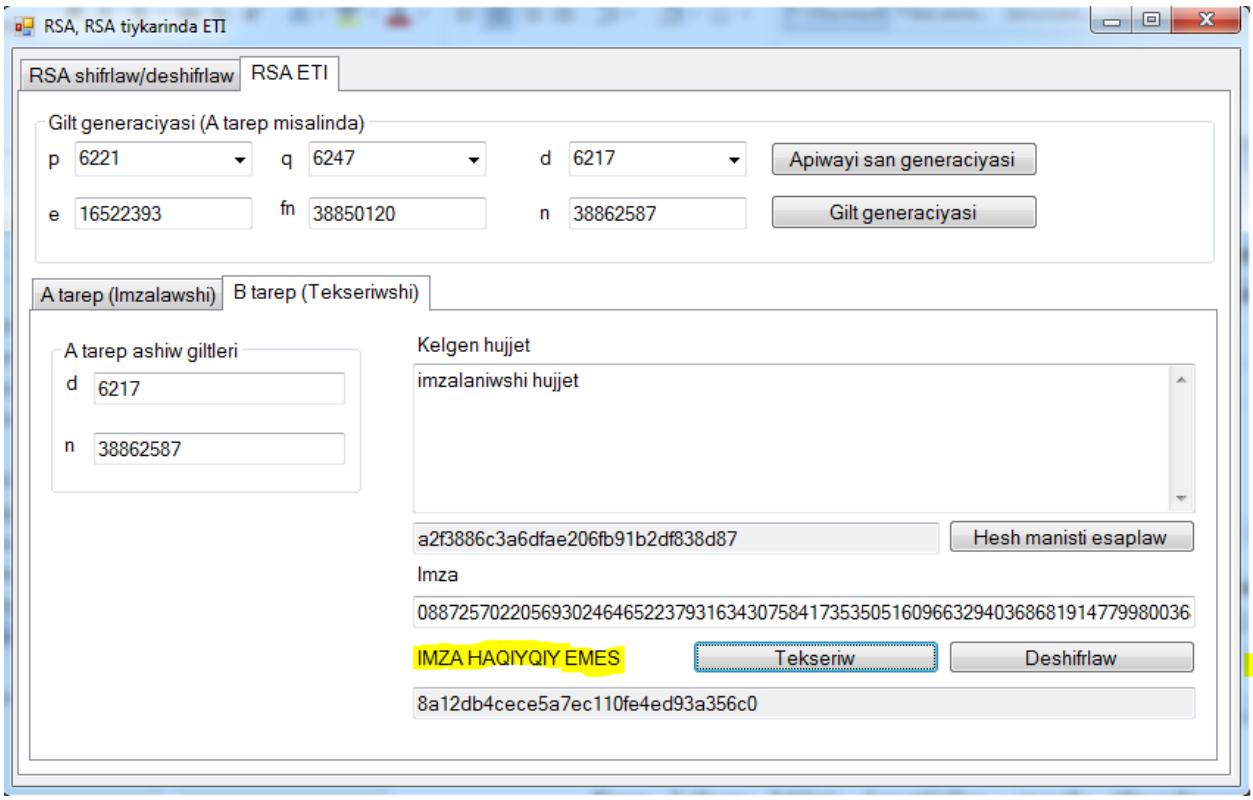
3.7-súwret. Deshifrlaw aynası

Suwretde kórip ótilgenindey, kelgen maǵlımatlar tekst hám oǵan qoyılǵan imzadan ibarat. Usı imzanı tekseriwde B tárep A táreptin' ashıq giltinen paydalanıladı. Imzanı tekseriw ushın B tárep kelgen maǵlımatti xesh ma`nisin aladı. Onıń ushın B tárep "*Xesh mánisti esaplaw* " tuymesin basadı. Kelgen imzanı ashıw ushın bolsa "*Deshifrlaw*" tuymesi basıladı. Ashılǵan imza hám payda etilgen xesh mánisti salıstırıw ushın "*Tekseriw*" tuymesi basıladı. Sonda tekseriw aynası qasında nátiyje kórinedi (Imza haqıyqıy yamasa haqıyqıy emes degen xabar). Tómende kelgen imzani tekseriw procesi keltirilgen.



3.8-súwret. Imzanı tekseriw procesi

Eger kelgen hújjet ózgertirilse, mısalı "Imzalanıwshı hújjet" ornına "imzalanıwshı hújjet" teksti kiritiledi. Bunda tek bas háripler úlken kishiliginen parıq etedi (I hám i). Usı jaǵdayda alınǵan nátiyje tómendegishe boladı :



3.9 -súwret. Qoldı tekseriw

Usı suwretten, kelgen tekstti tek bir bayt ózgeriwi pútkil qoyılǵan imzani haqıyqıy emesligine alıp keletug'inli'g'i'n kóremiz.

III-bapqa juwmaq

II-bapta qarastırılǵan asimmetriyalı algoritmdi realizaciyalaw maqsetinde Vsual Studio ortalığında C++ tilinde aynalı interfeys jaratıw etapların qarap óttik. Bul jerde programmalastırıw tiliniń ikmniyatlarınan nátiyjeli paydalanıldı. Kriptosistemada zárúrli bolǵan ápiwayı sanlar programma járdeminde generaciyalandı. Paydalanıwshı sol sanlardıń ishinen ózine maqul kórgenin saylap alıadı, al qalǵan parametrlerdi programmanıń ózi saylap alıwı názerde tutıldı.

Juwmaqlaw

Jaratılıwna bir qansha waqıt bolǵanı menen, RSA algoritmi elege shekem ashıq giltli algoritmlerdiń arasında eń isenimli hám eń keń kóp tarqalǵan kriptosistemalardıń biri bolıp esaplanadı. Onıń tiykarında kóplegen jańa texnologiyalar jaratılǵan. Sonlıqtan RSA algoritminiń kemshiliklerin anıqlaw asimmetriyalı shifrlaw algoritmin paydalanıwshı, atap aytqanda bank sistemaları hám elektron kommerciyadağı hár qıylı shifrlaw algoritmleriniń “qulawına” alıp keliwi múmkin.

Kriptosistemalardı dúziw usılların úyreniw menen birgelikte olardı buzıw múmkin bolǵan jolların da birgelikte úyreniw zárúr. Bul kriptografiyalıq sistemalardıń ázzi táreplerin bahalaw ushın zárúr bolıp esaplanadı. Hár bir sistemanı ashıw ushın islengen is háreketlerdiń tiykarında matematikalıq usıllar jatadı. Olardı bile otırıp biz elede quramalı hám turaqlı bolǵan sistemalardı dúziwimiz múmkin. Biraqta ilimde bolıp atırǵan jańalıqlar, yaǵnıy esaplaw texnikasınıń rawajlanıw tendenciyaları, sonıń menen birgelikte hár qıylı esaplaw algoritmlerdiń payda bolıwı hám bar bolǵanlarınıń jetilistiriliwleri elede hár tárepleme jetilisken kriptosistemalardı dúziw kerek ekenligin ańlatadı.

Dissertaciyada informaciyalardı qorǵaw tarawındaǵı eń aktual mashqalalardan biri bolǵan asimmetriyalı kriptosistemalardaǵı RSA algoritmi qaraladı.

Bul magistrlik dissertaciya jumısı úsh baptan ibarat bolıp, birinshi bap kriptografiya haqqında tiykarǵı túsiniklerberiplip, simmetriyalı hám asimmetriyalı kriptosistemalardı úyretiw hám olaraǵa tiyisli bolǵan algorimtler háqqında sóz etiledi.

Ekinshi bapta faktorizaciyalaw máselesine tiykarlanǵan kriptografiyalıq sistemalar bolǵan algoritmdi úyreniw wazıypaları keltirilgen. Bul bapta matematikadaǵı ayırım klassikalıq teorema hám anıqlamalar keltirip ótilgen. Ámeliy jaqtan bekkemlew ushın mısallar islengen. Birinshi asimmetriyalı

kriptosistema bolǵan RSA algoritminiń maǵlıwmatlardı shifrlaw hám olardı imzalaw algoritmleri úyrenip shıǵıldı.

Úshinshi bapta RSA algoritmi tiykarında maǵlıwmatlardı shifrlaw hám imzalawdı ámelge asırıwshı programmalıq támiynattı islep shıǵıwǵa qaratılǵan. Visual Studio 2010 otralığında islep shıǵılǵan programmalıq ónimi qolaylı interfeyske iye bolıp, onı bakalavr baǵdarındaǵı “Informaciyalardı qorǵaw” pániniń ámeliy hám laborotoriya sabaqlarında hár túrli eksperimentler ótkeriw maqsetinde qollanılıwı múmkin. Jaratılǵan programma ónimi hám ol arqalı alınǵan natiyjeler dissertaciya jumısında maqsetke erisilgenligin kórsetedi.

Paydalanǵan ádebiyatlar dizimi

I. ÓZBEKISTAN RESPUBLIKASÍNÍŃ NÍZAMLARÍ

1. O`zbekiston Respublikasi Konstitutsiyasi Toshkent, «O`zbekiston», 16-aprel` 2014-yil.
2. O`zbekiston Respublikasi Prezidentining PQ-1836-son qarori asosida “Axborot – kommunikatsiya texnologiyalarini joriy etish va rivojlantirish to`g`risida”gi farmoni. 23-oktyabr` 2012 yil.
3. O‘zbekiston Respublikasining “Axborotlashtirish to‘g‘risida”gi Qonuni 2003 yil 11 dekabr`, 562–II-son
4. O‘zbekiston Respublikasining “Elektron raqamli imzo to‘g‘risida”gi Qonuni 2003 yil 11 dekabr`, 562–II-son
5. O‘zbekiston Respublikasining “Elektron hujjat aylanishi to‘g‘risida”gi Qonuni 2004 yil 29 aprel`, 611-II-son
6. O‘zbekiston Respublikasi Prezidentining 2018 yil 13 dekabrdagi “O‘zbekiston Respublikasi davlat boshqaruviga raqamli iqtisodiyot, elektron hukumat hamda axborot tizimlarini joriy etish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi PF-5598-son Farmoni
7. O‘zbekiston Respublikasi Prezidentining "O‘zbekiston Respublikasida axborotni kriptografik muhofaza qilishni tashkil etish chora-tadbirlari to‘g‘risida”gi Qarori 2007 yil 3 aprel`, PQ-614-son

II. ÓZBEKISTAN RESPUBLIKASÍ PREZIDENTI SHÍǴARMALARÍ

8. Mirziyoyev Sh.M. Qonun ustuvorligi va inson manfaatlarini ta’minlash – yurt taraqqiyoti va xalq farovonligining garovi. Toshkent-“O’zbekiston” -2017
9. Mirziyoyev Sh.M. Tanqidiy tahlil, qat'iy tartib-intizom va shaxsiy javobgarlik – har bir rahbar faoliyatining kundalik qoidasi bo'lishi kerak. Toshkent-“O’zbekiston” -2017
10. Mirziyoyev Sh.M. Erkin va farovon, demokratik o‘zbekiston davlatini birgalikda barpo etamiz. Toshkent-“O’zbekiston” -2017

III. TIYKARǴÍ ÁDEBIYATLAR

11. Вельшенбах М. Криптография на Си и С++ в дейтвии. Учебное пособие. М., Изд. Триумф. 2004, 464с.
12. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. М., Постмаркет, 2001, 328с.
13. Коблиц Н. Курс теории чисел и криптографии. М., Научное издательство ТВП. 2001, 254с.
14. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. М., Горячая линия–Телеком. 2005, 209с.
15. Смарт Н. Криптография. М., Техносфера. 2005, 528с.
16. Харин Ю. С., Берник В. И., Матвеев Г. В., Агиевич С. В. Математические и компьютерные основы криптологии. Мн., Новое знание. 2003, 382с.
17. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. М., Изд.Триумф. 2002, 616с.

IV. QOSÍMSHA ÁDEBIYATLAR

18. Аграновский А.В., Хади Р.А. Практическая криптография: алгоритмы и их программирование. М. САЛОН-Пресс, 2009, 256с.
19. Арипов М., Пудовченко Ю.Е. Основы криптологии. Ташкент. НУУз им. М.Улугбека. 2004, 136с.
20. Баричев С.Г., Серов Р.Е. Основы современной криптографии. М., Горячая линия-телеком. 2001, 152с.
21. Ростовцев А.Г., Маховенко Е. Б. Теоритическая криптография. С-П., Профессионал. 1994, 486с.

V. ILIMIY JURNALLARDAǴÍ MAQALALAR

22. VII INTERNATIONAL CORRESPONDENCE SCIENTIFIC SPECIALIZED CONFERENCE «INTERNATIONAL SCIENTIFIC REVIEW OF THE TECHNICAL SCIENCES, MATHEMATICS AND COMPUTER SCIENCE» (Boston. USA. November 11-12, 2018) ОБЗОР К ВОПРОСУ АЛГОРИТМА RSA ДЛЯ ШИФРОВАНИЯ ИНФОРМАЦИИ Балтабаев Ж.Е. (Республика Узбекистан)
23. ВЕСТНИК НАУКИ И ОБРАЗОВАНИЯ 2019. № 23 (77).Часть 2

ИЗУЧЕНИЕ ПРОБЛЕМЫ ФАКТОРИЗАЦИИ ПАРАМЕТРА N В АЛГОРИТМЕ RSA С ПОМОЩЬЮ СИСТЕМЫ «MATHEMATICA»

Бердимуратов М.К. Ибрагимов К.И. Балтабаев Ж.Е

VI. INTERNET MATERIALLARÍ HÁM SAYTLARÍ

22. http://intuit.ru/. Интернет-Университет Информационных Технологий.
23. http://mf.grsu.by/. Гродненский госуниверситет им. Янки Купалы.
24. http://infoch.info/index.php. Мир защиты информации.
25. http://software.intel.com/ru-ru/. Intel® Software Network.
26. http://kek.ksu.ru/Student/Crypto/Main.htm
27. http://cryptography.ru/. Сайт учрежден Московским университетом им. М. В. Ломоносова и ООО “Умище”.
28. http://Lex.uz.

Qosımsha

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;
using System.Numerics;
using System.Security.Cryptography;

namespace RSA
{
   public partial class Form1 : Form
   {
      public Form1()
      {
         InitializeComponent();
      }
      private Int64 p,q,d;
      private void button1_Click(object sender, EventArgs e)
      {
         p=Convert.ToInt64(comboBox2.SelectedItem);
         q=Convert.ToInt64(comboBox1.SelectedItem);
         d = Convert.ToInt64(comboBox3.SelectedItem);
         Int64 n = q * p;
         textBox3.Text = n.ToString();
         Int64 fn=(q-1)*(p-1);
         textBox4.Text = fn.ToString();
         Int64 E = eyler(fn, d);
         textBox5.Text = E.ToString();
         textBox9.Text = d.ToString();
         textBox11.Text = n.ToString();
         textBox10.Text = E.ToString();
         textBox12.Text = n.ToString();

      }
      private Int64 eyler(Int64 fn, Int64 d)
      {
         Int64[] u = { fn, 1, 0 };
         Int64[] v = { d, 0, 1 };
```

```
    Int64[] t = new Int64[3];
    Int64 result=0;
    while(v[0]!=0)
    {
        Int64 q = u[0] / v[0];
        t[0]=u[0]%v[0];
        t[1]=u[1]-q*v[1];
        t[2]=u[2]-q*v[2];
        u[0]=v[0];
        u[1]=v[1];
        u[2]=v[2];
        v[0]=t[0];
        v[1]=t[1];
        v[2]=t[2];
    }
    if(u[2]<0){result=fn+u[2];}
    else { result=u[2];}
    return result;

}
private readonly Encoding enc = Encoding.ASCII;
private void button2_Click(object sender, EventArgs e)
{
    //textBox8.Text = "";
    //double dareje, qaldiq = 1;
    //long N = Convert.ToInt32(textBox11.Text);
    //string text = textBox7.Text;
    //for (int i = 0; i < text.Length; i++)
    //{
    //    double sani = Convert.ToChar(text[i]);
    //    int D = Convert.ToInt32(textBox9.Text);
    //    for (int j = 1; j <= D; j++)
    //    {
    //        dareje = qaldiq * sani;
    //        qaldiq = dareje % N;
    //    }
    //    string tanba = qaldiq.ToString();
    //    int l = 0;
    //    for (int s = 0; s < textBox11.TextLength; s++)
    //    {
    //        if (tanba.Length + l == textBox11.TextLength)
    //        { textBox8.Text += qaldiq.ToString(); break; }
    //        else
    //        { textBox8.Text += "0"; l++; }
    //    }
```

```
            //    qaldiq = 1;
            //}
            textBox8.Text =
encryption(textBox7.Text,Convert.ToInt16(textBox9.Text),Convert.ToInt32(tex
tBox11.Text));
        }
        public string encryption(string plain_text, long dd, long nn)
        {
          string result = "";
           double dareje, qaldiq = 1;
           long N = nn;// Convert.ToInt32(textBox11.Text);
           string text = plain_text;
           for (int i = 0; i < text.Length; i++)
           {
              double sani = Convert.ToChar(text[i]);
              long D = dd;
              for (int j = 1; j <= D; j++)
              {
                 dareje = qaldiq * sani;
                 qaldiq = dareje % N;
              }
              string tanba = qaldiq.ToString();
              int l = 0;
              for (int s = 0; s < nn.ToString().Length; s++)
              {
                 if (tanba.Length + l == nn.ToString().Length)
                 { result += qaldiq.ToString(); break; }
                 else
                 { result += "0"; l++; }
              }
              qaldiq = 1;
           }
           return result;
        }
        public string decryption(string dec_text, long ee, long nn)
        {
          string result = "";
           string DeshifrText = dec_text;
           int g = 0;
           string sanesh = textBox12.Text;
           long N = nn;
           long E = ee;
           string jaz = "";
           double[] massiv = new double[DeshifrText.Length /
nn.ToString().Length];
```

```
            for (int y = 0; y < DeshifrText.Length; y++)
            {
                jaz += DeshifrText[y];
                if (jaz.Length == nn.ToString().Length)
                {
                    massiv[g] = Convert.ToDouble(jaz);
                    jaz = "";
                    g++;
                }
            }
            double dareje;
            double qaldiq = 1;
            for (int i = 0; i < g; i++)
            {

                for (int j = 1; j <= E; j++)
                {
                    dareje = qaldiq * massiv[i];
                    qaldiq = dareje % N;
                }
                string sanaw = Convert.ToChar(Convert.ToInt32(qaldiq)).ToString();
                result += sanaw;
                qaldiq = 1;
            }
            return result;
        }

        private void button3_Click(object sender, EventArgs e)
        {
            textBox7.Text = decryption(textBox8.Text,
Convert.ToInt32(textBox10.Text), Convert.ToInt32(textBox12.Text));
        }

        private void button4_Click(object sender, EventArgs e)
        {
            textBox7.Clear();

        }

        private void button5_Click(object sender, EventArgs e)
        {
             textBox8.Clear();
        }

        private void button6_Click(object sender, EventArgs e)
```

```
{
        int j = 1, pi = 6000;
        for (int i = 6000; i < 10000; i++)
        {
            for (int k = 1; k < (pi + 1) / 2; k++)
            {
                if (pi % k == 0) j++;
                if (j > 2) break;
            }
            if (j > 2) j = 1;
            else
            {
                comboBox1.Items.Add(pi);
                comboBox2.Items.Add(pi);
                comboBox3.Items.Add(pi);
            }
            pi++;
        }

}

private void button7_Click(object sender, EventArgs e)
{
    int j = 1, pi = 6000;
    for (int i = 6000; i < 10000; i++)
    {
        for (int k = 1; k < (pi + 1) / 2; k++)
        {
            if (pi % k == 0) j++;
            if (j > 2) break;
        }
        if (j > 2) j = 1;
        else
        {
            comboBox4.Items.Add(pi);
            comboBox5.Items.Add(pi);
            comboBox6.Items.Add(pi);
        }
        pi++;
    }
}

private void button8_Click(object sender, EventArgs e)
{
    p = Convert.ToInt64(comboBox5.SelectedItem);
```

```
            q = Convert.ToInt64(comboBox4.SelectedItem);
            d = Convert.ToInt64(comboBox6.SelectedItem);
            Int64 n = q * p;
            textBox6.Text = n.ToString();
            Int64 fn = (q - 1) * (p - 1);
            textBox2.Text = fn.ToString();
            Int64 E = eyler(fn, d);
            textBox1.Text = E.ToString();
            textBox19.Text = d.ToString();
            textBox18.Text = n.ToString();
            textBox13.Text = E.ToString();
            textBox14.Text = n.ToString();
        }
        private static string MD5hash(string data)
        {
            byte[] bytes = Encoding.Unicode.GetBytes(data);
            MD5CryptoServiceProvider hashstring = new
MD5CryptoServiceProvider();
            byte[] hash = hashstring.ComputeHash(bytes);
            string hashString = string.Empty;
            foreach (byte x in hash)
            {
                hashString += String.Format("{0:x2}", x);
            }
            return hashString;
        }
        private void button10_Click(object sender, EventArgs e)
        {
            string text = textBox15.Text;
            string hesh = MD5hash(text);
            textBox16.Text = hesh;

        }

        private void button11_Click(object sender, EventArgs e)
        {
            textBox17.Text = encryption(textBox16.Text,
Convert.ToInt32(textBox13.Text), Convert.ToInt32(textBox14.Text));
        }

        private void button12_Click(object sender, EventArgs e)
        {
            textBox20.Text = textBox17.Text;
            textBox21.Text = textBox15.Text;
```

```
        }

        private void button14_Click(object sender, EventArgs e)
        {
            textBox22.Text = MD5hash(textBox21.Text);
        }

        private void button13_Click(object sender, EventArgs e)
        {
            string shifr = textBox20.Text;
            long d = Convert.ToInt32(textBox19.Text);
            long n = Convert.ToInt32(textBox18.Text);
            textBox23.Text = decryption(shifr, d, n);

        }

        private void button15_Click(object sender, EventArgs e)
        {
            if (textBox22.Text == textBox23.Text)
            {
                label26.Text = "IMZA HAQIYQIY";
            } else {label26.Text="IMZA HAQIYQIY EMES";}
        }

        private void comboBox2_SelectedIndexChanged(object sender, EventArgs
e)
        {

        }

        private void tabPage4_Click(object sender, EventArgs e)
        {

        }

        private void button9_Click(object sender, EventArgs e)
        {
            textBox15.Clear();
        }
    }
}
```

VII INTERNATIONAL CORRESPONDENCE SCIENTIFIC SPECIALIZED CONFERENCE «INTERNATIONAL SCIENTIFIC REVIEW OF THE TECHNICAL SCIENCES, MATHEMATICS AND COMPUTER SCIENCE»

INTERNATIONAL SCIENTIFIC REVIEW

PROBLEMS OF SCIENCE

ISBN 978-1-948507-58-5

SCIENTIFIC ELECTRONIC LIBRARY LIBRARY.RU

Google scholar

HTTPS://SCIENTIFIC-CONFERENCE.COM

LIBRARY OF CONGRESS (USA)

VII INTERNATIONAL CORRESPONDENCE SCIENTIFIC SPECIALIZED CONFERENCE

INTERNATIONAL SCIENTIFIC REVIEW OF THE TECHNICAL SCIENCES, MATHEMATICS AND COMPUTER SCIENCES

Boston. USA. November 11-12, 2018

ISBN 978-1-948507-58-5
UDC 08

VII INTERNATIONAL CORRESPONDENCE SCIENTIFIC SPECIALIZED CONFERENCE «INTERNATIONAL SCIENTIFIC REVIEW OF THE TECHNICAL SCIENCES, MATHEMATICS AND COMPUTER SCIENCE»

(Boston. USA. November 11-12, 2018)

BOSTON. MASSACHUSETTS
PRINTED IN THE UNITED STATES OF AMERICA
2018

SYSTEM ANALYSIS, MANAGEMENT AND INFORMATION PROCESSING

THE REVIEW TO QUESTION OF RSA ALGORITHM FOR ENCIPHERING OF INFORMATION

Baltabaev J.E. (Republic of Uzbekistan)
Email: Baltabaev57@scientifictext.ru

Baltabaev Jahangir Eliwbaevich – Master,
DEPARTMENT OF APPLIED MATHEMATICS,
KARAKALPAK STATE UNIVERSITY, NUKUS, REPUBLIC OF UZBEKISTAN

Abstract: *in article problem definition information security and for their decision RSA algorithm is considered. In the last two decades, thanking first of all to inquiries of cryptography and wide circulation of the COMPUTER, researches on algorithmic questions of the theory of numbers endure the period of rough and very fruitful development. It is provided the full theoretical review of the RSA method and a short example. Results are received in the program C ++.*
Keywords: *asymmetric cryptography, the RSA system, enciphering, interpretation, an open key, the closed key.*

ОБЗОР К ВОПРОСУ АЛГОРИТМА RSA ДЛЯ ШИФРОВАНИЯ ИНФОРМАЦИИ

Балтабаев Ж.Е. (Республика Узбекистан)

Балтабаев Жахангир Елиубаевич – магистрант,
кафедра прикладной математики,
Каракалпакский государственный университет, г. Нукус, Республика Узбекистан

Аннотация: *в статье рассматривается постановка задачи защиты информации и для их решения алгоритм RSA. В последние два десятилетия, благодаря, в первую очередь, запросам криптографии и широкому распространению ЭВМ, исследования по алгоритмическим вопросам теории чисел переживают период бурного и весьма плодотворного развития. Приведен полный теоретический обзор метода RSA и короткий пример. Результаты получены в программе C++.*
Ключевые слова: *асимметричная криптография, система RSA, шифрования, расшифровка, открытый ключ, закрытый ключ.*

В середине 70-х годов произошел настоящий прорыв в современной криптографии - появление асимметричных криптосистем, которые не требовали передачи секретного ключа между сторонами. Здесь отправной точкой принято считать работу, опубликованную Уитфилдом Диффи и Мартином Хеллманом в 1976 году под названием «Новые направления в современной криптографии». В ней впервые сформулированы принципы обмена шифрованной информацией без обмена секретным ключом. Независимо к идее асимметричных криптосистем подошел Ральф Меркли. Несколькими годами позже Рон Ривест, Ади Шамир и Леонард Адлеман открыли систему RSA, первую практическую асимметричную криптосистему,

стойкость которой была основана на проблеме факторизации больших простых чисел. Асимметричная криптография открыла сразу несколько новых прикладных направлений, в частности системы электронной цифровой подписи (ЭЦП) и электронных денег.

В 80-90-е годы появились совершенно новые направления криптографии: вероятностное шифрование, квантовая криптография и другие. Осознание их практической ценности еще впереди. Актуальной остается и задача совершенствования симметричных криптосистем. В 80-90-х годах были разработаны нефейстеловские шифры (SAFER, RC6 и др.), а в 2000 году после открытого международного конкурса был принят новый национальный стандарт шифрования США - AES.

1. ПОСТАНОВКА ЗАДАЧИ

Безопасность передачи данных по каналам связи является актуальной. Современные компьютерные сети не исключение. К сожалению, в сетевых операционных системах (Windows NT/XP, Novell и т.д.) иностранного производства, как следствие, из-за экспортных соображений уровень алгоритмов шифрования заметно снижен.

Задача: исследовать современные методы шифрования и их приложимость к шифрованию потоков данных. Разработать собственную библиотеку алгоритмов шифрования и программный продукт, демонстрирующий работу этих алгоритмов при передаче данных в сети.

2. АЛГОРИТМ RSA

Труды Евклида и Диофанта, Ферма и Эйлера, Гаусса, Чебышева и Эрмита содержат остроумные и весьма эффективные алгоритмы решения диофантовых уравнений, выяснения разрешимости сравнений, построения больших по тем временам простых чисел, нахождения наилучших приближений и т.д.

Возможности ЭВМ имеют определённые границы. Приходится разбивать длинную цифровую последовательность на блоки ограниченной длины и шифровать каждый такой блок отдельно [1]. Мы будем считать в дальнейшем, что все шифруемые целые числа неотрицательны и по величине меньше некоторого заданного (скажем, техническими ограничениями) числа m. Таким же условиям будут удовлетворять и числа, получаемые в процессе шифрования. Это позволяет считать и те, и другие числа элементами кольца вычетов $\mathrm{Z}/m\mathrm{Z}$. Шифрующая функция при этом может рассматриваться как взаимно однозначное отображение колец вычетов

$$f : \mathrm{Z}/m\mathrm{Z} \to \mathrm{Z}/m\mathrm{Z}$$

а число $f(x)$ представляет собой сообщение X в зашифрованном виде.

Простейший шифр такого рода - шифр замены, соответствует отображению $f : x \to x + k \pmod m$ при некотором фиксированном целом k. Подобный шифр использовал еще Юлий Цезарь. Конечно, не каждое отображение f подходит для целей надежного сокрытия информации.

В 1978 г. американцы Р. Ривест, А. Шамир и Л. Адлеман (R.L.Rivest. A.Shamir. L.Adleman) предложили пример функции f, обладающей рядом замечательных достоинств. На её основе была построена реально используемая система

шифрования, получившая название по первым буквам имен авторов -система RSA. Эта функция такова, что

1) существует достаточно быстрый алгоритм вычисления значений $f(x)$;

2) существует достаточно быстрый алгоритм вычисления значений обратной функции $f^{-1}(x)$;

3) функция $f(x)$ обладает некоторым «секретом», знание которого позволяет быстро вычислять значения $f^{-1}(x)$; в противном же случае вычисление $f^{-1}(x)$ становится трудно разрешимой в вычислительном отношении задачей, требующей для своего решения столь много времени, что по его прошествии зашифрованная информация перестает представлять интерес для лиц, использующих отображение f в качестве шифра.

3 . СИСТЕМА ШИФРОВАНИЯ RSA

Пусть m и e натуральные числа. Функция f реализующая схему RSA, устроена следующим образом

$$f : x \to x^e \pmod m. \qquad (1)$$

Для расшифровки сообщения $a = f(x)$ достаточно решить сравнение

$$x^e = a \pmod m. \qquad (2)$$

При некоторых условиях на m и e это сравнение имеет единственное решение x.

Для того чтобы описать эти условия и объяснить, как можно найти решение, нам потребуется одна теоретико-числовая функция, так называемая функция Эйлера. Эта функция натурального аргумента m обозначается $\varphi(m)$ и равняется количеству целых чисел на отрезке от 1 до m, взаимно простых с m. Так $\varphi(1) = 1$ и $\varphi(p^r) = p^{r-1}(p-1)$ для любого простого числа p и натурального r. Кроме того, $\varphi(ab) = \varphi(a)\varphi(b)$ для любых натуральных взаимно простых a и b. Эти свойства позволяют легко вычислить значение $\varphi(m)$, если известно разложение числа m на простые сомножители.

Если показатель степени e в сравнении (2) взаимно прост с $\varphi(m)$, то сравнение (2) имеет единственное решение. Для того, чтобы найти его, определим целое число d, удовлетворяющее условиям

$$de \equiv 1 \pmod{\varphi(m)}, \quad 1 \le d < \varphi(m). \qquad (3)$$

Такое число существует, поскольку $(e, \varphi(m)) = 1$, и притом единственно. Здесь и далее символом (a, b) будет обозначаться наибольший общий делитель чисел a и b. Классическая теорема Эйлера, утверждает, что для каждого числа x, взаимно простого с m, выполняется сравнение $x^{\varphi(m)} \equiv 1 \pmod m$ и, следовательно.

$$a^d \equiv x^{de} \equiv x \pmod m. \qquad (4)$$

Таким образом, в предположении $(a, m) = 1$, единственное решение сравнения (2) может быть найдено в виде

$$x \equiv a^d \pmod{m}. \qquad (5)$$

Если дополнительно предположить, что число m состоит из различных простых сомножителей, то сравнение (5) будет выполняться и без предположения $(a, m) = 1$. Действительно, обозначим $r = (a, m)$ и $s = m/r$. Тогда $\varphi(m)$ делится на $\varphi(s)$, а из (2) следует, что $(x, s) = 1$. Подобно (4), теперь легко находим $x \equiv a^d \pmod{s}$. А кроме того, имеем $x \equiv 0 \equiv a^d \pmod{r}$. Получившиеся сравнения в силу $(r, s) = 1$ дают нам (5).

Функция (1), принятая в системе RSA, может быть вычислена достаточно быстро. Обратная к $f(x)$ функция $f^{-1} : x \to x^d \pmod{m}$ вычисляется по тем же правилам, что и $f(x)$, лишь с заменой показателя степени e на d. Таким образом, для функции (1) будут выполнены указанные выше свойства 1) и 2).

Для вычисления функции (1) достаточно знать лишь числа e и m. Именно они составляют открытый ключ для шифрования. А вот для вычисления обратной функции требуется знать число d. оно и является «секретом», о котором речь идёт в пункте в). Казалось бы, ничего не стоит, зная число m разложить его на простые сомножители, вычислить затем с помощью известных правил значение $\varphi(m)$ и, наконец, с помощью (3) определить нужное число d. Все шаги этого вычисления могут быть реализованы достаточно быстро, за исключением первого. Именно разложение числа m на простые множители и составляет наиболее трудоемкую часть вычислений. В теории чисел несмотря на многолетнюю её историю и на очень интенсивные поиски в течение последних 20 лет, эффективный алгоритм разложения натуральных чисел на множители так и не найден [2]. Конечно, можно, перебирая все простые числа до $\sqrt{m}$, и деля на них m, найти требуемое разложение. Но, учитывая, что количество простых в этом промежутке, асимптотически равно $2\sqrt{m} \cdot (\ln m)^{-1}$, находим, что при m, записываемом 100 десятичными цифрами, найдётся не менее $4 \cdot 10^{42}$ простых чисел, на которые придётся делить m при разложении его на множители. Очень грубые прикидки показывают, что компьютеру, выполняющему миллион делений в секунду, для разложения числа $m > 10^{99}$ таким способом на простые сомножители потребуется не менее, чем 10^{35} лет. Известны и более эффективные способы разложения целых чисел на множители, чем простой перебор простых делителей, но и они работают очень медленно.

Авторы схемы RSA предложили выбирать число m в виде произведения двух простых множителей p и q, примерно одинаковых по величине. Так как

$$\varphi(m) = \varphi(pq) = (p-1)(q-1), \qquad (6)$$

то единственное условие на выбор показателя степени e в отображении (1) есть

$$(e, p-1) = (e, q-1) = 1. \qquad (7)$$

Итак, лицо, заинтересованное в организации шифрованной переписки с помощью схемы RSA, выбирает два достаточно больших простых числа p и q. Перемножая их, оно находит число $m = pq$. Затем выбирается число e, удовлетворяющее условиям (7), вычисляется с помощью (6) число $\varphi(m)$ и с помощью (3) - число d. Числа m и e публикуются, число d остается секретным. Теперь любой может отправлять зашифрованные с помощью (1) сообщения организатору этой системы, а организатор легко сможет расшифровывать их с помощью (5).

4. ПРИМЕР: ШИФРОВАНИЕ СООБЩЕНИЯ

Для наглядности вычисления, будем использовать небольшие числа. Но на практике используют очень большие числа (длиной 200-300 десятичных разрядов).

Действия объекта B:

- Берет $P = 3, Q = 11$.
- Берет модуль $N = P \times Q = 3 \times 11 = 33$.
- Берет значение функции Эйлера для $N = 33$: $\varphi(N) = (P-1) \times (Q-1) = 2 \times 10 = 20$.
- Берет в качестве открытого ключа $K_в$ произвольное число с учетом условия: $1 < K_в \leq \varphi(N), mod\ (K_в, \varphi(N)) = 1$, допустим $K_в = 7$.
- Решаем значение секретного ключа $к_в$ используя алгоритм Евклида: $к_в \equiv = 3$.
- объект В передает объекту А пару чисел $(N = 33, K_в = 7)$.

Действия объекта A:

- Показывает шифруемое сообщение как последовательность целых чисел в диапазоне 0…32. Допустим буква А представляется как число 1, буква В это 2 и $C = 3$. Припустим что сообщение $C\,A\,B$ можно показать как последовательность числе 321, то есть $M1 = 3, M2 = 1, M3 = 2$.
- Шифрует сообщение, М используя ключ $K_в = 7$ и $N = 33$ по формуле: $C_i = M_i K_в\ (mod\ N) = M_i 7 (mod\ 3)$.
- Получаем:
  - $C_i = 3^7 (mod\ 33) = 2187\ (mod\ 33) = 9$
  - $C_i = 1^7\ (mod\ 33) = 1\ (mod\ 33) = 1$
  - $C_i = 2^7 (mod\ 33) = 128\ (mod\ 33) = 29$
- Передает объекту В криптограмму: $C_1, C_2, C_3 = 9, 1, 29$.

Действия объекта B:

- Расшифровывает принятую криптограмму C_1, C_2, C_3 используя секретный ключ ≡ = 3 по формуле: $\boldsymbol{M_i = C_i^{K_в}\ (mod\ N) = C_i^3\ (mod\ 3)}$
  - $M_1 = 9^3\ (mod\ 33) = 729\ (mod\ 33) = 3$.
  - $M_2 = 1^3\ (mod\ 33) = 1\ (mod\ 33) = 1$.
  - $M_2 = 29^3\ (mod\ 33) = 24389\ (mod\ 33) = 2$.

Объект получил исходное сообщение, которое послал объект А.

Список литературы / References

1. *Кнут Д.* Искусство программирования для ЭВМ. Т. 2. Получисленные алгоритмы. М.: Мир, 1977.
2. *Schneier B.* «Applied Cryptography: Protocols, Algorithms, and Source Code in C». John Wiley & Sons, New York, 2nd edition, 1996.

СООТВЕТСТВУЕТ
ГОСТ 7.56-2002
СЕТЕВОЕ ИЗДАНИЕ
ISSN 2541-7851

№ 23 (77). Ч.2. ДЕКАБРЬ 2019

ВЕСТНИК НАУКИ И ОБРАЗОВАНИЯ

НАУЧНО-МЕТОДИЧЕСКИЙ ЖУРНАЛ

РОСКОМНАДЗОР
ПИ № ФС 77-50633 • ЭЛ № ФС 77-58456

НАУЧНО-МЕТОДИЧЕСКИЙ ЖУРНАЛ «ВЕСТНИК НАУКИ И ОБРАЗОВАНИЯ» № 23 (77) Ч.2. 2019

ИЗДАТЕЛЬСТВО «ПРОБЛЕМЫ НАУКИ»
HTTPS://SCIENCEPROBLEMS.RU
ЖУРНАЛ: HTTP://SCIENTIFICJOURNAL.RU

НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА
eLIBRARY.RU

ISSN 2541-7851 (сетевое издание)

ВЕСТНИК НАУКИ И ОБРАЗОВАНИЯ

2019. № 23 (77).Часть 2

Москва
2019

Содержание

ИЗУЧЕНИЕ ПРОБЛЕМЫ ФАКТОРИЗАЦИИ ПАРАМЕТРА N В АЛГОРИТМЕ RSA С ПОМОЩЬЮ СИСТЕМЫ «MATHEMATICA»

Бердимуратов М.К.[1], Ибрагимов К.И.[2], Балтабаев Ж.Е.[3]
Email: Baltabaev677@scientifictext.ru

[1]Бердимуратов Мурат Карлыбаевич - кандидат физико-математических наук, доцент;
[2]Ибрагимов Куанышбай Исмайлович – ассистент;
[3]Балтабаев Жахангир Елибаевич – магистрант.
кафедра прикладной математики,
Каракалпакский государственный университет,
г. Нукус, Республика Узбекистан

Аннотация: *немногие из криптографических алгоритмов являются и безопасными, и практичными. Обычно эти алгоритмы основаны на одной из трудно разрешимых проблем математики. Некоторые из этих безопасных и практичных алгоритмов подходят только для распределения ключей. Другие подходят только для шифрования данных и для цифровых подписей. В статье рассматривается первый полноценный алгоритм с открытым ключом, который можно использовать для шифрования и цифровых подписей - алгоритм RSA. В алгоритме для генерации двух ключей используются два (p и q) больших случайно выбранных простых числа равной длины.*

Ключевые слова: *ключ шифрования, дешифрования, алгоритм Евклида, Mathematica.*

STUDYING THE PROBLEM OF FACTORIZATION PARAMETER N IN THE RSA ALGORITHM BY USING THE "MATHEMATICA" SYSTEM

Berdimuratov M.K.[1], Ibragimov K.I.[2], Baltabaev J.E.[3]

[1]Berdimuratov Murat Karlybaevich - Candidate of physical and mathematical sciences, Associate Professor;
[2]Ibragimov Kuanishbay Ismaylovich – Assistant;
[3]Baltabaev Jahangir Elibaevich - Undergraduate,
DEPARTMENT OF APPLIED MATHEMATICS,
KARAKALPAK STATE UNIVERSITY,
NUKUS, REPUBLIC OF UZBEKISTAN

Abstract: *few of the cryptographic algorithms are both safe and practical. Typically, these algorithms are based on one of the difficult solvable problems of mathematics. Some of these safe and practical algorithms are only suitable for key distribution. Others are only suitable for data encryption and for digital signatures. The article considers the first full-fledged public key algorithm that can be used for encryption and digital signatures - the RSA algorithm. The algorithm uses two (and) large randomly chosen primes of equal length to generate two keys.*

Keywords: *key encryption, decryption, Euclidean algorithm, Mathematica.*

Рассчитывается произведение $n = pq$. Затем случайным образом выбирается ключ шифрования e, такой что $НОД(e,(p-1)(q-1)) = 1$. Используем расширенный алгоритм Евклида для вычисления ключа дешифрования d, такого что

$ed = 1(\mathrm{mod}(p-1)(q-1))$. d и n взаимно простые числа. Числа e и n открытый ключ, а число d закрытый. Простые числа p и q больше не нужны, но они не должны быть раскрыты. Для шифрования сообщения используется формула $C_i = M_i^e \bmod n$, а для дешифрования $M_i = C_i^d \bmod n$ [2] - [4].

В теории чисел не смотря на многолетнюю историю и на очень интенсивные поиски в течение последних несколько лет, эффективный алгоритм разложения натуральных чисел на множители так и не найден. Конечно можно перебирая все простые числа до $\sqrt{n}$, и, деля на них n, найти требуемое разложение. Асимптотически оно равно $2\sqrt{n}(\ln n)^{-1}$. Если n стозначное число, то для разложения n на множители, компьютеру, выполняющему миллионы делений в секунду, потребуется не менее 10^{35} лет. Во время введения RSA Шроппель предложил модификацию алгоритма факторизации Моррисона и Бриллхарта. Она включала $e^{\sqrt{\ln n \ln\ln n}}$ операций.

При построении следующей таблицы, дающей представление о росте этого выражения, используются функций *TableForm, Table, Exp, Sqrt, Log* и *N* из пакета "Mathematica".

```
(Debug) In[7]:= TableForm[Table[{k, N[Exp[Sqrt[Log[10^k] *
                    Log[Log[10^k]]]], 3]}, {k, 25, 250, 25}],
                TableHeadings → {{}, {"длина в цифрах", "сложность"}},
                TableAlignments → {Center}]
```

(Debug) Out[7]//TableForm=

длина в цифрах	сложность
25	4.30×10^{7}
50	1.62×10^{16}
75	8.99×10^{22}
100	2.34×10^{28}
125	3.41×10^{33}
150	3.26×10^{38}
175	2.25×10^{43}
200	1.20×10^{48}
225	5.17×10^{52}
250	1.86×10^{57}

Вероятность того, что произойдет, можно быть вычислена с помощью функций Эйлера $\varphi(n)$:

$$\frac{n-\varphi(n)}{n} = \frac{pq-(p-1)(q-1)}{pq} = \frac{p+q-1}{pq} \approx \frac{1}{p}$$

в предположении, что $q < p$. То, что p нельзя брать слишком маленьким, вытекает из алгоритма факторизации, рассматриваемой ниже.

Полларда описал способ разложения числа n за $\sqrt{n}$ шагов, где p- наименьший простой делитель числа n. Основным предположением в (p-1)-методе Полларда разложение числа n хотя бы один из двух делителей обладает тем свойством что p-1 или q-1 имеет только малые простые делители. Натуральное число называется S-гладким, если все его простые делители не превосходят *S*. Будем предполагать p-1 гладкое относительно некоторого S.

Пусть p=70877, с помощью функции FactoringInteger и PrimeQ пакета "Mathematica" можно проверить гладкость этого числа. [1]

```
In[1]:= p = 70877;
        PrimeQ[p]
        FactorInteger[p - 1]

Out[2]= True

Out[3]= {{2, 2}, {13, 1}, {29, 1}, {47, 1}}
```

Это число гладкое относительно S=50. Для каждого простого числа $r \le S$ наибольшая степень r, которая не превосходить n, удовлетворяет неравенству $r^i \le n, \quad i \le \log_r n$

Определим равенство

$$R = \prod_{r \le S, r\ простое} r^{\lfloor \log_r n \rfloor}$$

Например $n = 6700892281$. Предположим для простого делителя p число $p-1$ гладко относительно $S = 50$.

```
In[4]:= Prime[15]
        Prime[16]

Out[4]= 47

Out[5]= 53
```

Отсюда вытекает, что имеются 15 простых чисел, не превосходящих $S = 50$. Для вычисления R используем функции Prime, Log и Floor.

```
(Debug) In[8]:= n = 6 700 892 281;
                R = Product[(Prime[i])^Floor[Log[Prime[i], n]], {i, 1, 15}]

(Debug) Out[9]=
        4 049 567 180 360 871 571 548 109 887 351 145 051 687 154
        638 935 149 024 506 072 707 670 221 428 242 481 373 494
        650 191 940 316 796 203 975 457 787 003 008 948 633 600
        000 000 000 000
```

Если $p-1$ - гладкое относительно S, то каждая степень r^i простого числа, который делит $p-1$, будет также делителем числа R, так как i не превосходить $\lfloor \log_r n \rfloor$. Отсюда следует, что $p-1$ делит R. По теореме Ферма любое целое $a, 2 \le a < p$ удовлетворяет $a^{p-1} (\mathrm{mod}\, p) \equiv 1$. Поскольку $(p-1) \mid R$, также имеем $a^R (\mathrm{mod}\, p) \equiv 1$.

Возьмем случайно число $a \in [2, p)$. Если $НОД(a,n) \ne 1$, то мы нашли делитель числа n. Противном случае из $a^R (\mathrm{mod}\, p) \equiv 1$ следует, $p \mid (a^R - 1)$.

Например, делитель числа $n = 6700892281$ можно найти с помощью функции Random, PowerMod и GCD.

```
a = Random[Integer, {2, n}]
GCD[PowerMod[a, R, n] - 1, n]
```

(Debug) Out[9]=

```
3786054151
```

(Debug) Out[10]=

```
81919
```

Это означает, что 81919 является делителем числа n.

Для того чтобы рассмотренный метод имел высокую стойкость число $p-1$ должно содержать обязательно большой простой множитель. В противном случае легко можно найти простой множитель данного числа. Поэтому число p выбирается таким, чтобы выполнялось равенство $p = 2q + 1$, где $q -$ простое число.

Список литературы / References

1. *Дьяконов В.П.* Mathematica 5.1/5.2/6. Программирование и математические вычисления. М.: ДМКПресс, 2008. 576 с.: ил.
2. *Смарт Н.* Криптография. М., Техносфера, 2005. 528 с.
3. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. М., Изд. Триумф. 2002. 616 с.
4. *Балтабаев Ж.Е.* Обзор к вопросу алгоритма RSA для шифрования информации «International scientific review of the problems of technical sciences, mathematics and computer science // Usa, Boston. November 11-12, 2018. P. 49-54 (ISBN 978-1-948507-00-4).