ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АЛОҚА, АХБОРОТЛАШТИРИШ ВА ТЕЛЕКОММУНИКАЦИЯ ТЕХНОЛОГИЯЛАРИ ДАВЛАТ ҚЎМИТАСИ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

Қўл ёзма ҳуқуқида

УДК 004.056

Мардиев Улугбек Расулович

НОССИМЕТРИК КРИПТОТИЗИМЛАРДА КАЛИТЛАРНИ ГЕНЕРАЦИЯЛАШ АЛГОРИТМЛАРИ ТАДҚИҚИ

5А330301 - Криптография ва криптотаҳлил

Магистр
академик даражасини олиш учун ёзилган
диссертация

Илмий раҳбар:
т.ф.н. Мусаев А.И

АННОТАЦИЯ

Диссертация мавзусининг асосланиши ва унинг долзарблиги.

Бутун жаҳонда сўнгги йилларда ахборот технологияларининг жадал суръатлар билан ривожланиб бориши натижасида ахборот хавфсизлиги муаммоси Ўзбекистон Республикаси учун ҳам долзарб муаммога айланди. Ахборот-коммуникация тизимида маълумотларни махфий ёки конфиденциал алмашув жараёни учун криптографик тизимлар яратиш билан бир қаторда шу тизимда бардошли калитлар яратиш масаласини ишончли ҳал этиш муҳим ўрин тутади. Мазкур магистрлик диссертация иши криптографик бардошлиги юқори бўлган калитларни генерация қилиш алгоритмларининг таҳлили ва тадқиқига қаратилганлиги унинг долзарблилигидан далолат беради

Тадқиқот мақсади ва вазифалари.

Носимметрик криптотизимларга асосланган калитларни генерация қилиш алгоритмларининг тадқиқига асосланган ҳолда криптобардошлилиги юқори бўлган такомиллашган алгоритм таклиф этишдан иборат.

Тадқиқот объекти ва предметининг белгиланиши.

Тадқиқот объекти бўлиб калитларни генерация қилиш алгоритмлари хизмат қилади.

Тадқиқот предмети сифатида генерация қилинадиган сонларни тубликка синаш амаллари хизмат қилади.

Тадқиқотда қўлланилган услубларнинг қисқача тавсифи.

Ахборотни криптографик ҳимоялаш тизимлари назарияси, информатика ва математика асослари, сонлар назарияси, модуль арифметикаси, дискрет логарифмлашдан фойдаланилган.

Тадқиқотнинг илмий янгилиги.

Бардошлилиги юқори бўлган туб сонларни генерация қилиш алгоритми ишлаб чиқилди ва уни носимметрик криптотизимларда қўллаш асосида бардошлилиги юқори бўлган, такомиллаштирилган алгоритм ишлаб чиқилди ва дастури яратилди.

Тадқиқот натижаларининг назарий ва амалий аҳамияти.

Ишлаб чиқилган бардошли калитларни генерация қилиш алгоритмлардан миллий электрон ҳужжат айланиш тизимларида қўлланилиши мумкинлиги билан амалий аҳамиятга эгадир.

Диссертация таркибининг қисқача тавсифи.

Ушбу диссертация иши кириш қисми, 3 та бўлим, хулоса, фойдаланилган адабиётлар рўйхати ва иловадан иборат. Ушбу тадқиқот ишида 3 та жадвал, 8 та расмдан иборат. Илмий тадқиқот ишининг умумий ҳажми 83 саҳифани ташкил этади.

Магистрлик диссертация иши бўйича 2 та тезис чоп этилган.

Хулоса ва таклифларни қисқача умумлаштирилган ифодаси

Бардошли туб сонларни генерация қилиш, тубликка тестлашнинг комлекс усули таклиф қилиниб, параметрли алгебрадан фойдаланиб носсиметрик криптотизимлар учун дастур яратилди.

МУНДАРИЖА

КИРИШ

Диссертация ишининг долзарблиги. Бутун жаҳонда сўнгги йилларда ахборот технологияларининг жадал суръатлар билан ривожланиб бориши натижасида ахборот хавфсизлиги муаммоси Ўзбекистон Республикаси учун ҳам долзарб муаммога айланди. Ҳозирги кунда ахборот хавфсизлигини таъминлашда энг ишончли воситалардан бири ахборотни криптографик ҳимоя қилиш воситалари ҳисобланади. Шу боис Республикамизда бу йўналиш жадал суръатлар билан ривожланмоқда. Президентимизнинг 2007 йил 3 апрелда қабул қилган «Ўзбекистон Республикасида ахборотнинг криптографик ҳимоясини ташкил этиш чора-тадбирлари тўғрисидаги» ПҚ-614–сон қарори шулар жумласидандир[2].

Ахборот-коммуникация тизимида маълумотларни махфий ёки конфиденциал алмашув жараёни учун криптографик тизимлар яратиш билан бир қаторда шу тизимда бардошли калитлар яратиш масаласини ишончли ҳал этиш муҳим ўрин тутади. Чунки танланган криптотизим мураккаб ва ишончли бўлиши ундан амалда фойдаланиш жараёнлари бардошли калитларни генерация қилиш масаласи билан боғлиқдир.

Мазкур диссертация иши Ўзбекистон Республикаси Президентининг ПҚ-614–сон қарори ижросини таъминлаш йўлида бажарилаётган илмий-тадқиқот ишларидан бири ҳисобланади [2]. Криптографияда бардошли калитларни генерация қилиш доимо асосий муаммолардан бири бўлиб келган. Хорижий давлатларда бу соҳада қатор илмий изланишлар қилинган ва криптографик алгоритмлар яратилган.

Мазкур магистрлик диссертация иши криптографик бардошлиги юқори бўлган калитларни генерация қилиш алгоритмларининг таҳлили ва тадқиқига қаратилганлиги унинг долзарблилигидан далолат беради.

Диссертация ишининг объекти ва предметининг белгиланиши. Ушбу магистрлик диссертация ишида тадқиқот объекти бўлиб калитларни генерация қилиш алгоритмлари хизмат қилади.

Тадқиқот предмети сифатида генерация қилинадиган сонларни тубликка синаш амаллари хизмат қилади.

Диссертация ишининг мақсади ва вазифалари. Ушбу магистрлик диссертация ишини бажаришдан кўзланган мақсад носимметрик криптотизимларда калитларни генерация қилиш алгоритмларининг таҳлили ва тадқиқини амалга ошириш ҳамда криптобардошлилиги юқори бўлган калитларни генерациялаш алгоритмини ишлаб чиқишдан иборат.

Кўзланган мақсадни амалга ошириш учун магистрлик диссертация ишини бажаришда қуйидаги вазифалар қўйилди:

- калитларни генерация қилиш бўйича мавжуд алгоритмларни тадқиқ қилиш ва қиёсий таҳлил этиш;

- калитларни генерация қилиш алгоритмларини маълум белгилар асосида таснифлаш;

- туб сонларни генерация қилиш алгоритмлари тадқиқи ва қиёсий таҳлили;

- сонларни генерация қилишда уларни тубликка синаш алгоритмлари таҳлили;

- криптобардошлиги юқори бўлган калитларни генерация қилиш алгоритмларини ишлаб чиқиш;

- криптобардошлиги юқори бўлган калитларни генерация қилиш алгоритмларини дастурини яратиш;

Илмий тадқиқотнинг асосий масалалари ва фаразлари. Ахборот-коммуникацион тизимларида ахборот хавфсизлигини таъминлашда очиқ калитли криптотизимларни тадқиқ этиш, уларни криптобардошлигини баҳолаш ва ушбу талаблар асосида криптографик бардошли калитлар

генерация қилиш алгоритмини ва дастурини яратиш масалалари ечимига эришиш.

Мавзу бўйича қисқача адабиётлар таҳлили. Ҳозирги кунда ахборот хавфсизлигини таъминлашда энг ишончли воситалардан бири ахборотни криптографик ҳимоя қилиш воситалари ҳисобланади. Ахборот-коммуникация тизимида маълумотларни махфий ёки конфиденциал алмашув жараёни учун криптографик тизимлар яратиш билан бир қаторда шу тизимда криптографик бардошли калитлар яратиш масаласини ишончли ҳал этиш муҳим ўрин тутади.

Носсиметрик криптотизимларда тасодифий калит генераторлари, сонларни тубликка синаш алгоритмлари борасида Рабби-Миллер, П.Ферма, Н.Саксене, М.Агравал, У. Диффи, Шеннон К.Е. томонидан олиб борилган тадқиқотларни келтириш мумкин. Ушбу олиб борилган тадқиқотлар шуни кўрсатдики носсиметрик криптотизимларда калитлар туб сонларга асосланган, бардошли калитларни генерация қилишда уларни тубликка синаш тестидан ўтказиш талаб қилинади. Шуларни ҳисобга олиб криптографик тизимларда криптобардошли калитларни яратиш мақсадида калит генераторлари алгоритмлари яратилди.

Бу соҳада Ўзбекистон Республикаси олимлари томонидан ҳам етарли тадқиқот ишлари олиб борилмоқда, бунга Хасанов П.Ф., Арипов М.М., Каримов М.М., Акбаров Д.Е., Ғаниев С.К., Хасанов Х.П., Ахмедова О.П. томонидан эришилган натижаларни келтириш мумкин.

Криптографик тизимларга қўйилган талабларга асосан, ҳозирги замон криптографиясида калитларнинг бардошлилигини таъминлашда уларнинг тасодифий танланиши билан туб сонлардан ташкил топганлигини ҳисобга олган ҳолда, носсиметрик криптотизимлар учун туб сонларни генерация қилувчи алгоритмларни хусусиятлари ва самарадорлигини чуқур таҳлил қилиниши ва етарли даражада ўрганилиши керак.

Илмий тадқиқот ишида қўлланилган услубларнинг қисқача тавсифи. Ушбу диссертация ишида ахборотни криптографик ҳимоялаш тизимлари назарияси, информатика ва математика асослари, сонлар назарияси, модуль арифметикаси, дискрет логарифмлашдан фойдаланилган.

Тадқиқот натижаларининг назарий ва амалий аҳамияти. Мавжуд очиқ калитли криптотизимларда калитларни генерация қилиш алгоритмларини таҳлил этиш, уларни қуриш усулларини ўрганиш, криптобардошлигини баҳолаш ва бардошли калитларни генерация қилиш алгоритмларини ишлаб чиқиш магистрлик диссертациясининг назарий аҳамияти ҳисобланади.

Магистрлик диссертациясининг амалий аҳамияти – магистрлик диссертацияси ишида ишлаб чиқилган алгоритмлардан миллий электрон ҳужжат айланиш тизимларида фойдаланиш мумкин.

Диссертация ишининг илмий янгилиги. Мазкур магистрлик диссертацияси натижасида бардошлилиги юқори бўлган туб сонларни генерация қилиш алгоритми ишлаб чиқилди ва уни носимметрик криптотизимларда қўллаш асосида бардошлилиги юқори бўлган, такомиллаштирилган алгоритм ишлаб чиқилди ва дастури яратилди.

Диссертация ишининг тузилмаси ва ҳажми.

Ушбу диссертация иши кириш қисми, 3 та бўлим, хулоса, фойдаланилган адабиётлар рўйхати ва иловадан иборат. Ушбу тадқиқот ишида 3 та жадвал, 9 та расмдан иборат. Илмий тадқиқот ишининг умумий ҳажми 83 саҳифани ташкил этади.

I боб. Носимметрик криптотизимлар ва уларнинг таҳлили

1. Носимметрик шифрлаш алгоритмлари таҳлили

Симметрик криптоалгоритмлар асосида яратилган криптотизим ахборот-коммуникация тармоқларида маълумотлар алмашинувининг муҳофазасини таъминлаш масалаларини ечишда қанчалик ишончли бўлмасин, барибир ундан амалда фойдаланиш жараёнида айрим қўшимча хавфсизликни таъминлаш масалалари келиб чиқиб, уларнинг ечилиши талаб этилади. Шундай масалалардан бири калитларни тизим фойдаланувчиларига тарқатиш масаласидир. Ишлаб чиқилган бардошли калитларни тизим фойдаланувчиларига етказиш хавфсизлиги кафолати таъминланган бўлиши талаб этилади. Бунинг учун эса қўшимча ҳолда яна бирор бошқа криптотизимдан фойдаланишга тўғри келади. Бу масала ечимининг қўшимча криптотизимдан фойдаланмай ҳал этилиши классик ва замонавий алгебрада олинган илмий натижалар асосида яратилган *очиқ калитли (ошкора калитли, носимметрик) криптотизим*ларнинг вужудга келиши билан амалга оширилди [5].

Носимметрик криптотизимлар бундан 1976 йил муқаддам АҚШ олимлари У. Диффи ва М. Хэллман[10-11] томонидан кашф этилган бўлиб, улар катта сонли чекли тўпламларда бир томонлама функциялардан фойдаланишга асосланган. У. Диффи ва М. Хэллманнинг 1976 йилда босилиб чиққан “Криптологияда янги йўналишлар” мақоласида илгари сурилган “махфий калитни узатишни талаб этмайдиган амалий бардошли махфий тизимларни тузиш мумкин” деган фикри криптологияда носимметрик криптотизимларнинг юзага келиши ҳамда уларнинг ривожланиш даврининг бошланишига сабаб бўлди.

Носимметрик криптотизимларнинг юзага келиши симметрик тизимларда ечилмай қолган махфий шифрлаш калитларини тарқатиш ва

электрон рақамли имзо тизимларини яратиш ҳамда қатор замонавий масалаларни ечиш имкониятини берди.

Носимметрик криптотизимлар симметрик криптотизимларга нисбатан ўнлаб марта катта узунликдаги (*512, 1024, 2048, 4096* битли) калитлардан фойдаланади ва шу сабаб юзлаб марта секинроқ ишлайди. Носимметрик криптотизимларнинг математик асосида бир томонлама осон ҳисобланадиган функциялар (модуль бўйича дискрет даражага ошириш функцияси, эгри чизиқли эллиптик функция ва ш.к.) ётади. Носимметрик криптотизимлар ахборот хавфсизлигининг барча муаммоларини ечиб беришга қодир ҳисобланади.

Очиқ калитли криптотизим моҳияти ҳар бир фойдаланувчи учун бирини билган ҳолда иккинчисини топиш, ечилиши мураккаб бўлган масала билан боғлиқ калитлар жуфтлигини яратишдан иборат. Бу жуфтликни ташкил этувчи калитлардан бири очиқ (ошкора), иккинчиси махфий (шахсий) деб эълон қилинади. Очиқ калит ошкора эълон қилинади, махфий калит фақат унинг эгасигагина маълум бўлади. Бирор фойдаланувчининг очиқ калитини билган ҳолда унинг махфий калитини топишнинг амалий жиҳатдан мумкин эмаслиги, ечилиши мураккаб бўлган масаланинг ҳал этилишини талаб қилиши билан кафолатланади. Очиқ маълумот, шу маълумотни олиши керак бўлган фойдаланувчининг очиқ калити билан шифрланиб унга узатилади. Шифрланган маълумотни олган фойдаланувчи фақат унинг ўзига маълум бўлган махфий калит билан уни дешифрлаб, очиқ маъумотга эга бўлади.

Очиқ калитли криптотизимлар алгоритмлари уларнинг асосини ташкил этувчи бир томонли функциялар билан фарқланади. Аммо ҳар қандай бир томонли функция ҳам очиқ калитли криптотизимлар яратиш учун ва улардан амалдаги аҳборотлар тизимида маҳфий алоқа хизматини ўрнатиш алгоритмини қуриш учун қулайлик туғдирмайди.

Бир томонли функцияларни аниқланиш таърифида назарий жиҳатдан тескариси мавжуд бўлмаган функциялар эмас балки, берилган функцияга тескари бўлган функциянинг қийматларини ҳисоблаш амалий жиҳатдан мақсадга мувофиқ бўлмаган функциялар тушинилади. Шунинг учун маълумотнинг ишончли муҳофазасини таъминловчи очиқ калитли криптотизимларга муҳим бўлган қуйидаги талаблар қўйилади[5]:

1. Дастлабки очиқ маълумотни шифрмаълумот кўринишига ўтказиш биртомонли жараён ва шифрлаш калити билан шифрмаълумотни очиш-дешифрлаш мумкин эмас, яъни шифрлаш калитини билиш шифрмаълумотни дешифрлаш учун етарли эмас.

2. Очиқ калитнинг маълумлигига асосланиб, маҳфий калитни замонавий фан ва техника ютуқлари ёрдамида аниқлаш учун бўладиган сарф-ҳаражатлар ҳамда вақт мақсадга мувофиқ эмас. Бунда, шифрни очиш учун бажарилиши керак бўладиган энг кам миқдордаги амаллар сонини аниқлаш муҳимдир.

Очиқ калитли шифрлаш алгоритмларидан ахборотлар тизимида маълумотларнинг маҳфийлигини таъминлашда замонавий илғор услуб сифатида фойдаланиб келинмоқда. Очиқ калитли криптотизимларни яратишнинг RSA алгоритми жаҳон стандарти сифатида қабул қилинган. Умуман олганда замонавий очиқ калитли криптотизимлар қуйидаги типдаги масалаларни ечишнинг кўп вақт талаб қилиши ва ҳисоб-китоблар учун ҳисоблаш қурилмаларида катта ҳажмдаги хотирани талаб этилиши билан боғлиқ бўлган мураккабликларга таянади[4]:

1. Етарли катта сонларни туб кўпайтувчиларга ёйиш.

2. Характеристикаси етарли катта бўлган чекли майдонларда дискрет логарифмларни ҳисоблаш.

3. Етарли катта тартибдаги алгебраик тенгламалар системасининг илдизларини чекли майдонларда ҳисоблаш.

4. Эллиптик эгри чизиқларда рационал координатали нуқталарни топиш, уларни қўшиш ҳамда тартибини аниқлаш каби.

RSA шифрлаш алгоритми. Диффи ва Хелман критография соҳасида янгича ёндашишни тарғиб қилиб, очиқ калитли криптотизимларнинг барча талабларига жавоб берадиган криптографик алгоритм яратиш таклифи билан чиқди. Биринчилардан бўлиб бунга жавобан 1978 йил Рон Райветс (Ron Rivest), Ади Шамир (Adi Shamir) ва Лен Адлмен (Len Adlmen)лар шу вақтгача тан олинган ва амалий кенг қўлланиб келинган очиқ калитли шифрлаш алгоритм схемасини таклиф қилди ва бу алгоритм уларнинг номи шарафига RSA алгоритми деб аталди. RSA алгоритми факторлаш мураккаблигига асосланган шифрлаш алгоритми ҳисобланади[6].

Райвест, Шамир ва Адлмен томонидан яратилган схема даража кўрсаткичига асосланган. Очиқ матн блокларга ажратилиб шифрланади, ҳар бир блок баъзи берилган n сонидан кичик бўлган иккилик қийматга эга бўлади. Бундан келиб чиқадики блок узунлиги $log_2(n)$дан кичик ёки тенг бўлиши керак. Умуман олганда амалиётда блок узунлиги 2^kга тенг деб олинади, бу ерда $2^k < n \leq 2^{k+1}$. Очиқ матн M блоки ва шифрланган матн C блоки учун шифрлаш ва дешифрлаш қуйидаги формула билан ҳисоблаш мумкин.

$$M = M^e mod n,$$

$$M = C^d mod n = (M^e)^d mod n = M^{ed} mod n.$$

Жўнатувчи ҳам, қабул қилувқи ҳам n ни қийматини билиши керак. Жўнатувчи e ни қийматини, қабул қилувчи эса фақат d ни қийматини билишади. Ушбу схема очиқ калитли шифрлаш алгоритми ҳисобланади, $KU=\{e,n\}$- очиқ калит ва $KR=\{d,n\}$-махфий калит ҳисобланади.Бу алгоритм очиқ калит ёрдамида шифрланиши учун, қуйидаги талаблар бажарилиши керак[7, 8].

1. Шундай e, d ва n қийматлар мавжуд бўлиш керакки, барча $M < n$ учун $M^{ed} = Mmodn$ тенглик ўринли бўлиши керак.

2. Барча $M < n$ учун M^e ва C^d ни ҳисоблаш осон бўлиши керак.

3. Амалий жиҳатдан e ва n ни билмасдан туриб d ни қийматини билиш мумкин бўлмаслиги керак.

Биринчи шартга биноан қуйидаги муносабатни топиш керак

$$M^{ed} = Mmodn.$$

Эйлер функциясига асосан: ҳар қандай иккита p ва q туб сон ва ҳар қандай n ва m бутун сонлар учун, $n=pq$ ва $0 < m < n$, ва ихтиёрий k бутун сон учун қуйидаги муносабат бажарилади.

$$m^{k\varphi(n)+1} = m^{k(p-1)(q-1)+1} \equiv mmodn,$$

Бу ерда $\varphi(n)$ Эйлер функцияси бўлиб, n дан кичик ва n билан ўзаро туб бўлган мусбат бутун сон. Эйлер функцияси $\varphi(n)$ билан ўзаро туб бўлган e сон танлаб олинади ва талаб қилинаётган муносабат қуйидаги шарт асосида бажарилади.

$$ed = k\varphi(n) + 1.$$

Бу қуйидаги муносабат билан эквивалент:

$$ed \equiv 1\ mod\varphi(n),$$

$$d \equiv e^{-1}mod\varphi(n),$$

e ва d, $\varphi(n)$ модул бўйича ўзаро тескари сон, яъни

$$gcd(\varphi(n), e) = 1.$$

Юқорида келтирилган параметрлар асосида RSA схемасини қуйидаги таьснифлаш мумкин:

- p ва q - туб сонлар (махфий, танлаб олинади);
- $n=pq$ (очиқ, ҳисобланади);
- шундай e, $gcd(\varphi(n), e) = 1,\ 1 < e, \varphi(n)$ (очиқ, танлаб олинади);

- $d \equiv e^{-1} mod \varphi(n)$ (махфий, ҳисобланади).

Махфий калит $\{d,n\}$ дан, очиқ калит эса $\{e,n\}$ дан иборат бўлади. Фараз қилайлик *A* фойдаланувчи очиқ калитини элон қилди ва *B* фойдаланувчи унга *M* хабарни жўнатмоқчи. *B*фойдаланувчи $C = M^e (mod n)$ ҳисоблаб *C* ни жўнатади. Шифрланган матнни қабул қилган *A* фойдаланувчи $M = C^d (mod n)$ ёрдамида дешифрлаб дастлабки очиқ матнга эга бўлади[9].

Қуйида келтирилган мисолда RSA алгоритми амалий қўллаш кўрсатилган.

1. Иккита туб сон танлаб олинади, $p=7$ ва $q=17$.

2. $n=p*q=7*17$ ҳисобланади.

3. Эйлер функцияси ҳисобланади $\varphi(n) = (p-1)(q-1) = 96$.

4. Эйлер функцияси $\varphi(n) = 96$ билан ўзаро туб бўлган ва ундан кичкина бўлнаг *e* танлаб олинади; бу мисолда $e=5$.

5. $de=1 mod\ 96$ ва$d<96$шартни қаноатлантирувчи *d*сони топилади. $d=77$, $77*5=385=4*96+1$.

Натижада очиқ калит $KU=\{5,119\}$ ва ёпиқ калит $KR=\{77,119\}$ ҳосил бўлади. Би мисолда очиқ матн қиймати $M=19$ олинган. Шифрлаш формуласига кўра очиқ матн қиймати очиқ калит қиймати ёрдамида даражага кўтарилиб, *n* модул бўйича қиймати олинади, яъни 19 сони 5 даражага кўтарилади, натижада 2476099 ҳосил бўлади. Натижани 119 га бўлсак, қолдиқ 66 га тенг бўлади. $19^5 = 66\ mod\ 119$ ва шунинг учун ҳам шифрланган матн 66 га тенг бўлади. Дешифрлаш учун эса шифрланган матн қиймати махфий калит қиймати ёрдамида даражага кўтарилиб, *n* модул бўйича қиймати олинади, яъни$66^{77} = 19\ mod\ 119$ амални ҳисоблаймиз ва дастлабки очиқ матн қийматига эга бўлтнади яъни 19 га.

Калитларни ҳисоблаш. Очиқ калитли криптотизимларга калитларни генерацтя қилиш муҳим аҳамият касб этади. Ҳар бир томон иккитадан калит

генерация қилиши керак бўлади. Буни амалга ошириш учун эса қуйидаги вазифаларни бажариш керак бўлади:

- иккита p ва q дан иборат туб сон аниқлаб олиниш;
- иккинчисини ҳисоблаш учун, e ёки d сонларидан бирини танлаш.

Биринчи бўлиб p ва q ни танлаш процедурасини кўриб чиқсак. $n=pq$ қиймати ҳамма маълумлигини инобатга олган ҳолда, p ва q ни қийматини оддий перебор усулда топиш имкониятига йўл қўймаслик учун, бу туб сонлар етарли даражада катта бўлиши керак. Шу билан бир қаторда катта туб сонларни топиш методи амалий жиҳатдан унумли бўлиши керак.

Ҳозирги кундагача самарадорлиги яхши бўлган, иҳтиёрий катта сондаги туб сонни ҳисоблаш методи ишлаб чиқилмаган. Бу методларда кўпроқ тахминан исталган узунликдаги ва аниқликдаги, танлаб олинган тоқ сонни тубликка текшириш процедураси ётади. Агар танлаб олинган сон туб бўлиб чиқмаса, кейинги туб сон танлаб олинади токи туб сон танлаб олинмагунча. Сонларни тубликка текширувчи бир қатор тестлар мавжуд бўлиб, бу тестларининг деярли барчаси эҳтимоллик характерига эга. Яъни тестлаш натижаси берилган бутун сонни эҳтимолий тублигини аниқлайди. Тўлиқ ишонч бўлмаслигига қарамасдан, бундай тестларнинг бажарилиши, ишончлилиги таъминланганлиги эҳтимоли бирга яқин бўлади[9, 12].

Рабби-Миллер ва аксарият шунга ўхшаш алгоритмларда, берилган бутун n сонни тубликка синаш процедураси, тасодифий танлаб олинган бутун сон a ва n иштирокидаги бир қатор ҳисоблашларни бажаришдан иборат. Агар n бундай тестлашларга жавоб бера олса, у ҳолда n туб сон бўлиб чиқади, акс ҳолда туб эмас. Агар n ҳар хил тасодифий танланган a нинг қийматларида,бир қатор шундай синовлардан муваффақиятли ўтса, n нинг туб сон эканлигининг ишончлилиги даражаси ортади.

Хулоса қилиб шуни айтиш мумкинки, туб сонни танлаб олиш процедурасини қуйидаги кўринишда кўрсатиш мумкин.

1. Тоқ бўлган бутун n сонни қандайдир тасодифий равишда танлаб олиш(масалан псевдотасодифий генератор орқали).
2. Тасодифий равишда $a<n$ бўлган бутун a сон танлаб олиш.
3. Танлаб олинган сонни тубликка синаш тестидан ўтказиш. Агар n сони тестдан ўта олмаса, кейинги тасодифий равишда танлаб олинган сонни шу кетма-кетликда бажариш керак.
4. Агар n етарлича қайта тестлардан муваффақиятли ўтса, n қийматни муносиб деб олиш керак, акс ҳолда 2 қадамга ўтиш керак.

Шуни эсдан чиқармаслик керакки, бу жараён фақат, қачонки янги калитлар жуфтлигини (KU,KR) яратиш талаб қилинсагина бажарилади. Сонлар назарияси ҳақидаги теоремаларидан бири, туб сонлар ҳақидаги теорема шуни тасдиқлайдики, N гача бўлган бутун сонлардан $ln(N)$ таси туб бўлиши мумкин. Бундан келиб чиқадики туб сонни топиш учун, $ln(N)$ гача бўлган бутун сонларни тубликка синашга тўғри келади, бунга эса ўз-ўзидан кўп вақт ҳамда супер замонавий ҳисоблаш машинаси керак бўлади. Жуфт сонларни чиқариб ташласак сонлар тартиби $ln(N)/2$ тага етади. Масалан туб сонни узунлиги тартиби 2^{2000} бўлган ораликда излайдиган бўлсак, туб сонни топиш учун $ln(N)/2=70$ га яқин уриниш керак бўлади. p ва q туб сонни аниқлагандан кейин, e қийматни танлаб d ни ҳисоблаш ёки тескари, d қийматни танлаб e ни ҳисоблаш билан калитларни ҳисоблаш жараёни тугайди. Биринчи навбатда e ни шундай танлиш керакки, у Эйлер функцияси билан ўзаро туб бўлиши керак яъни $gcd(\varphi(n), e)=1$, шундан сўнг e га ўзаро тескари бўлган d топилади $d = e^{-1} mod \varphi(n)$. Бундай ўзаро туб сонларни топиш Евклиднинг умумлашган алгоритми бўйича топилади, яъни процедура шундан иборатки тасодифий равишда генерацияланган сонни $\varphi(n)$ билан ўзаро туб бўлмагунча таққосланади. Танлаб олинган сонларнинг туб бўлиш

эҳтимоли 0.6 га тенг бўлиб, тўғри келадиган қийматни топиш учун бир неча текширишлар етарли бўлади.

RSA алгоритмининг ҳимояланганлиги. RSA алгоритмининг уч хил мумкин бўлган криптотиҳлил усули мавжуд бўлиб, улар қуйидагилардан иборат[12]:

- Оддий танлаш усули. Бунда барча мумкин бўлган махфий калитларни текшириш таклиф қилинади.
- Математик анализ. Бундай бир нечта усуллар мавжуд бўлиб, уларнинг ҳаммаси иккита туб сонли кўпайтманинг кўпайтувчиларини топиш моҳияти бўйича эквивалентдир.
- Вақт сарфи бўйича анализ. Шифрлаш алгориминиг бажарилишига кетган вақтни анализ қилишга қаратилган.

Оддий танлаш усулига қарши ҳимоя RSA да ҳам, қолган барча криптотизимлардагидек катта ҳажмдаги калитларни ишлатишдир. Бундай ёндашишда e ва d қанча катта битдан иборат бўлса шунча яхши. Лекин калитларни генерация қилишда мураккаб ҳисоблашларни ишлатиш ҳамда шифрлаш/дешифрлаш калитларининг узунлигининг катта бўлиши тизимни секин ишлашига олиб келади.

RSA криптотаҳлилида 3 хил математик ёндашувни ажратиб кўрсатиш мумкин.

- n ни иккита туб кўпайтувчиларга ажратиш. Бу ўз навбатида $\varphi(n) = (p-1)(q-1)$ ҳисоблашни, бу эса $d = e^{-1}(mod\varphi(n))$ ни аниқлаб олиш имконини беради.
- Олдиндан p ва q ни ҳисобламасдан туриб, тўғридан тўғри $\varphi(n)$ аниқлаш.
- Олдиндан $\varphi(n)$ ни аниқламасдан туриб, тўғридан тўғри d ни аниқлаш.

Кўп ҳолларда RSA шифри криптотаҳлилида n қийматни иккита туб кўпайтувчига ажратиш масаласи муҳокама қилинади. Берилган n бўйича $\varphi(n)$ ни аниқлаш масаласи билан n ни кўпайтувчиларга ажратиш масаласи билан эквивалент ҳисобланади. Ҳозирги кундаги маълум алгоритмларда e ва n орқали d ни аниқлаш муаммосига кетадиган вақт билан, кўпайтувчиларга ажратиш муаммосига кетадиган вақт бир хил. Шундай экан кўпайтувчиларга ажратиш масаласини ечишга кетадиган вақтни RSA ни ҳимояланганлини баҳолашга сарфлаш мумкин.

ЭЛ-ГАМАЛ шифрлаш алгоритми. Эль-Гамал алгоритмида криптотизимнинг ҳар бир i-фойдаланувчисига туб модуль p ва ҳосил қилувчи (генератор) g маълум ҳисобланади ва i-фойдаланувчи учун шахсий калитни ифодаловчи x_i-сон бўйича ҳисобланадиган $y_i = a^{x_i} \bmod p$ - очиқ калит генерация қилинади ва у барчага ошкор этилади[5,29]. Агарда мана шу i-фойдаланувчи билан бирор бошқа j-фойдаланувчи очиқ маълумот M ни шифрматнга ўгирилган ҳолда ахборот алмашувини амалга оширмоқчи бўлса, у ҳолда j-фойдаланувчи p сонидан кичик бўлган бирор k -сонини танлаб олиб

$$y_1 = g^k (\bmod p) \quad \text{ва} \quad y_2 = (M / y^k)(\bmod p),$$

сонларини ҳисоблайди. Сўнгра j-фойдаланувчи $(y_1;y_2)$ маълумотларини i-фойдаланувчига жўнатади. Ўз навбатида i-фойдаланувчи бу шифрланган маълумотни қабул қилиб, қуйидагича

$$(y_1^x \cdot y_2) \bmod p = M$$

ҳисоблаш билан очиқ маълумотни тиклайди.

Эль Гамал криптоалгоритмига асосланган криптотизимнинг ҳар бир i-фойдаланувчиси учун $\langle y_i, x_i \rangle$ - калитлар жуфтлиги қуйидагича яратилиши ҳам мумкин: бирор p_i-туб сони ва $g_i < p_i$ - тенгсизликни қаноатлантирувчи g_i

(фойдаланувчилар гуруҳи учун умумий p ва $g < p$ тенгсизликни қаноатлантирувчи g) сонлари танланади. Ушбу $x_i < p_i$ тенгсизликни қаноатлантирувчи махфий бўлган x_i- сони бўйича очиқ деб эълон қилинадиган y_i-сони ушбу формула $y_i = g_i^{x_i} (\mathrm{mod}\, p_i)$ (фойдаланувчилар гуруҳи учун $x_i < p$ ҳамда $y_i = g^{x_i} \bmod p$) орқали ҳисобланади. Шундай қилиб, Эль Гамал критотизимида (p_i, g_i, y_i) – учлик (фойдаланувчилар гуруҳи учун p ва g умумий бўлиб, (p, g, y_i) – учлик) очиқ калит, x_i - эса махфий (шахсий) калит деб олинади.

Шундан сўнг i-фойдаланувчидан j - фойдаланувчига шифрланган маълумотни жўнатиш қуйидагича амалга оширилади:

1. **Шифрлаш қоидаси**: ушбу ифода $a_j = g_j^k \bmod p_j$, $b_j = y_j^k M \bmod p_j$ (фойдаланувчилар гуруҳи учун p ва g умумий бўлганда: $a = g^k \bmod p$, $b = y_j^{\,k} M \bmod p$) ҳисобланади, бу ерда M - очиқ маълумот, k - маълумотни шифрлаб жўнатувчи томонидан танланган тасодифий сон бўлиб, у ($p_j - 1$) – сони билан ўзаро туб, $(a_j, b_j) = C$ (p ва g умумий бўлганда $(a, b) = C$ – шифрланган маълумот);

2. **Дешифрлаш қоидаси**: $b_j / a_j^{x_j} \bmod p_j = M$ (p ва g умумий бўлганда: $b / a^{x_j} \bmod p = M$), ҳақиқатан ҳам, $b_j / a_j^{x_j} \bmod p_j \equiv g_j^{x_i k} M / g_j^{k x_i} \bmod p_j \equiv M$ (p ва g умумий бўлганда: $b / a^{x_j} \bmod p \equiv y_j^k M / a^{x_j} \bmod p \equiv g^{x_j k} M / g^{k x_j} \bmod p = M \bmod p = M$, чунки $M < p$).

Криптотизимнинг ҳар бир i-фойдаланувчиси учун очиқ ва махфий калитларни x_i- сони маълум бўлганда $y_i = g_i^{x_i} \bmod p_i$ (фойдаланувчилар гуруҳи учун $x_i < p$ ҳамда $y_i = g^{x_i} \bmod p$) тенглик бўйича генерация қилинади.

Аммо x_i- сони фойдаланувчиларга номаълум бўлганда, очиқ калитни ифодаловчи $y_i = g_i^{x_i} \bmod p_i$ тенгликдан $x_i = \log_{g_i} y_i (\bmod p_i)$ - сонини топиш, чекли майдон характеристикаси p_i етарли катта бўлганда, мураккаблашади ва бугунги кунда чекли майдонларда логарифмлаш масаласи ечимининг самарали усуллари мавжуд эмас.

2. Носимметрик электрон рақамли имзо алгоритмлари таҳлили

RSA очиқ калитли шифрлаш алгоритми асосидаги ЭРИ. Тизимнинг ҳар бир i- фойдаланувчиси (e_i, d_i) - калитлар жуфтлигини яратади. Бунинг учун етарли катта бўлган p ва q - туб сонлари олиниб (бу сонлар маҳфий тутилади), $n = pq$- сони ва Эйлер функциясининг қиймати $\varphi(n) = (p-1)(q-1)$ ҳисобланади (бу сон ҳам маҳфий тутилади). Сўнгра, $(e_i, \varphi(n)) = 1$ шартни қаноатлантирувчи, яъни $\varphi(n)$ -сони билан ўзаро туб бўлган e_i -сон бўйича d_i- сони ушбу $e_i d_i = 1 \bmod \varphi(n)$ формула орқали ҳисобланади. Бу $(e_i; d_i)$ – жуфтликда e_i - очиқ калит ва d_i- маҳфий калит деб эълон қилинади.

Шундан сўнг i- фойдаланувчидан j- фойдаланувчига шифрланган маълумотни имзолаган ҳолда жўнатиши қуйидагича амалга оширилади:

1. Шифрлаш қоидаси: $M^{e_j} \bmod n = C$, бу ерда M - очиқ маълумот, C – шифрланган маълумот;

2. Дешифрлаш қоидаси: $C^{d_j} \bmod n = M^{e_j d_j} \bmod n = M$;

3. ЭРИ ни ҳисоблаш: $H(M)^{d_i} \bmod n = P_i$,

бу ерда i- фойдаланувчининг P_i- имзоси M - маълумотнинг $H(M)$- хеш функция қиймати бўйича ҳисобланган;

4. ЭРИ ни текшириш:

$P_i^{e_i} \bmod n = H(M)^{e_i d_i} \bmod n = H(M)$, агар $H(M) = H(M_1)$ бўлса (бу ерда M_1 - дешифрланган маълумот), у ҳолда электрон хужжат ҳақиқий, акс ҳолда

ҳақиқий эмас, чунки хэш функция хоссасига кўра $M = M_1$ бўлса уларнинг хэш қийматлари ҳам тенг бўлади.

5. Маълумотни махфий узатиш протоколи:

$$\left[M \cup H\left(M\right)^{d_i}\right]^{e_j} \bmod n = \left[M \cup P_i\right]^{e_j} \bmod n = C;$$

6. Махфий узатилган маълумотни қабул қилиш протоколи:

$C^{d_j} \bmod n = \left[M \cup P_i\right]^{e_j d_j} \bmod n = M \cup P_i$, умуман қараганда дастлабки маълумот ўзгартирилган бўлиши мумкин, шунинг учун $C^{d_j} \bmod n = M_1 \cup P_i$ бўлиб, натижада, хеш қиймат имзо бўйича ушбу ифода $\left(P_i\right)^{e_i} \bmod n = H\left(M\right)^{e_i d_i} \bmod n = H\left(M\right)$ билан ҳисобланади ва қабул қилиб олинган маълумотнинг хеш қиймати $H\left(M_1\right)$ бўлса, у ҳолда $H\left(M\right) = H\left(M_1\right)$ бўлганда электрон ҳужжат ҳақиқий, аксинча бўлса қалбаки ҳисобланади.

Эл-Гамал очиқ калитли шифрлаш алгоритми асосидаги ЭРИ. Эл-Гамал очиқ калитли шифрлаш алгоритмига асосланган криптотизимнинг ҳар бир i- фойдаланувчиси учун очиқ ва маҳфий калитлар генерацияси қуйидагича амалга оширилади, очиқ эълон қлинадиган p_i- туб сон (ёки фойдаланувчилар гуруҳи учун умумий бўлган p- туб сон) танланади, ушбу $g_i < p_i$ (ёки фойдаланувчилар гуруҳи учун $g < p$) шартни қаноатлантирувчи g_i (ёки фойдаланувчилар гуруҳ учун g) сони танланади, ушбу $y_i = g^{x_i} \bmod p_i$ (p- умумий бўлганда $y_i = g^{x_i} \bmod p$, $x_i < p$) формула билан x_i - махфий калит бўйича y_i сони ҳисобланади. Шундай қилиб, $\left(p_i, g_i, y_i\right)$-параметрлар бирикмаси (умумий p ва g учун $\left(p, g, y_i\right)$- параметрлар бирикмаси очиқ калитни ташкил этади, маҳфий калит x_i ҳисобланади[5].

Тизимда i- фойдаланувчидан j- фойдаланувчига шифрланган маълумотнинг имзоланган ҳолда жўнатилиши қуйидагича амалга оширилади:

1. **Шифрлаш қоидаси**: $a_j = g_j^k \bmod p_j$, $b_j = y_j^k M \bmod p_j$ (умумий p и g лар учун $a = g^k \bmod p$, $b_j = y_j^k M \bmod p$), бу ерда k-тасодифий сон бўлиб маълумотни имзоловчи томонидан танланади, бу сон $(p_j - 1)$ сони билан ўзаро туб ЭКУБ$(k, p_j - 1) = 1$ (p ва g умумий бўлганда ЭКУБ$(k, p-1) = 1$), M-очиқ маълумот, шифрланган маълумот $(a, b_j) = C$ (p ва g умумий бўлганда, $(a, b_j) = C$).

2. Дешифрлаш қоидаси: $b_j / a_j^{x_j} \bmod p_j = M$ (p ва g умумий бўлганда $b / a^{x_j} \bmod p = M$), ҳақиқатан ҳам $b_j / a_j^{x_j} \bmod p_j \equiv g_j^{x_i k} M / g_j^{k x_i} \bmod p_j \equiv M$ (p ва g умумий бўлганда $b / a^{x_j} \bmod p \equiv y_j^k M / a^{x_j} \bmod p \equiv g^{x_j k} M / g^{k x_j} \bmod p = M \bmod p = M$, так как $M < p$);

3. ЭРИ ни ҳисоблаш қоидаси: $a_i = g_i^k \bmod p_i$, b_i сони эса $M = (x_i a_i + k b_i) \bmod (p_i - 1)$ ёки $H(M) = (x_i a_i + k b_i) \bmod (p_i - 1)$ тенгламадан топилади, яъни $b_i = (M - a_i x_i) k^{-1} \bmod (p_i - 1)$ ёки $b_i = (H(M) - a_i x_i) k^{-1} \bmod (p_i - 1)$ (p ва g умумий бўлганда $a = g^k \bmod p$, b сони эса $M = (x_i a + k b) \bmod (p - 1)$ ёки $H(M) = (x a + k b) \bmod (p - 1)$ тенгламадан топилади, яъни $b = (M - a x_i) k^{-1} \bmod (p - 1)$ ёки $b = (H(M) - a x_i) k^{-1} \bmod (p - 1)$, ЭКУБ$(k, p-1) = 1$) $H(M)$-маълумотнинг хэш қиймати, x_i-махфий калит, имзо сифатида a_i ва b_i жуфтлик, яъни $(a_i, b_i) = P_i$, (p ва g умумий бўлганда (a, b)) имзо деб қабул қилинади.

4. Имзони текшириш қоидаси: Агар $y_i^{a_i} a_i^{b_i} \bmod p_i = g_i^M \bmod p_i$ ёки $y_i^{a_i} a_i^{b_i} \bmod p_i = g_i^{H(M)} \bmod p_i$ бўлса, у ҳолда электрон хужжат ҳақиқий, акс ҳолда қалбаки ҳисобланади. Чунки,

$$y_i = g_i^{x_i} \bmod p_i \text{ ва } a_i = g_i^k \bmod p_i$$

тенгликлар ўринли бўлиб, Ферма теоремасига кўра ушбу айният ўринли:

$$y_i^{a_i} a_i^{b_i} \bmod p_i = (g_i^{x_i})^{a_i} (g_i^{k})^{b_i} \bmod p_i = g_i^{a_i x_i + k b_i} \bmod p_i = g_i^{d(p_i-1)+M} \bmod p_i =$$

$$= g_i^{d(p_i-1)} g_i^{M} \bmod p_i = (g_i^{(p_i-1)})^{d} \bmod p_i \cdot g_i^{M} \bmod p_i \left(\bmod p_i\right) =$$

$$= 1^{d} \bmod p_i \cdot g_i^{M} \bmod p_i \left(\bmod p_i\right) = g_i^{M} \bmod p_i ;$$

5. **Маълумотни махфий узатиш протоколи**:

$a_j = g_j^k \bmod p_j$, $b_j = y_j^k M' \bmod p_j = y_j^k \left[M \cup P_i\right] \bmod p_j$, $\left(a_j, b_j\right) = C$ - шифрмаълумот;

6. Махфий узатилган маълумотни қабул қилиш протоколи:

$$b_j \Big/ a_j^{x_j} \bmod p_j = M' = M \cup P_i ,$$

умуман қараганда, дастлабки маълумот ўзгартирилган бўлиши мумкин, шунинг учун

$$b_j \Big/ a_j^{x_j} \bmod p_j = M' = M_1 \cup P_i ,$$

бўлиб, $H\left(M_1\right)$ - хэш қиймат ҳисобланади. Агар $y_i^{a_i} a_i^{b_i} \bmod p_i = g_i^{M_1} \bmod p_i$ ёки $y_i^{a_i} a_i^{b_i} \bmod p_i = g_i^{H(M_1)} \bmod p_i$ бўлса, у ҳолда электрон хужжат ҳақиқий, акс ҳолда қалбаки ҳисобланади.

Энди имзони ҳисоблаш ва уни текширишга асосланган ЭРИ алгоритмлари DSA ва ГОСТ Р 34.10-94 стандарлари билан танишилади. Бу алгоритмларнинг асосини Эл-Гамал шифрлаш алгоритми ташкил этади.

DSA ЭРИ стандарти. 1991 йилда NIST (National Institute of Standard and Technology) томонидан DSA (Digital Signature Algorithm) алгоритмига асосланган DSS (Digital Signature Standard) ЭРИ стандартининг лойиҳаси муҳокамага қўйилди. Ушбу алгоритм бардошлилиги етарли катта туб характеристикага эга бўлган чекли майдонда дискрет логарифмлаш масаласининг мураккаблигига асосланган [5, 20]. Қуйида алгоритм қадамлари кетма-кетлиги келтирилган.

Имзони шакллантириш

1. Маълумот жўнатувчи M -маълумотни ва қуйидаги параметрларни кенг доирадаги тизим фойдаланувчиларига очиқ эълон қилади:

p – туб сон, $2^{512} < p < 2^{1024}$, бит узунлиги 64 га каррали;

q - туб сон, $2^{159} < q < 2^{160}$, $p-1$ нинг бўлувчиси;

$g = h^{(p-1)/q} \bmod p$, бу ерда h ушбу $0 < h < p$ ва $h^{(p-1)/q} \bmod p > 1$ шартларни қаноатлантирувчи бутун сон;

y – очиқ калит бўлиб, $y = q^x \bmod p$ формула орқали аниқланади. Бу ерда x – махфий калит бўлиб, $0<x<q$ ораликдан олинган ва фақат имзоловчининг ўзигагина маълум;

$H(M)$ – M маълумотдан $[1;q]$ ораликдаги бутун сонни генерация қилувчи хеш-функция.

2. Маълумот жўнатувчи $0 < k < q$ ораликдан тасодифий k сонни танлайди, уни махфий тутади ва имзо генерациясидан кейин дарҳол йўқотади.

3. Маълумот жўнатувчи r ва s қийматларни қуйидаги қонуният орқали ҳисоблайди:

$$r = g^k \bmod p \bmod q,$$

$$s = k^{-1}(xr + H(M)) \bmod q.$$

M - маълумотга қўйилган имзо (r, s) сонлар жуфтлигидан иборат.

Имзони текшириш. Қабул қилувчи M' маълумотни ва (r', s') имзони қабул қилиб олади. У M ва M' маълумотларнинг мос келишини текшириши лозим. Бунинг учун у қуйидаги қадамлар кетма-кетлигини бажаради:

1. $0 < s' < q$ ёки $0 < r' < q$ шартлардан бирортаси бажарилмаса, имзо қалбаки деб ҳисобланади ва имзони текшириш тугатилади.

2. $v = (s')^{-1} (\bmod q)$ топилади.

3. $z_1 = H(M') v \bmod q$, $z_2 = r' v \bmod q$ ҳисобланади.

4. Кейин $u = g^{z_1} y^{z_2} \bmod p \bmod q$ ҳисобланади.

5. Агар $r' = u$ тенглик ўринли бўлса, у ҳолда имзо ҳақиқий ва $M = M'$ тенглик тўғри.

Алгоритмнинг тўғрилиги. $M = M'$, $s' = s$ ва $r' = r$ бўлсин. У ҳолда $r = u$ тенглик ўринли бўлиши кўрсатилади.

Демак, $v = (s')^{-1} \bmod q$, $z_1 = H(M')\, v \bmod q$, $z_2 = r'\, v \bmod q$ эканлигидан, қуйидагини ёзиш мумкин:

$$u = g^{z1}\, y^{z1} \bmod p \bmod q = g^{H(M)s-1}\, g^{xrs-1} \bmod p \bmod q =$$
$$= g^{k(xr+H(M))-1(xr+H(M))} \bmod p \bmod q = g^{k} \bmod p \bmod q = r.$$

Бундан кўриш мумкинки, $r = u$ тенглик ўринли. Шундай қилиб, алгоритм тўғрилиги исботланди.

ГОСТ Р 34.10-94 электрон рақамли имзоси. Ушбу бўлимда 2000 йилгача Россия стандарти ҳисобланган ГОСТ Р 34.10–94 ЭРИ алгоритми қараб чиқилади. Бу алгоритм DSA алгоритмига ўхшаш ва қуйидаги бошланғич очиқ параметрлардан фойдаланади:

1) Узунлиги L бўлган катта p туб сон танланади, бу ерда L сон 509 битдан 512 битгача ёки 1020 битдан 1024 битгача оралиқдан танланади, яъни $2^{509} < p < 2^{512}$ ёки $2^{1020} < p < 2^{1024}$.

2) Узунлиги L_1 бўлган катта q туб сон танланади, бу ерда L_1 сон 254 битдан 256 битгача оралиқдан танланади, яъни $2^{254} < p < 2^{256}$.

3) $g^q \bmod p = 1$ шартни қаноатлантирувчи $0 < g < p-1$ оралиқдаги g сон танланади.

4) $y = g^x \bmod p$ дан y- очиқ калит ҳисобланади, бу ерда $0 < x < q$ оралиқдан олинган x -махфий калит.

5) $H(M)$ - хэш-функция берилган M- маълумот бўйича ҳисобланган бутун сон бўлиб, *1* дан q гача оралиқдаги қийматларни қабул қилади, яъни $1 < H(M) < q$.

Имзони генерация қилиш алгоритми. Бошланғич маълумотлар: M - маълумот, берилган параметрлар ва махфий калит. Натижа: имзо - (r,s).

1) $1 \le k \le q$ интервалдан тасодифий k сони олинади, у махфий сақланади ва имзо қўйилгандан кейин дарҳол йўқотилади.

2) $r = (g^k \bmod p)(\bmod q)$ ҳисобланади.

3) Жўнатилаётган M - маълумотнинг $e := H(M)$ - хэш қиймати ҳисобланади.

4) Агар $r = 0$ ёки $H(M) \bmod q = 0$ бўлса, у ҳолда 1- қадамга ўтилиб, бошқа k танланади.

5) $s = (xr + kH(M)) \bmod q$ ҳисобланади, бу ерда махфий калит x фақат имзо қўювчининг ўзигагина маълум.

6) Агар $s = 0$ бўлса, у ҳолда 1-қадамга борилади.

7) M маълумот имзоси - (r,s) жуфтлигидан иборат.

Имзони текшириш алгоритми. Бошланғич маълумотлар: M маълумот, берилган параметрлар, имзони текшириш калити ва M маълумот имзоси. Натижа: имзо ҳақиқийлиги ёки қалбакилиги ҳақидаги тасдиқ.

1) Агар $1 \le r, s \le n-1$ шарт бажарилмаса, у ҳолда имзо қалбаки ва имзони текшириш алгоритми тугатилади. Бу шартлар бажарилса кейинги қадамга ўтилади.

2) $e := h(m)$ ҳисобланади.

3) $w := H(M)^{(q-2)} \bmod q$ ҳисобланади.

4) $u_1 := sw \bmod q$ ҳисобланади.

5) $u_2 := (q-r)w \bmod q$ ҳисобланади.

6) $u := (g^{u_1} y^{u_2} \bmod p)(\bmod q)$ ҳисобланади.

7) Агар $u = r$ шарт бажарилса, у ҳолда имзо ҳақиқий, акс ҳолда имзо қалбаки ва имзони текшириш алгоритми тугатилади.

ГОСТ Р 34.10-94 имзо алгоритмининг тўғрилиги. ГОСТ Р 34.10-94 электрон рақамли имзо генерацияси алгоритмидан олинган r параметрнинг қийматини имзони текшириш алгоритмидаги u параметр қиймати билан тенглигини кўрсатишимиз керак.

Ҳақиқатан, $u = (g^{u_1} y^{u_2} \bmod p)(\bmod q) = g^{sw \bmod q} \cdot g^{x(q-r)w \bmod q} \bmod p \bmod q$

$= g^{(s+xq-xr)w \bmod q} \bmod p \bmod q = g^{(xr+kH(M)+xq-xr)w \bmod q} \bmod p \bmod q =$

$= g^{(kH(M)+xq)w \bmod q} \bmod p \bmod q =$

$= g^{kH(M)w \bmod q} \bmod p \cdot (g^q \bmod p)^{xw \bmod q} (\bmod q) =$

$= / (g^q \bmod p)=1$ шартга кўра, $(g^q \bmod p)^{xw \bmod q} (\bmod q)=1$ тенглик ўринли

$= g^{kH(M)w \bmod q} \bmod p \ (\bmod q) = / \ w=H(M)^{(q-2)} \bmod q$, $0<H(M)<q$ (q –туб) шартга ва Эйлера – Ферма теоремасига кўра $H(M)^{(q-2)} \bmod q= H(M)^{-1}$ эканлиги келиб чиқади, шунга кўра g нинг даражасини $kH(M)w=kH(M)H(M)^{q-2} \bmod q= kH(M)H(M)^{-1}=k$ каби ифодалаш мумкин $/ = g^k \bmod p \ (\bmod q) = r.$ Шундай қилиб талаб қилинган шарт кўрсатилди.

3. Носимметрик алгоритмларнинг криптобардошлиги таҳлили

Юқоридаги бўлимларда факторлаш ва дискрет логарифмлаш муаммосига асосланган RSA ва Эл-Гамал шифрлаш тизимлари ва ЭРИ алгоритлари кўриб чиқилди. Қуйида ушбу алгоритмларнинг таҳлили келтирилган.

Туб майдонда дискрет логарифмлаш учун биринчи субэкспоненциал алгоритм Леонард Адлеман томонидан таклиф этилган. Бироқ амалиётда бу алгоритм етарли даражада самарали бўлиб чиқмаган. Дон Копперсмит, Эндрю Одлижко ва Ричард Шреппель дискрет логарифмлаш учун “COS” номи остида субэкспоненциал алгоритмнинг ўз русумларини таклиф этдилар. Оливер Широкаур томонидан таклиф этилган сонли майдон ғалвири алгоритми $p>10^{100}$ бўлганда COS алгоритмининг барча модификацияларига нисбатан самаралироқ ишлайди [20, 28]. Сонли майдон умумлашган ғалвир

усулининг мураккаблиги $C=O(exp(c(ln\ p)^{1/3}\ (ln\ ln\ p)^{2/3}))$ амал билан баҳоланади, бу ерда $c\approx1,92$ [29-30].

Фараз қилинсинки, G - мультипликатив Абель группаси бўлсин. a асос бўйича дискрет логарифм b ни ҳисоблаш, шундай $x\in G$ ни топишга келтириладики, $a^x=b$ бўлсин. Дискрет логарифмнинг хоссалари ҳақиқий сонлар майдонидаги одатдаги логарифм хоссаларига кўп жиҳатлардан ўхшаш. Масалан,

$$log_a\ (h*j)\equiv log_a\ (h)+ log_a\ (j)\ (mod\ |G|)$$

кўринишдаги айният кучга эга, бу ерда $|G|$- группанинг тартиби, a - ҳосил қилувчи (генератор).

Индексли ҳисоблаш усулининг асосий ғояси шундаки, агар чекли майдон Z_p нинг баъзи элементлари учун

$$\prod^m_{i=1}x_i\equiv\prod^m_{j=1}y_j$$

бўлса, унда

$$\sum^m_{i=1}log\ _ax_i\equiv\sum^m_{j=1}log\ _ay_j\ mod\ (p-1).$$

Охирги таққосламалардан бир қанчасини ҳосил қилингач, $log\ _ax_i$ ва $_1log\ _ay_j$ номаълумларга нисбатан чегирмалар ҳалқаси Z_{p-1} да унча кўп номаълумларга эга бўлмаган тенгламалар системасини тузиш ва ҳал этиш мумкин. Шуни унутмаслик керакки, охирги таққосламада, ҳеч бўлмаганда log_ag қиймати маълум бўлган битта элемент g қатнашиши шарт.

Охирги таққосламани генерация қилишнинг энг осон усули, бу бирор $g\in Z_p$ ни танлаш, $u=a^g\ (mod\ p)$ ҳисоблаш ва кетма-кет танлаш усулида

$$u=\prod^k_{i=1}p^{\alpha i}\ _i$$

муносабатни қаноатлантирувчи сонларни топишдир. Бу ерда p_i - B дан кичик туб сонлар. Агар шундай сонларни топишнинг иложи бўлса, унда u силлиқлик чегараси B га эга бўлган силлиқ элементдир.

Дискрет логарифмлаш алгоритмида ҳам факторлаш алгоритмига ўхшаш икки босқич кўзга ташланади:

- биринчи, тайёрланиш босқичида бирор чегара B танланади ва фактор базаси ва бу база асосида тенгламалар системаси шакллантирилади;

- иккинчи босқичда тенгламалар системасининг ечими топилади.

Шундай қилиб, дискрет логарифмлашнинг барча усуллари ҳам охир оқибатда тенгламалар системасини ҳал қилишга келтирилади.

Факторлаш муаммосининг мураккаблигига асосланган носимметрик криптотизимларнинг криптотаҳлили. Факторлаш муаммосининг юзага келиши антик даврларга, Эратосфен яшаган даврларга, тахминан, эрамизгача 284-202 йилларга тўғри келади, муаммонинг ундан кейинги тарихи Фиббаночи (тахминан 1180-1250 йй.), Ферма (1601-1665 йй.), Эйлер (1707-1783 йй), Лежандр (1752-1833 йй.), Гаусс (1777-1855 йй.) каби улуғ математиклар номи билан боғланган [5, 31].

Факторлаш муаммосини ҳал этишга бағишланган адабиётлар [29, 30] да келтирилган. n модулни факторлаш масаласини ечишда биринчи навбатда ҳаёлга келадиган усул, бу $\sqrt{n}$ дан ошмайдиган туб сонларни танлаб уларга бўлиб кўришдир. Бошқа танлаш усули Фермага тегишли бўлиб, n ни квадратлар айирмаси кўринишида ифодалашга асосланган:

$$n=a^2-b^2=(a+b)(a-b).$$

Ферма энг катта умумий бўлувчи - $EKUB(n, a-b)$ ни, яъни n нинг нотривиал бўлувчисини топишга ҳаракат қилишни ҳамда бунга имкон берувчи усулни ҳам таклиф этган. Агар n нинг кўпайтувчилари бир-биридан катта фарқ қилмаса, бу усул оддий танлаш усулига нисбатан тез ечим беради ва унинг мураккаблиги $O(\sqrt{n})$ кўринишида ифодаланади, аммо ҳозирги кунда криптографик тизимларда амалда фойдаланиладиган ҳоллар учун аҳамиятга эга эмас. Лежандр мазкур ёндашувда $a^2 \equiv b^2 \pmod{n}$ га эга бўлиш лозимлигига

эътибор қаратган. Аммо, келтирилган таққослама ҳар қандай n учун етарли эмаслигини ҳам кўрсатган ва кўзланган мақсадга эришиш учун узлуксиз касрлардан фойдаланиш йўлини таклиф этган.

Компьютерлар асрида дастлабки 1970 йилларда таклиф этилган факторлаш алгоритмларидан бири $(p-1)$ Поллард алгоритми бўлган. Ундан сўнг $(p+1)$ Вильямс алгоритми ва ЭЭЧлардан фойдаланишга асосланган Ленстра алгоритми ишлаб чиқилди. Кейинчалик $(p-1)$ Поллард алгоритми $(p+1)$ Поллард алгоритми сифатида, Поллард r -, λ - усули номлари остида такомиллаштирилди. r - λ - Поллард усулининг мураккаблиги $I_p = \sqrt{\pi q/4}$ амал билан белгиланади. Ҳозирги кунга келиб, факторлаш муаммосининг энг тезкор усуллари бўлиб, чизиқли ғалвир, квадратик ғалвир, сонли майдон ғалвири, умумлашган сонли майдон ғалвири усуллари тан олинган [30].

Ҳозирги кунда энг самарали криптотаҳлил алгоритмларининг мураккаблиги экспоненциал эмас, балки субэкспоненциал мураккабликка эга.

Алгоритм экспоненциал мураккабликка эга дейилади, агарда унинг мураккаблиги қийматининг тартиби $O(t^{f(n)})$ бўлса [7].

Алгоритм полиномиал мураккабликка эга дейилади, агарда унинг мураккаблиги қийматининг тартиби $O(n^m)$ бўлса. Субэкспоненциал мураккабликка эга бўлган алгоритм мураккаблиги қийматининг тартиби $O(n^m)$ ва $O(t^{f(n)})$ орасида бўлади.

Факторлаш муаммоси асос қилиб олинган RSA алгоритмининг муаллифларидан бири Рональд Райвест 1977 йилда 125 разрядли сонни факторлаш учун 40 квадратиллион йил керак бўлади деб “башорат” қилган эди. Аммо, 1994 йилдаёқ 129 ўнли хонали сон факторланди.

Эллиптик эгри чизиқларга асосланган носимметрик алгоритмлар ҳозирда ЭРИ алгоритмларида ва шифрлаш алгоритмларида кенг қўлланилсада, ҳозирда RSA ва Эл-Гамал алгоритмларига асосланган, яъни факторлашга ва дискрет логарифмлаш муаммосига асосланган алгоритмлар

ҳам носимметрик тизимлар ичида муҳим аҳамият касб этади. Ундаги мавжуд камчилик сифатида эса калитлар узунлигини ортиб борилиши ва бу орқали шифрлашда ва дешифрлашда кетадиган вақтни ортишини олишимиз мумкин. Масадан, ҳозирда RSA алгоритмининг 2048 бит калит билан ҳам фойдаланиш давлат аҳамиятига эга бўлган ташкилотларга маслаҳат берилмайди. Ушбу камчилик албатта ҳозирда шахсий компьютерларнинг ривожланиши билан бартараф этиляпти. 1-жадвалга ушбу икки алгоритмнинг қиёсий таҳлили берилган.

1-жадвал

RSA ва Эл-Гамал алгоритмлари хусусиятлари

Хусусиятлари	**RSA шифрлаш ва ЭРИ**	**Эл-Гамал шифрлаш ва ЭРИ**
Муаммо тури	Факторлаш муаммоси	Дискрет логарифмлаш (факторлаш муаммосига қараганда мураккаброқ)
Криптобардошлиги	1300 бит учун $2.7*10^{28}$	1300 бит учун $2.7*10^{28}$
Калит узунлиги	4096 битгача	4096 битгача
ЭРИда имзо узунлиги	-	1.5 марта узунроқ
Махфий параметрлар	Q, P ва d параметрлар	X параметр
Ҳисоблашга кетадиган қувват	2 марта кам Эл-Гамалга қараганда (14.5%)	-
Шифрлашга кетадиган вақт	1000 марта кўпроқ	-

I **боб бўйича хулосалар**

Ушбу бўлимда факторлаш ва дискрет логарифмлашга асосланган носимметрик алгоритмлар ва улар асосидаги ЭРИ алгоритмлари таҳлили кўриб ўтилди. Ушбу муммо турига асосланган алгоритмлар ҳозирда кенг фойдаланилмасада, аммо носимметрик тизимларда муҳим аҳамият касб этади. Ушбу бўлимда қуйидаги натижа ва хулосалар олинди.

1. Носимметрик алгоритмларнинг математик асосига кўра таҳлиллар асосида дискрет логарифмлаш муаммосини факторлаш муаммосига кўра бардошли эканлиги ва буни ҳал қилиш учун кўп қувват ва вақт сарф этилади. Бу хусусият эса ушбу алгоритмнинг фойдаланиш даражасини кўрсатади.

2. Ушбу алгоритмлар бир хил калит узунлигида бир хил криптобардошликка эга эканлиги, бу ҳолда фақат шифрлашга кетган вақт бўйича Эл-Гамал тизими яхшироқ натижага эга эканлиги аниқланди. Криптобардошлиги ундаги махфий калитлар сони билан ҳам белгиланишини ҳисобга олсак, унда RSA алгоритми 2 та махфий калитлар (q, p ва d) орқали, Эл-Гамал эса фақат (x параметр) асосида таъминланиши аниқланди.

3. Шунингдек ушбу бўлимда, дискрет логарифмлаш муаммосига асосланган ЭРИ алгоритмлари кўриб чиқилди.

Бу муаммо турлари албатта ҳозирда замонавий компьютерларнинг ривожланиши билан ҳал қилиниб келинмоқда. Ушбу муаммонинг мураккаблик даражасини ортириш учун қўшимча параметрларнинг киритилиши (параметрли алгебра муаммосига асосланган) улардаги криптобардошлиликни ортиради. Бу хусусида эса учинчи бўлимда келтирилиб ўтилган.

II боб. Калитларни генерация қилиш алгоритмлари тадқиқи

1. Туб сонларни генерация қилиш алгоритмлари

Туб сонлар криптографик схемаларда узоқ вақтли параметр ҳисобланиши билан, криптографик тизимларда муҳим аҳамият касб этади. Очиқ калитли криптотизимларда туб сонларни генерация қилиш ва уларни тубликка текшириш муҳим ҳисобланади[19].

Сонлар назарияси ва криптографиянинг кўплаб масалаларида берилган узунликдаги туб сонларни генерация қилиш зарурати туғилади. Туб сонларни яратишнинг яхши усулларидан бири, қандайдир функция ёрдамида ҳосил қилиш усулидар. Мисол сифатида Л.Эйлер таклиф қилган кўпҳадни қарайдиган бўлсак

$$p(x) = x^2 + x + 41,$$

кўпҳадни қийматларининг дастлабки 40 ҳади туб сондан иборат бўлади.

Бироқ Юрий Матиясевич бунданда яхшироқ натижа олиш мумкинлигиги исботлади, яъни бутун коэффицентли бир нечта ўзгарувчилардан ташкил топган кўп ҳад мавжудки, унинг барча қийматлари туб сондан иборат бўлади.

$$F(a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z) = (k+2)(1 - (wz+h+j-q)^2 - (2n+p+q+z-e)^2 - (a^2y^2 - y^2 + 1 - x^2)^2 - \left((e^4+2e^3)(a+1)^2 - o^2\right)^2 - (16(k+1)^3(k+2)(n+1)^2 + 1 - f^2)^2 - \left(((a+u^4-u^2a)^2 - 1)(n+4dy)^2 + 1 - (x+cu)^2\right)^2 - (ai+k+1-l-i^2 - ((gk+2g+k+1)(h+j)+h-z)^2 - (16r^2y^4(a^2-1)+1-u^2)^2 - \left(p-m+l(a-n-1)+b(2an+2a-n^2-2n-2)\right)^2 - \left(z-pm+pla-p^2l+t(2ap-p^2-1)\right)^2 - \left(q-x+y(a-p-1)+s(2ap+2a-p^2-2p-2)\right)^2 - (a^2l^2-l^2+1-mr)^2 - (n+l+v-y)^2))$$

Яна шуни таъкидлаш керакки, Ю.Матиясевич ушбу кўпҳад ёрдамида Гилбертнинг машҳур 10-муаммосини, диафант тенгламаларининг ечими

бутун сондан иборат бўлишини аниқлайдиган умумий алгоритм йўқлигини исботлаган ҳолда ечишга эришди. Бу натижа математиканинг турли йўналишларидаги ечилмаган масалаларни ечишга хизмат қилди[15,17].

Поклингтон тестига асосланган туб сонларни генерация қилиш алгоритми. *Поклингтон Теоремаси*: $n = pR + 1$бўлсин ва *R* кўпайтувчининг тўлиқ ажратилган туб кўпайтувчилари маълум бўлади. Қачонки агар баъзи бир *a*<*n* учун қуйидаги шартлар бажарилса:

1) $a^{n-1} \equiv 1 mod n$,

2) Барча *R* га бўлинувчи *q* лар учун $q|R$, $НОД(a^{n-1/q}, n) \neq 1$бўлса, у ҳолда *n* сонини ихтиёрий бўлувчисини 1 билан *R* модул бўйича солиштирамиз.

Қандайдир туб сон берилган бўлсин *p:*

1. Тасодифий равишда $p \leq R \leq 4p + 2$ оралиқда ётувчи жуфт сон *R* ни танлаймиз ва *n=pR+1* аниқлаймиз.
2. *n* ни туб кўпайтувчиларга ажратиб, кичик туб бўлувчиси йўқлигига текширамиз.
3. Ҳар хил қийматларда *a*<*p* учун, Рабби-Миллер тести ёрдамида *n* сонни тубликка текширамиз.

Бу усулнинг эффективлиги, туб соннинг тўлиқ тақсимланганлигига ва иккита қўшни туб соннинг орасидаги масофасига боғлиқ. Асимметрик криптографик алгоритмларда электрон рақамли имзони шакллантириш ва текшириш жараёнида туб сонларни ҳосил қилишда Поклингтон теоремасига асосланади[16].

Яна шундай катта сондаши туб сонларни ҳосил қилиш усуллари мавжудки, нафақат *n-1* туб бўлувчиларини, балки *n+1*,$n^2 + 1, n^2 + n + 1$сонларининг туб бўлувчиларини ишлатган ҳолда ҳисоблаш мумкин.

***p-1* ни маълум бўлакларга ажратиш орқали туб сонларни яратишнинг рекурсив алгоритми.** Бу алгоритм 1994 йил Пред Михалуску томонидан таклиф қилинган бўлиб, туб сонларни ҳосил қилишда арифметик прогрессиядан фойдаланилади, яъни туб сонларни арифметик прогрессия орасидан қидиради. Танланган *p* сонни туб эканини исботлаш учун қуйидаги кетма кетликни бажарилади[16,22]:

Теорема 1. *(Рабин, 1980). Шундай m тоқ мураккаб сон топилсинки, НОД(6, m)=1 шарт бажарилсин. m-1=$2^n q$ тенгликни қаноатлантирувчи n, q бутун сон танлаб олинади ва ифода $S \in Z_m$ тўпламга тегишли деб айтиш мумкин бўлади қачонки қуйидаги икки шартдан бири бажарилса*

1. $a^q \equiv 1 (mod\ m)$,
2. $a^{2^k q} \equiv -1 (mod\ m)$ *бир нечта k учун,* $0 \leq k < n$.

Шунда S тўпламнинг қуввати $\frac{m}{4}$ *дан ошмайди.*

1. *p* сонни кичик туб сонга бўлинишини текширилади.
2. Катта туб бўлувчиларга эга бўлган мураккаб сонларни ажратиб олиш учун Рабби-Миллер тести бажарилади.
3. *p*сонни тублигини исботлаш учун Ламер, (*теорема 2*) теоремаси ишлатилади.

Теорема 2. (Ламер, 1927). $m > 0$ *тоқ сон берилган бўлсин. Агар m сони 3-теорема шартни қаноатлантирса ва* $f^2 \geq \sqrt{m}$ *бўлса, у ҳолда m- туб сон бўлади.*

Теорема 3. (Поклингтон, 1918**).** *Шундай m тоқ натурал сон берилган бўлсин, f соннингкўпайтувчилари таркибига кирувчи барча туб сонлар* q_k, $k = 1, \dots n$ *учун, баъзи бир m лар билан ўзаро туб бўлган шундай* a_k *бутун сон топилиб,* $a_k^{m-1} \equiv 1\ (mod\ m)$ ва $\text{НОД}\left(a_k^{\frac{m-1}{q_k}} - 1, m\right) = 1$ *шартлар*

бажарилса ҳамдар сонит нинг ихтиёрий туб бўлувчиси бўлса, у ҳолда $p \equiv 1(mod\, f)$*бўлади. Исбот:* Агар 3-теорема шартлари бажарилса, у ҳолда *m* нинг иҳтиёрий туб бўлувчиси *p* учун$p=1+kf$ шарт бажарилади, бир қанча $k \in Z$ учун. Шундай экан иҳтиёрий *p* туб бўлувчи учун$p = 1 + kf \geq 1 + \sqrt{m} > \sqrt{m}$ шарт бажарилади, бу эса 1-Леммага зид. Келиб чиққан зиддият эса исботни тасдиқлайди.

1-Лемма.n>1 бўлган мураккаб соннинг энг кичик туб бўлувчисир, $p \leq \sqrt{n}$*шартни қаноатлантиради.*

1-Лемма исботи. n=pm бўлсин, бу ерда *p, n* соннинг энг кичик туб бўлувчиси, у ҳолда $n > m > p > 1$бўлади. Агар $p > \sqrt{n}$ деб ҳисобланса, у ҳолда қуйидаги тенгсилик бажарилади $n = pm > p^2 > (\sqrt{n})^2 = n,$ бу эса зиддиятни келтириб чиқаради ва бу леммани тасдиқлайди.

Мисол-1. $m = 156 \cdot 5^{202} + 1$ ҳол учун қараймиз. ЭҲМ дан фойдаланиб қуйидагини топамиз.

$$13^m \equiv 1\ (mod\, m)\text{ва НОД}\left(13^{156 \cdot 5^{201}}, m\right) = 1,$$

шундай экан *m* нинг ҳар қандай *p* туб бўлувчиси учун $p = 1 + k5^{202}$ кўринишга ега бўлади. Модомики $5^{202} > \sqrt{m}$ бўлса, у ҳолда *m* туб сон бўлади.

Келтирилган бу алгоритмда$p = kq + 1$ кўринишидаги туб сон топилади, бу ерда *q*, $q > \sqrt{p}$ тенгсизликни қаноатлантирувчи туб сон, *k* иҳтиёрий бутун жуфт сон. Бу алгоритмда иккита берилган натурал сон орасидаги туб сон топилади, яъни шундайиккита *A,B* натурал сон бериладики *B>A+1,* қуйидаги тенгсизликни қаноатлантирувчи *p* туб сон топилади

$$A<p<B. \quad (1)$$

1-тенгсизликдан q ва k ни баҳолаш мумкин бўлади. Модомики $q, q > \sqrt{p}$ шартни қаноатлантирувчи бутун сон бўлса, у ҳолда 1-тенгсизликдан q устидан қуйидаги баҳолаш келтиртлади

$$q \geq \lceil \sqrt{B} \rceil > \sqrt{p}.$$

$q_A = \lceil \sqrt{B} \rceil$ деб белгиланади ва q туб сони юқоридан чегараланади, яъни ихтиёрий ҳақиқий $\alpha > 1$сон учун$q_A \leq q \leq \alpha q_A$ деб оламиз, у ҳолда k учун қуйидаги баҳолаш бажарилади.

Агар $k < \left\lfloor \frac{B-1}{\alpha q_A} \right\rfloor$ бўлса, у ҳолда қуйидаги бажарилади

$$p = kq + 1 \leq k\alpha q_A + 1 < \alpha q_A \frac{B-1}{\alpha q_A} + 1 = B$$

ва p учун юқоридан баҳолаш тўғри бўлади.

Ҳудди шундайин, агар $k \geq \left\lceil \frac{A}{q_A} \right\rceil$ бўлса, у ҳолда қуйидаги бажарилади

$$p = kq + 1 > kq \geq kq_A \geq q_A \frac{A}{q_A} = A,$$

ва p учун қуйидан баҳолаш тўғри бўлади. Бундан k қиймат учун оралиқ бўш бўлмаслиги келиб чиқади, αпараметр қиймати устидан баҳолаш юқоридан олинади. Ҳақиқатдан $\left\lceil \frac{A}{q_A} \right\rceil < \left\lfloor \frac{B-1}{\alpha q_A} \right\rfloor$тенгсизликдан қуйидагига эга бўламиз, α юқоридан $\frac{B-1}{A}$ қиймат билан юқоридан чегараланган, яъни қуйидаги оралиққа тегишли бўлади

$$1 < \alpha < \frac{B-1}{A}. \quad (2)$$

Модомики $\frac{B-1}{A} > 1$миқдор, шундай A,B қийматлар учун $B>A+1$ экан, кўрсатилган оралиқ бўш бўлмайди. Алгоритмда α қийматни $\alpha = \frac{B+A-1}{2A}$ кўринишида ишлатилади.

Шундай қилиб туб сон арифметик прогрессия $p_k = kq + 1$орасидан топилади, берилган оралиқда жуфт k ларини саралаган ҳолда ва k ни қийматини кетма-кет иккига ошириб борилади.

Ушбу бажарилган тартибни оптималлаштириш учун, қуйидаги фактга асосланади. Фараз қилинсин p сони кичик туб сонларга $d_1, \dots, d_n$ажратилсин ва шундай $\delta_{1,\dots,}\delta_n$бўлишлардан қолдиқларни топилиб $p \equiv \delta_n (mod\ d_n)$ тенглик бажарилади. Фараз қилинсин қолдиқ $\delta_i \equiv 0\ (mod\ d_i)$ га тенг бўлади, $1 \le i \le n$, у ҳолда p сони d_iга бўлинади ва мураккаб сон ҳисобланади.

Кейинги сонни текшириш учун, $p + 2 \equiv \delta_i + 2\ (mod\ d_i)$ келтирамиз барча i лар учун, $i \le i \le n$. Шу тарзда кейинги сонни катта сонларга ажратмасдан кичик туб сонларга ажратиб қолдиқни топишимиз мумкин. Амалиётда $n=10$ деб олинади ва p сони қуйидаги туб бўлувчиларга бўлинишига текшириб кўрилади 3,5,7,11,13,17,19,23,29 ва 31 га. 2 сонини чиқариб ташланади сабаби, модомики p сони ҳар доим тоқ сон.

Алгоритм-1 (Туб сонларни ҳосил қилувчи алгоритм):

Кириш: $A+1<B$ тенгсизликни қаноатлантирувчи шундай A,B натурал сонлар.

Чиқиш: $2^A < p < 2^B$оралиққа тушувчи p туб сон.

1. Агар $B \le 2^{16}$бўлса, у ҳолда p тубсонни тасодифий равишда туб сонлар жалвалидан танлаб олиб, жараённи тугатиш керак.
2. Ўзгарувчиларни аниқлаб олиш $q_A = \lceil \sqrt{B} \rceil, \alpha = \frac{B+A-1}{2A}$ва $k_1 = \left\lceil \frac{A}{q_A} \right\rceil, k_2 = \left\lfloor \frac{B-1}{q_A} \right\rfloor$.
3. $k_n = k_2$аниқлаш. Ҳудди шу алгоритмдан фойдаланилиб, $q_A < q < \lfloor \alpha q_A \rfloor$ тенгсизликни қаноатлантирувчи q туб сон ҳосил қилинади.

4. $k_1 < k < k_n$ оралиққа тушувчи тасодифан k сон танлаб олинади. Агар k тоқ бўлса, у ҳолда $k = k - 1$ деб белгиланади. $k_s = k_n$,- $k_n = k$ни ва бутун сон $p=kq+1$ аниқлаб олинади.
5. $d_1 = 3$, ..., $d_{10} = 31$туб сонлар учун, p сонни туб $d_1, \dots, d_{10}$сонларга бўлгандаги қолдиқ$\delta_1, \dots, \delta_{10}$аниқланади, яъни $\delta_i \equiv p \pmod{d_i}$, $1 \le i \le 10$.
6. Барча i учун, $1 \le i \le 10$, $k = k + 2, p = p + 2q$ва $\delta_i = \delta_i + 2 \pmod{d_i}$ лар ҳисобланади.
7. Агар $k > k_s$ бўлса 4-қадамга қайтиш керак бўлади.
8. Агар индекс $i, 1 \le i \le 10$ аниқланиб ҳамда $\delta_i = 0$ бўлса, у ҳолда 6-қадамга қайтиш керак бўлади.
9. p сони учун Рабби-Миллер тести бажарилади. Агар тестдан ўта олмаса, у ҳолда 6-қадамга қайтиш керак бўлади.
10. Ҳисоблагич $n=10$ қийматини аниқлаш.
11. Тасодифий бутун a ва $n=n-1$ сони ҳисобланади.
12. Агар $\text{НОД}(a^k - 1,\ p) = 1$ ва $a^{p-1} \equiv 1 \pmod{p}$бўлса, у ҳолда p сон тублигини билдириб алгоритмни якурлаш керак бўлади.
13. Агар $n=0$ бўлса, у ҳолда 6-қадамга қайтиш керак, бошқа ҳолда 11-қадамга қайтиш керак бўлади.

Кучли туб сонларни ҳосил қилиш алгоритми. Кўпчилик иловаларда қўшимча шартлар ёрдамида туб сонларни ҳосил қилиш зарурати туғилади[25,40].

Тариф 1. *Биз p тоқ туб сонникучли туб деб аташ мумкин қачонки, агар шундай тоқ туб сонлар q, s ва r учун*

$$p \equiv 1 \pmod{q},\ p \equiv -1 \pmod{s},\ q \equiv 1 \pmod{r}, \quad (3)$$

тенглик бажарилса, ҳамда қуйидаги тенгмала билан тенг кучли бўлса

$$\begin{cases} p = kq + 1, \\ p = is - 1, \\ q = jr + 1, \end{cases}$$

бир нечта тоқ сонлар учун i, j, k.

Модомики юқорида келтирилган 1-алгоритм p туб сонни ҳосил қилиш имконини берсада, (3) тенгликдаги фақат биринчи ҳамда учинчи шартни қагоатлантиради, шунинг учун кучли туб сонни ҳосил қилиш учун бир мунча ўзгартиришларни ўтказиш керак бўлади.

1979 йилда Вильям ва Шмидт (H.C. Williams & B. Schmid)лар қуйида келтирадиган алгоритмни таклиф қилишди.

Фараз қилинсин иккита туб сони r, s ҳосил қилинди ва қолган иккита туб сонларни pва q ни ҳосил қилиш керак бўлади (3)-тенглик шартлари бажарилиши учун. Бунинг учун $a \geq 1$ бўлган сон олиб, шундай x бутун сони топиладики, $x \equiv -\frac{(1+a)}{ar} \ (mod\ s)$тенгликни қаноатлантиради ҳамда арифметик прогрессия орасидан q туб сони топилади

$$q = (ks + x)r + 1, \qquad k = 0,1, \ldots$$

Шундай q сонни топиш учун 1-алгоритмга ўхшаш саралаш алгоритмдан фойдаланиш мумкин. Қачонки, агар $p = 2aq + 1$сони туб бўлса, изланаётган кучли туб сони қуйидаги тенгламадан топилади.

$$p = 2aq + 1 = 2a\big((ks + x)r + 1\big) + 1) + 1 = 2aksr + 2arx + (2a + 1) \equiv$$
$$\equiv -1 \ (mod\ s).$$

Агар $r > \sqrt{q}$бўлса, у ҳолда Ламер теоремасидан фойдаланилиб q ни тублигини исботлагандек, p ни ҳам тублигини исботлаш мумкин бўлади.

Агар $a = 1$бўлса, у ҳолда pтуб сон $p = 2q + 1$ тенгликни қаноатлантиради. Бу тенгликни қаноатлантирувчи p ва q туб сонлар эгизак-туб сон деб аталади ва камдан-кам ҳолатларда учрайди. Шунинг учун, амалиётда ҳисоблаш жараёнида a ни етарлича катта қилиб олинади.

Кучли туб p сонни ҳосил қилиш алгоритмини келтиришдан олдин, параметрлар устидан қуйидан ва юқоридан баҳолаш келтирилади, қайсики аниқланилиши лозим бўлган. Қуйидаги тенгсизликни *қаноатлантирувчир* туб сонни ҳосил қилинади

$A < p < B$ бўлса, у ҳолда $q_A = \left\lceil \frac{A-1}{2a} \right\rceil \le q = \frac{p-1}{2a} \le \left\lfloor \frac{B-1}{2a} \right\rfloor = q_B$ бўлади,

бир нечта бутун шундай *A, B*сон учун, B$< A + 2a$бажарилади. Ламер теоремасидаги *p*ни тублигини исботловчи шарт бажарилиши учун, $q > \sqrt{p}$ шарти бажарилиши лозим. Шундай қилиб a устидан юқоридан баҳоланилади

$$\frac{B-1}{2\sqrt{A}} > \frac{p-1}{2q} = a.$$

Енди, ҳудди юқоридагидек, r устидан баҳолаш олинади. Ламер теоремаси бажарилиши учун ва q ни тублигини исботлаш учун, қуйидаги белгиланади

$$r \ge \left\lceil \sqrt{q_A} \right\rceil = r_A,$$

у ҳолда бир нечта ҳақийқий $\alpha > 1$ параметр учун $\lfloor \alpha r_A \rfloor \ge r \ge r_A$бўлади.

Агар $ks + x \le \left\lfloor \frac{q_B - 1}{\alpha r_A} \right\rfloor$бўлса, у ҳолда юқоридан баҳолаш бажарилади

$$q = (ks + x)r + 1 < \frac{q_B - 1}{\alpha r_A} \alpha r_A + 1 \le q_B.$$

Ҳудди шундай, агар $ks + x \ge \left\lceil \frac{q_A}{r_A} \right\rceil$бўлса, у ҳолда қуйидан баҳолаш бажарилади

$$q = (ks + x)r + 1 \ge \frac{q_A}{r_A} r_A + 1 > q_A.$$

Шундай тарзда, сараланаётган k параметр устидан қуйидан ва юқоридан чегаралар олинади.

$$\left\lfloor \frac{q_B - 1}{\alpha r_A} \right\rfloor \ge (ks + x) \ge \left\lceil \frac{q_A}{r_A} \right\rceil. \quad (4)$$

Сараланаётган интервал бўш бўлмаслигидан келиб чиққан ҳолда, α параметр устидан юқоридан баҳолашга эга бўлинади. Ҳақиқатдан $\alpha < \frac{q_B-1}{q_A} < \frac{B-2a}{A}$ бўлганда кўрсатилган оралиқ бўш бўлмайди. Амалиётда ҳисоблашлар амалга ошираётганда α ни қиймати $\alpha = \frac{q_B+q_A-1}{2q_A}$ бўлади.

(4)-тенгсизликдан келиб чиқиб, *k* учун баҳолашга эга бўлинади

$$\left\lfloor \frac{q_B-1}{\alpha s r_A} \right\rfloor - x \geq k \geq \left\lceil \frac{q_A}{s r_A} \right\rceil - x,$$

шунингдек *s* устидан юқоридан баҳолашга эга бўлинади. Модомики қуриш давомида $s > x > 0$ ва $k \geq 1$ бўлса, у ҳолда қуйидаги тенгсизликка эга бўлинади

$$\frac{q_B-1}{\alpha r_A} \geq \left\lfloor \frac{q_B-1}{\alpha r_A} \right\rfloor \geq (k+1)s > ks + x,$$

бундан $s < \left\lfloor \frac{q_B-1}{2\alpha r_A} \right\rfloor = s_A$тенгсизлик келиб чиқади, қайсики *s* ни юқоридан баҳолаш учун ишлатилувчи. Қуйидан баҳолаш учун $\lceil \sqrt{s_A} \rceil$ қиймати ишлатилади.

Алгоритм-2 таснифи(Кучли туб сонларни ҳосил қилувчи алгоритм):

Кириш: $A + 2 < B$ тенгсизликни қаноатлантирувчи шундай *A,B* натурал сонлар.

Чиқиш: $A < p < B$тенгсизликни қагоатлантирувчикучли *p* туб сон.

1. $1 \leq a \leq \left\lfloor \frac{B-1}{2\sqrt{A}} \right\rfloor$ тенгсизликни қаноатлантирувчи, тасодифий *a*натурал сони ҳисобланади.
2. $q_A = \left\lceil \frac{A-1}{2a} \right\rceil$, $q_B = \left\lfloor \frac{B-1}{2a} \right\rfloor$, $r_A = \lceil \sqrt{q_A} \rceil$, $\alpha = \frac{q_B+q_A-1}{2q_A}$ва $s_A = \left\lfloor \frac{q_B-1}{2\alpha r_A} \right\rfloor$ларни аниқланади.

3. 1-алгоритмдан фойдаланиб, $r_A < r < \lfloor \alpha r_A \rfloor$тенгсизликни қаноатлантирувчи *r* туб сони ҳисобланади.
4. 1-алгоритмдан фойдаланиб, $\lceil \sqrt{s_A} \rceil < s < s_A$тенгсизликни қаноатлантирувчи *s* туб сони ҳисобланади.
5. $x \equiv -\frac{(1+a)}{ar} \pmod{s}$тенгламани қаноатлантирувчи кичик мусбат бутун *x*сони ҳисобланади.
6. $k_2 = \left\lfloor \frac{q_B - 1}{asr_A} \right\rfloor - x$ва $k_1 = \left\lceil \frac{q_A}{sr_A} \right\rceil - x$ аниқланади.
7. Тасодифий сон *k*ни ҳисоблаш, $k_1 \le k \le k_2$.
8. Агар *x* ва *k*-жуфт бўлса, у ҳолда *k* ни *k=k+1*деб белгиланади 10-қадамга утилади.
9. Агар *x* ва *k*-тоқ бўлса, у ҳолда *k* ни *k=k+1* деб белгиланса.
10. $q = (ks + x)r + 1$ ва $p = 2aq + 1$ аниқланади.
11. $k = k + 2$, $q = q + 2sr$ ва $p = p + 4asr$ ҳисобланади.
12. Агар $k > k_2$бўлса, у ҳолда 3-қадамга қайтилади.
13. q сони учун Рабби-Миллер тести ўтказилади, агар тестдан ўта олмаса, у ҳолда 11-қадамга қайтилади.
14. p сони учун Рабби-Миллер тести ўтказилади, агар тестдан ўта олмаса, у ҳолда 11-қадамга қайтилади.
15. Ҳисоблагич *n=10* қиймати аниқланади.
16. Тасодифий бутун сон *a* ва *n=n-1* ҳисобланади.
17. Агар $\text{НОД}(a^{ks+x} - 1, q) = 1$ ва $a^{q-1} \equiv 1 \pmod{q}$ бўлса, у ҳолда 19-қадамга ўтилади.
18. Агар $n = 0$ бўлса, у ҳолда 11-қадамга ўтилади, акс ҳолда 16-қадамга ўтилади.
19. Ҳисоблашич $n = 10$ қиймати аниқланади.
20. Тасодифий бутун сон *a* ва *n=n-1* ҳисобланади.

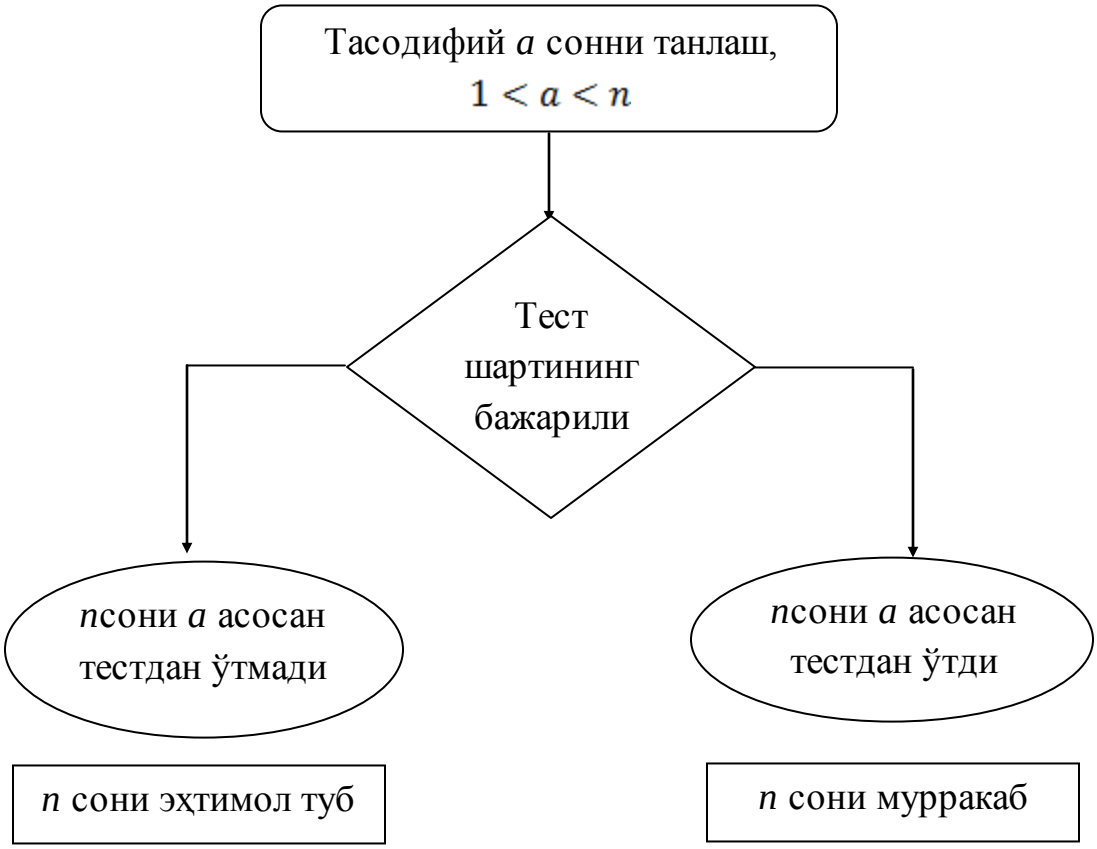
21. Агар $НОД(a^{q-1}-1,p)=1$ ва $a^{p-1}\equiv 1\ (mod\ p)$ бўлса, у ҳолда p сонни туб эканини билдирган ҳолда алгоритм якунланади.
22. Агар $n=0$ бўлса, у ҳолда 11-қадамга қайтилади, акс ҳолда 20-қадамга қайтилади.

2. Сонларни тубликка синаш алгоритмлари.

Очиқ калитли крипто тизимларда сонларни тубликка синаш, туб сонларни генерация қилиш алгоритмларининг таркибий қисми ҳисобланади. Сонларни тубликка алгоритмларини эҳтимолий ва детерминантланган алгоритмларга бўлиш мумкин.

Детерминантланган алгоритм ҳар доим бир ҳил схемадан фойдаланади ва масалаларни ечишда кафиллиги таъминланади. Эҳтимолий алгоритм тасодифий сон генераторидан фойдаланади ва аниқ бўлмаган жавобни беради. Умуман олганда эҳтимолий алгоритмлар самаралиги детерминантланган алгоритмларга қараганда кам эмас. Агар тасодифий сонларни генерация қилувчи алгоритмлар ҳар доим бир ҳил қиймат берса, кирувчи маълумотга боғлиқ ҳолда эҳтимолий алгоритм детерминантланган алгоритмга айланиши мумкин.

Бутун сон n ни туб сон эканлигини эҳтимолий алгоритм билан текшириш учун, тасодифий $1<a<n$ оралиқда ётувчи a сон танлаб олинади ва алгоритм шартларига текширилади. Агар n сони, а га асосланган ҳолда тестдан ўта олмаса, у ҳолда алгоритм "n сони мураккаб сон" деган натижа беради ва n сони ҳақиқатдан ҳам мураккаб сон ҳисобланади (1-расм).



1-расм. Сонларни тубликка синашнинг эҳтимолий алгоритми схемаси

Агар n сони a асосланиб тесдан ўтса, бу бизга n ни ҳақиқатдан ҳам туб сон эканини англатмайди. Кетма-кет ҳолда ҳар хил a лар учун ҳудди шундай тестлаш орқали бир қатор текширишларни ўтказиб ва ҳар бири учун "n сони эҳтимолан туб" деган жавоб олсак, n сонини бирга яқин эҳтимоллик билан туб сон эканини тасдиқлашимиз мумкин.

Ферма тести. Ферма кичик теоремасига биноан p туб сон ва ихтиёрий a бутун сон$1 \le a \le p-1$, учун қуйидаги тенглик бажарилади

$$a^{p-1} \equiv 1 \ (mod\ p). \quad (5)$$

Модомики, агар n тоқ сон учун шундай бутун a сони мавжуд бўлиб $1 \le a \le n$, $НОД(a,n) = 1$ ва $a^{n-1} = 1 \ (mod\ p)$ тенглик бажарилса, у ҳолда n сони мураккаб сон бўлади. Бу ердан қуйидаги, сонни тубликка синаш эҳтимолий алгоритмга эга бўлинади.

Алгоритм-3(Ферма тести).

Кириш: Тоқ бутун сон $n \geq 5$.

Чиқиш: " *n* сони эҳтимолан туб" ёки "*n* мураккаб сон".

1. Тасодифий *a* бутун сон танлаб олинади, $2 \leq a \leq n-2$.
2. $r \leftarrow a^{n-1} \ (mod\, n)$ ҳисобланади.
3. *r=1* бўлганда "*n* сони эҳтимолан туб" натижа олинади. Акс ҳолда: "*n* мураккаб сон" натижа олинади.

Ферма тестининг мураккаблиги "устун бўйича" кўпайтиришда $O(log^3 n)$ га тенг ва Шенхаге-Штрассен алгоритми бўйича кўпайтиришда $(tlog^2 nloglogn)$ га тенг.

Тариф 1. *n>0* сони тоқ мураккаб сон ва *n* билан ўзаро туб бўлган *a* сони ихтиёрий бутун сон бўлсин. *n* сони *a* га асосан псевдотуб дейилади, агар (5)-тенглик бажарилса, у ҳолда *n* сони учун 3-алгоритм "*n* сони эҳтимолан туб" деган жавобни беради.

Мисол-2. *n=527=17*31* сони 1, 154, 373, 526 сонларга асосан псевдотуб ҳисобланади, модомики $1^{526} \equiv 154^{526} \equiv 373^{526} \equiv 526^{526} \equiv 1 \ (mod\, 527)$ тенглама бажарилади.

Теорема 4. *n>0* тоқ мураккаб сон учун қуйидаги тасдиқлар тўғри.

1. *n* сони *a* асосга кўра псевдотуб ҳисобланади ўшанда ва фақат ўшанда, қачонки *n-1*,*n* модул бўйича *a* соннинг тартибига бўлинса.
2. Агар *n* сони *a* ва *b* асосларга кўра псевдотуб ҳисобланса, у ҳолда *n*сони$ab \ (mod\, n)$, $ab^{-1} \ (mod\, n)$, $a^{-1}b \ (mod\, n)$ асосларга кўра псевдотуб бўлади.
3. Агар *n* сони ҳеч бўлмаганда битта *a* асоснинг ўзига кўра псевдотуб бўлмаса, у ҳолда *n* нинг псевдутуб ҳисобланиши, $\frac{\varphi(n)}{2}$ нинг *a* асосга

кўра псевдотуб бўлишига нисбатан кўп бўлмайди, бу ерда φ - Эйлер функцияси.

Исбот. Агар *d*сони-*n* модул бўйича *a* соннинг тартибидаги сон бўлиб ва бир нечта бутун *k* сонлар учун $n-1=kd$тенглик бажарилса, у ҳолда тенгликнинг иккала томонини *k* даражага кўтарилма (5)- муносабатга келинади.

Тескари ҳолда, *n* сони *a* асосга кўра псевдотуб сон бўлса, у ҳолда $a^{n-1}\equiv 1\ (mod\ n)$ тенглик бажарилади ва *d* сони -*n* модул бўйича *a* нинг тартибидаги сон бўлади. *n-1* сонни *d* сонга қолдиқ билан бўлинганда: $n-1=qd+r$ тенглик бажарилади бир нечта бутун манфий бўлмаган *q* ва *r* сонлар учун, бундан қуйидаги тенглик келиб чиқади

$1\equiv a^{n-1}=a^{qd+r}=(a^d)^q\cdot a^r\equiv a^r(mod\ n).$

Лекин *a, 1*билан модул *n* бўйича таққосланишида , *d* -энг кичик даража ҳисобланади. Демак, $r=0$ бўлади ва $n-1$, *d* га бўлинади. Биринчи тасдиқ исботланди.

Агар $a^{n-1}\equiv 1\ (mod\ n)$ ва $b^{n-1}\equiv 1\ (mod\ n)$ тенглик бажарилса, у ҳолда бу тенгламаларнинг кўпайтмасидан $(ab)^{n-1}\equiv 1\ (mod\ n)$ тенгликка эга бўлинади. $a^{n-1}\equiv b^{n-1}\ (mod\ n)$ тенгликдан, $(ab^{-1})^{n-1}\equiv (a^{-1}b)^{n-1}\ (mod\ n)$га эга бўлинади. Иккинчи тасдиқ исботланди.

ва ниҳоята учинчи тасдиқ исботланилади. $\{a_1,a_2,\dots,a_k\}$- барча асослар тўплами бўлсин, қайсики *n* сони псевдотуб ҳисобланадиган, яъни $1\le a_i\le n-1$, $НОД(a_i,n)=1$ва $a_i^{n-1}\equiv 1\ (mod\ n)$ тенглик ўринли бўлади, $1\le i\le k$учун. *a*- шундай асос бўлсинки, *n* сони псевдотуб ҳисобланмасин, у ҳолда $1\le a\le n-1$, $НОД(a,n)=1$ ва $a^{n-1}\equiv 1\ (mod\ n)$ бўлади. $b_1\equiv aa_1\ (mod\ n)$, $b_2\equiv aa_2\ (mod\ n)$, ..., $b_k\equiv aa_k\ (mod\ n)$ сонлари кўриб чиқилиб ва фараз қилинадики, *n* сони b_i асосга кўра псевдотуб бўлади ҳеч

бўлмаганда битта i учун, $1 \le i \le k$. У ҳолда иккинчи тасдиққа мувофиқ, *n* сони псевдотуб ҳисобланади ва асосга кўра $ba_i^{-1} \equiv (aa_i)a_i^{-1} \equiv a(mod\, n)$ тенглик келиб чиқади, бу эса нотўғри. Бинобарин, *n* сони турли ҳил $b_1, b_2, \dots, b_k$ асосдаги ҳар бир *k* учун псевдотуб ҳисобланмайди. Шундай қилиб (5)- тенгликни қаноатлантирувчи сонлар, шу тенгликни қаноатлантирмайдиган сонларга нисбатан кўп эмас, $НОД(a_i, n) = 1$ шартдан эса улар $\frac{\varphi(n)}{2}$ дан кўп эмаслиги келиб чиқади.

Учинчи шартдан келиб чиқадики, агар *n* сони ҳеч бўлмаганда битта асосга кўра псевдотуб бўлмаса, у ҳолда $\frac{n-1}{2}$ асосга кўра ҳам псевдотуб бўлмайди.

Ихтиёрий $a > 1$ сон учун чексиз кўп *a* асосга кўра псевдотуб сонлар мавжуд.

Мисол 4. Агар *n* сони 2 асосга кўра псевдотуб бўлса, у ҳолда $2^n - 1$сони ҳам псевдотуб бўлиши кўрсатилсин. $2^{n-1} \equiv 1(mod\, n)$ бўлсин, яъни бир нечта бутун *k* ларучун $2^{n-1} - 1 = kn$ тенглик бажарилсин. Шунда

$$2^{2n-2} = 2^{2(2^{n-1}-1)} = 2^{2kn} = (2^n)^{2k} = 1^{2k} = 1\ (mod\ 2^n - 1)$$

тенглик келиб чиқади. Шу тарзда, 2 асосга кўра псевдотуб сонлар чекчиз кўп эканлиги қелиб чиқади.

Тариф 2. *n* мураккаб тоқ сон, *n* сони билан ўзаро туб бўлган, $1 \le a \le n - 1$, *a* нинг ихтиёрий қийматида (5) тенглик бажарилса, бу сон Кармайкл сони деб аталади. Бундай сонлар учун Ферма тести ҳар доим "*n* сони эҳтимолан туб" деган натижани беради.

Мисол 5. Кармайклнинг энг кичик сони - $561 = 3 \cdot 11 \cdot 17$, $1105 = 5 \cdot 13 \cdot 17$, $1729 = 7 \cdot 13 \cdot 19$, $6601 = 7 \cdot 23 \cdot 113$, $29341 = 13 \cdot 37 \cdot 61$.

Теорема 5. (Корселт мезони)**.** Тоқ мураккаб *n* сони Кармайкл сони ҳисобланади ўшанда ва фақат ўшанда, қачон:

1. *n* квадратлардан ҳоли бўлса;

2. *n* ни бўлувчи ҳар бир *p* учун, *n-1* сони *p-1* га бўлинади.

Исбот. Биринчи навбатда келтирилган хоссаларни қаноатлантирувчи сонни Кармайкл сони эканлиги исботланилади. *n* сони каноник ажратилган сон бўлсин $n = p_1 p_2 \dots p_k$ва *n* сони билан ўзаро туб бўлган ихтиёрий *a* бутун сон бўлсин, $1 \le a \le n-1$. Ферма кичик теоремасига биноан, $1 \le i \le k$,барча iлар учун $a^{p_i-1} \equiv 1 \ (mod\ p_i)$тенглик бажарилади. 2- хоссадан $n-1$сони $p_i - 1$га бўлиниши келиб чиқади, яъни баъзи бир бутун q_i сонлари учун $n - 1 = (p_i - 1)q_i$тенглик бажарилади. Шунда

$$a^{n-1} = a^{(p_i-1)q_i} \equiv 1 \ (mod\ p_i)$$

тенглик бажарилади, яъни *n*сонни барча p_iбўлувчилари учун, $a^{n-1} - 1$айирма p_i га бўлинади. Шундайин p_iсонлар турли ҳил бўлади, у ҳолда 2 хоссага асосан ўзаро туб сон $a^{n-1} - 1$ бўлинади ва $n = p_1 p_2 \dots p_k$кўпайтувчиларга ажралади. aсони ихтиёрий танланади, шунинг учун $a^{n-1} \equiv 1 \ (mod\ n)$ тенглик, $1 \le a \le n-1$, *a* нинг ихтиёрий қиймати учун ўринли бўлади ва демак *n* сони Кармайкл сони ҳисобланади.

Энди Кармайклнинг ҳар қандай сони 2 хоссани қаноатлантириши исботланади. $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ифода *n* соннинг каноник кўпайтувчиларга ажралган ифодаси бўлсин. Ихтиёрий $p \ne 2$туб сон учун, *p* модул бўйича бошланғич илдизи мавжуд, шунга кўра ҳар бир p_iучун $p_i - 1$ тартибли a_iсони топилади. У ҳолда $a_i^{n-1} \equiv 1 (mod\ n)$шартдан $n-1$ сони $p_i - 1$га бўлиниши келиб чиқади.

Кармайкл сони квадратлардан ҳоли эканлиги исботланилади. $n = p^t r$бўлсин, бу ерда $t \ge 2$. *n* сони билан ўзаро туб бўлган ихтиёрий *a* учун

$a^{n-1} \equiv 1\ (mod\ n)$тенглик бажарилади, у ҳолда $a^{n-1} \equiv 1\ (mod\ p^2)$тенглик ўринли бўлади. a сифатида p^2модул бўйича бошланғич илдиз оламиз, яъни $p(p-1)$тартибли сон. У ҳолда $n-1$ сони $p(p-1)$га бўлиниши керак, яъни $n-1$сони pга бўлиниши керак. Бу эса n сонни p га бўлиниш аломатига зид.

Натижа: Ихтиёрий Кармайкл сони учтадан кам бўлмаган ҳар хил туб сооннинг кўпайтмаси ҳисобланади[22, 23].

Мулоҳаза: 5 - теоремадаги иккинчи шартни қуйидагича ёзиш мумкин: $n-1$ сони $\text{НОК}(p_1-1, p_2-1, \dots, p_s-1)$ га бўлиниши керак. Бу ердан қуйидаги Кармайкл сонини генерация қилиш усули олиниши мумкин.

Мисол 6. $p_1 = 6k+1$, $p_2 = 12k+1$, $p_3 = 18k+1$кўринишдаги туб сонлар қаралмин. $n = p_1 p_2 p_3$ сони Кармайкл сони эканлиги исботлансин.

Ферманинг кичик теоремасига биноан, p_1сони билан ўзаро туб бўлган ихтиёрий a сони учун $a^{6k} \equiv 1\ (mod\ p_1)$ тенглик бажарилади. Шу каби $a^{12k} \equiv 1\ (mod\ p_2)$, $a^{36k} \equiv 1\ (mod p_3)$ тенглик ҳам бажарилади. $36k$ сони, $6k$, $12k$, ва $18k$сонларнинг умумий квадратидан кичик бўдмайди, у ҳолда қолдиқлар ҳиқидаги хитой теоремасига асосан n билан ўзаро туб бўлган барча a сонлар учун $a^{36k} \equiv 1\ (mod\ n)$ тенглик бажарилади. Лекин $n-1 = 1296k^2 + 396k + 36k = 36k(36k^2 + 11k + 1)$ бўлади, демак n билан ўзаро туб бўлган барча a лар учун $a^{n-1} \equiv 1\ (mod\ n)$ бўлади.

Кармайкл сонини генерация қилиш учун қуйидаги алгоритмдан фойдаланиш мумкин [7].

Алшоритм-4(Эрдеш алгоритми 1956).

Кириш: Кучли мураккаб сон $m > 0$.

Чиқиш: Кармайкл сони.

1. $\text{НОД}(m, p) = 1$ва $p-1$га бўлинувчи m сони учун, p туб сонлардан иборат S тўплам тузилади.

2. S тўпламдан шундай сон танланадики $p_1, p_2, \dots, p_r$, $r \geq 3$, $p_1 p_2 \dots p_r \equiv 1 \ (mod\ m)$ тенглик бажарилади.
3. Белгилаб олинади $n \leftarrow p_1 p_2 \dots p_r$.
4. Натижа: n.

Мисол 7. $m = 120 = 2^3 \cdot 3 \cdot 5$иборат бўлсин.

$S = \{7, 11, 13, 31, 41, 61\}$ тўплам тузилсин. S тўплам элементлари қанчалик кўп бўлса, шунчалик Кармайкл сони кўп бўлади. S тўпламнинг бўлиши мумкин бўлган элементларини саралаб олсак, қуйидагига эга бўламиз:

$41041 = 7 \cdot 11 \cdot 13 \cdot 41 \equiv 1 \ (mod\ 120)$,

$852841 = 11 \cdot 31 \cdot 41 \cdot 61 \equiv 1 \ (mod\ 120)$

сонлари Кармайкл сони бўлади.

Кармайкл сонини чексиз кўп учратишимиз мумкин. Етарли даражада катта бўлган n сони учун қуйидаги тенгсизлик ўринли бўлади.

$$n^{\frac{2}{7}} < C(n) < n \exp\left(-\frac{\ln n \ln\ln\ln n}{\ln\ln n}\right),$$

Бу ерда $C(n)$ – Кармайкл сонининг nдан кичик миқдори[6, 25].

Агар n сони Кармайкл сони ҳисобланса ва унинг туб бўлувчилари етарли катта бўлса, у ҳолда катта эҳтимоллик билан Ферма тести n сонни туб деб эълон қилади. Агар ферма тестида a асос тасодифан эмас, олдиндан аниқлаб олинган бўлса, у ҳолда уни Кармайкл сонига тўғри келувчи сон билан алдаш мумкин. Бу камчиликни янада муккаммалроқ мезонлар билан қуйидаги тест орқали бартараф қилиш мумкин.

Словея-Штрассен тести. Бу тестни асосида қуйидаги теорема ётади.

Теорема 5(Эйлер мезони). Тоқ n сони туб ҳисобланади, шундаки ва фақат шундаки, қачонкиn билан ўзаро туб бўлган, $1 \leq a \leq n-1$, ихтиёрий a учун қуйидаги тенглик бажарилади[25]

$$a^{\frac{n-1}{2}} \equiv (\frac{a}{n})(mod n). \quad (6)$$

Исбот. Агар *n*сони туб бўлса, у ҳолда (6) – тенглик Лежандр символи бўлади. Тенглик бажарилган бўлсин ва *n* сони мураккаб сон бўлсин. У ҳолда

$$a^{n-1} = (a^{\frac{n-1}{2}})^2 \equiv \left(\frac{a}{n}\right)^2 = 1 \ (mod\ n)$$

тенглик бажарилади.

Шу тарзда, теорема шартини қаноатлантирувчи ихтиёрий a сони учун (5) – тенглик бажарилади ва *n* сони Кармайкл сони ҳисобланади. 4-теореманинг иккинчи хоссасига биноан, n соннинг каноник ажралмаси, $n = p_1 p_2 \dots p_s$ кўринишга эга бўлади. b сони p_1 модул бўйича кадврат чегирма бўлмасин, яъни $\left(\frac{b}{p_1}\right) = -1$ бўлади. Қолдиқлар хақидаги хитой теоремасига асосан шундай a сон топиладики натижада қуйидаги тенглик бажарилади

$$a \equiv b \ (mod\ p_1),\ a \equiv 1 \ (mod\ p_2),\ \dots,\ a \equiv 1 \ (mod\ p_s). \quad (7)$$

Якоби символи ҳисобланилади:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_s}\right) = \left(\frac{b}{p_1}\right)\left(\frac{1}{p_2}\right)\dots\left(\frac{1}{p_s}\right) = \left(\frac{b}{p_1}\right) = -1.)$$

Бу қийматни (6) тенгламага қўйиб, $a^{\frac{n-1}{2}} \equiv -1 \ (mod\ n)$ га эга бўлинади, демак барча $1 \le i \le s$, i лар учун, $a^{\frac{n-2}{2}} \equiv -1 \ (mod\ p_i)$ тенглик (7) - шартга зид бўлади. Эйлер мезони қуйидаги тубликнинг эҳтимолий тестига асосланган [10].

Алгоритм 5. Словэя - Штрассен тести

Кириш. $n \ge 5$ бўлган тоқ бутун сон.

Чиқиш. "*n* сони эҳтимолан туб" ёки "*n* сони мураккаб".

1. Тасодифий бутун *a* сони танланади, $2 \le a \le n-2$.
2. $r \leftarrow a^{\frac{n-1}{2}} (mod\ n)$ ҳисобланади.

3. $r \neq 1$ ва $r \neq n-1$ бўлганда натижа: "*n* сони мураккаб".

4. Якоби символи ҳисобланади $s \leftarrow \left(\frac{a}{n}\right)$.

5. $r \equiv s \ (mod\, n)$ бўлганда натижа: "*n* сони мураккаб". Акс ҳолда натижа: "*n* сони эҳтимолан туб".

Словэя-Штрассен тести мураккаблиги Якоби символини ҳисоблаш мураккаблиги билан аниқланади ва у $O(log^3 n)$ га тенг.

Тариф 3. *n* сони мураккаб тоқ сон бўлсин ва *n* билан ўзаро туб бўлган *a* ихтиёрий бутун сон бўлсин, $2 \leq a \leq n-1$. *n* сони *a* асосга кўра эйлер псевдотуб сони дейилади, агар (6) - тенглик бажарилса, яъни агар *n* сони учун 5-алгоритм "*n* сони эҳтимолан туб" деган натижани берса.

5-Теорема шуни кўтсатадики, Соловэя-Штрассен тести учун Кармайкл сонларига ўхшаш сонлар мавжуд эмас. Бундай натижани 1976 йил Д.Лемер, Р.Соловэем ва Ф.Штрассенлар томонидан олинган.

Мисол 8. $n = 527 = 17 \cdot 31$ сони эйлер псевдртуб сони ҳисобланади, 1 ва 526 асосларга кўра, модомики $1^{263} \equiv 526^{263} \equiv 1 \ (mod\, 527)$ ва $\left(\frac{1}{527}\right) = \left(\frac{526}{527}\right) = 1$.

Мисол 9. $n = 561$ сони учун Ферма тести *a* асосга кўра барча $320 = \varphi(561)$ учун "*n* сони эҳтимолан туб" натижа олинади. Шу сон учун Словэя-Штрассен тести ҳудди шундай натижа беради фақат *a* асосга кўра $80 = \frac{\varphi(561)}{4}$

учун. $a = 5$ бўлганда $a^{\frac{n-1}{2}} = 5^{280} \equiv 67 (mod\, n)$ га тенг натижа олинади ва 3-қадамда "*n* сони мураккаб сон" натижа олинади. $a = 13$ бўлганда $a^{\frac{n-1}{2}} = 13^{280} \equiv 1 \ (mod\, n)$, лекин $\left(\frac{13}{561}\right) = -1$ бўлади ва 5-қадамда "*n* сони мураккаб" натижа олинади.

Теорема 6. *n* мураккаб тоқ сон учун қуйидаги тасдиқ ўринли бўлади.

1. Агар *n* сони *a* асосга кўра эйлер псевдотуб сони ҳисобланса ва ҳудди шундайин *b* асосга кўра эйлер псевдотуб сони ҳисобланмаса, у ҳолда $ab(mod\ n)$ асосга кўра эйлер псевдотуб сони ҳисобланмайди.
2. Агар *n* сони *a* ва *b* асосларга кўра эйлер псеадотуб сони ҳисобланса, у ҳолда *n* сони $ab\ (mod\ n)$, $ab^{-1}\ (mod\ n)$ ва $a^{-1}b\ (mod\ n)$ асосларга кўра эйлер псевдотуб сони ҳисобланади.
3. Агар *n* сони ҳеч бўлмаганда битта *a* асосга кўра эйлер псеадотуб сони ҳисобланмаса, у ҳолда *n* сони, $\frac{\varphi(n)}{2}$ асосга кўра эйлер псеадотуб сони ҳисобланади.
4. Агар *n* сони *a* асосга кўра эйлер псевдутуб сони ҳисобланса, у ҳолда бу сон *a* асосга кўра псевдотуб сон ҳисобланади.

Рабби-Миллер тести. Ҳозирги кунда сонларни тубликка текшириш учун кўпроқ Рабби-Миллер тестидан фойдаланилмоқда. У қуйидагиларга асосланган. *n* сони тоқ сон бўлсин ва $n-1=2^s r$ тенглик бажарилсин, бу ерла *r* - тоқ сон. Агар *n* туб бўлса, у ҳолда *n* билан ўзаро туб бўлган ихтиёрий $a \geq 2$ сон учун (5) - тенглик бажарилади. a^{n-1} сонни кўпайтувчиларга ажратамиз:

$$a^{n-1}-1=a^{2^s r}-1=\left(a^{2^{s-1}r}-1\right)\left(a^{2^{s-1}r}+1\right)=$$
$$=\left(a^{2^{s-2}r}-1\right)\left(a^{2^{s-2}r}+1\right)\left(a^{2^{s-1}r}+1\right)=\cdots=$$
$$=(a^{2r}-1)(a^{2r}+1)\ldots\left(a^{2^{s-2}r}+1\right)\left(a^{2^{s-1}r}+1\right)=$$
$$=(a^{r}-1)(a^{r}+1)(a^{2r}+1)\ldots\left(a^{2^{s-2}r}+1\right)\left(a^{2^{s-1}r}+1\right).$$

У ҳолда оҳирги кўпайтма натижасидан ҳеч бўлмаганда қавсларнинг бири *n* га бўлинади, яъни ёки $a^r \equiv 1\ (mod\ n)$, ёки a^r, a^{2r}, ..., $a^{2^{s-1}r}$ сонлари орасидан *n* модул бўйича *-1* билан таққосланадигани топилади. Рабби-Миллер тести ушбу хосса асосида амалга оширилади.

Алгоритм 6. Рабби-Миллер тести.

Кириш. $n \geq 5$ бўлган тоқ бутун сон.

Чиқиш. "*n* сони эҳтимолан туб " ёки "*n* сони мураккаб сон".

1. $n-1$ ни $n-1=2^s r$ кўринишида ифодалаш, бу ерда r тоқ сон.
2. Тасодифий бутун *a* сони танланади, $2 \leq a \leq n-2$.
3. $y \leftarrow a^r (mod\, n)$ ҳисобланади.
4. $y \neq 1$ ва $y \neq n-1$ бўлганда қуйидаги амаллар бажарилади.

   4.1. $j \leftarrow 1$ деб белгиланади.

   4.2. Агар $j \leq s-1$ *ва* $y \neq n-1$ бўлса, у ҳолда

   4.2.1. $y \leftarrow y^2\ (mod\, n)$ деб белгиланади.

   4.2.2. $y=1$ бўлганда натижа: "*n* сони мураккаб сон" бўлади.

   4.2.3. $j \leftarrow j+1$ деб белгилаш.

   4.3. $y \neq n-1$ бўлганда натижа: "*n* сони мураккаб сон" бўлади.
5. Натижа: "*n* сони эҳтимолан туб".

Бу шуни англатадики, *n* туб сон учун $y^2 \equiv 1$ таққослама ечими $y \equiv \pm 1\ (mod\, n)$ бўлади. Агар *n* сони мураккаб сон бўлиб ва $k > 1$ бўлганда ҳар хил туб бўлувчилврга эга бўлса, у ҳолда қолдиқлар ҳақидаги хитой теоремасига асосан $y^2 \equiv 1\ (mod\, n)$ таққосланинг 2^k та ечими мавжуд. Ҳақиқатдан ҳам *n* соннинг ихтиёрий p_i туб бўлувчиси учун, берилган таққосланинг иккита ечими мавжуд бўлади: $y \equiv \pm 1\ (mod\, p_i)$.

Бу алгоритмнинг мураккаблик даражаси қиймати $O((\log n)^3)$ га тенг.

Тариф 4. *n* сони тоқ туб сон бўлсин, r - тоқ бўлганда, $n-1=2^s r$ тенглик бажарилсин ва *n* билан ўзаро туб бўлган *a* ихтиёрий бутун сон бўлсин, $1 \leq a \leq n-1$. *n* сони *a* асосга кўра кучли туб сон дейилади, агар

$a^r \equiv 1$ бўлса ва агар шундай бутун j сон учун, $0 \le j \le s-1$, $a^{2^j r} \equiv -1 \ (mod\, n)$ тенглик бажарилса.

Мисол 10. $n = 105 = 3 \cdot 5 \cdot 7$ сон учун $n - 1 = 2^3 \cdot 13$ тенгликка келади, яъни $s = 3$, $r = 13$ бўлади. *105* сони *1* ва *104* асосларга кўра кучли псевдотуб сон ҳисобланади.

n тоқ мураккаб сонни Рабби-Миллер тести, даражаси бўйича туб бўмаган сонни, туб деб элон қилиниш эҳтимоллиги $\frac{1}{4}$ дан кам бўлади.

Мулоҳаза. Агар *n* сони *a* ва *b* асосларга кўра кучли туб сон ҳисобланса, у ҳолда қоидага кўра *n* сони $ab \ (mod\, n)$ асосга кўра кучли туб сон ҳисобланади. Шунинг учун Рабби-Миллер тестидаги 2-қадамда *a* сонни тасодифан эмас, балки бошланғич бир нечта туб сонларни танлаш мумкин.

Лемма 2. Бир нечта бутун *a* сон учун, $a^{2^{s-1}r} \equiv -1 \ (mod\, n)$ тенглик бажарилсин, бу ерда $n - 1 = 2^s r$, p сони *n* нинг ихтиёрий туб бўлувчиси, $p - 1 = 2^{s'} r'$, r' сони тоқ. У ҳолда

$$\left(\frac{a}{p}\right) = \begin{cases} -1, & s' = s, \\ 1, & s' > s. \end{cases}$$

бўлади.

Исбот 2. $a^{2^{s-1}r} \equiv -1 (mod\, n)$ таққосламани иккала томонини r' тоқ даражага кўтарилади: $(a^{2^{s-1}r})^{r'} \equiv -1 \ (mod\, n)$. Бу таққослама *n* нинг ихтиёрий туб бўлувчиси модули бўйича, шу билан биргаликда *p* модул бўйича ҳам бажарилади. Агар $s' < s$ деб олсак, у ҳолда $a^{2^{s'} r'}$ ифода *1* билан *p* модул бўйича таққосланмайди, бу эса Ферманинг кичик теоремасига зид келади. Шунинг учун фақат $s' \ge s$ ҳолат учун бўлиши мумкин.

$s' = s$ бўлганда қуйидагига эга бўлинади

$$\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right)^r \equiv \left(a^{\frac{p-1}{2}}\right)^r = \left(a^{2^{s'-1} r'}\right)^r = \left(a^{2^{s-1} r'}\right)^r \equiv -1 \ (mod\, p).$$

$s' > s$ бўлганда, $\left(a^{2^{s-1}r}\right)^{r'} \equiv -1\ (mod\ p)$ таққосламани $2^{s'-s}$ даражага кўтарилма қуйидагига эга бўлинади

$$1 \equiv \left(\left(a^{2^{s-1}r}\right)^{r'}\right)^{2^{s'-s}} = \left(a^{2^{s'-1}r'}\right)^{r} = \left(\frac{a}{p}\right)^{r} = \left(\frac{a}{p}\right)(mod\ p).$$

Лемма 3. Бир нечта бутун a сони учун ва бир нечта бутун j учун $a^{2^{j-1}r} \equiv -1\ (mod\ n)$ таққослама бажарилсин, бу ерда $n-1 = 2^s r$, $1 \le j \le s-1$, n сонни ихтиёрий туб бўлувчиси p, $p-1 = 2^{s'} r'$, r' тоқ сон. У ҳолда

$$\left(\frac{a}{p}\right) = \begin{cases} -1, & s' = j, \\ 1, & s' > j. \end{cases}$$

бўлади.

Исботи юқоридаши леммага ўхшаш олиб борилади[2].

Теорема 7. Агар n сони a асосга кўра кучли туб сон ҳисобланса, у ҳолда бу сон a асосга кўра эйлер псевдотуб сони ҳисобланади.

Исбот[2]. $n-1$ сонни $n-1 = 2^s r$ кўринишида ёзамиз, бу ерда r сони тоқ сон. Қуйидаги уч ҳол қараб чиқилади.

1-ҳол. $a^r \equiv 1\ (mod\ n)$ таққослама бажарилсин. У ҳолда $a^{\frac{n-1}{2}} = a^{2^{s-1}r} = (a^r)^{2^{s-1}} \equiv 1\ (mod\ n)$ таққомлама ўринли бўлади. (6) - таққослама бажарилиши учун, a сони n модул бўйича квадрат чегирма бўлиши керак. Якоби символи хоссаларидан қуйидаги тенгликка эга бўлинади

$$1 = \left(\frac{1}{n}\right) = \left(\frac{a^r}{n}\right) = \left(\frac{a}{n}\right)^r = \left(\frac{a}{n}\right),$$

модомики r сони тоқ сон.

2-ҳол. $a^{\frac{n-1}{2}} = a^{2^{s-1}r} \equiv -1(mod\ n)$ таққослама бажарилсин. Энди a сон квадрат чегирма бўлмасин n модул бўйича. n сонни туб кўпайтувчиларга

ажратилади: $n = p_1 p_2 \dots p_m$, p_i ҳар хил бўлиши шарт эмас, ва $p_i - 1 = 2^{s_i} r_i$ тенглик бажарилади, r_i тоқ сон. *k* - p_i сонларнинг миқдори бўлсин, $s_i = s$ лар учун. 2-леммага асосан, барча i лар учун $s_i \geq s$ тенглик бажарилади, $\left(\frac{a}{n}\right) = \prod_i \left(\frac{a}{p_i}\right) = (-1)^k$ келиб чиқади.

Бундан ташқари, $p_i = 2^{s_i} r_i + 1 = 2^s r_i + 1 (mod\ 2^{s+1})$ тенг бўлади $s_i = s$ бўлганда, $p_i = 2^{s_i} r_i + 1 \equiv 1\ (mod\ 2^{s+1})$ тенг бўлади $s_i > s$ бўлганда ва $n = 2^s r + 1 \equiv 2^s + 1 (mod\ 2^{s+1})$ тенг бўлади. У ҳолда
$2^s + 1 \equiv n = p_1 p_2 \dots p_m \equiv (2^s + 1)^k \equiv k2^s + 1 (mod\ 2^{s+1})$ ўринли бўлади,
$k \equiv 1 (mod\ 2)$ келиб чиқади, яъни *k* тоқ сон ва $\left(\frac{a}{n}\right) = (-1)^k = -1$.

3-ҳол. Баъзи бир *j* лар учун, $1 \leq j \leq s - 1$, $a^{s^{s-1} r} \equiv -1 (mod\, n)$ бўлган ҳол қаралади. Таққосламани икки томонини керакли иккинчи даражага ошириш натижасида, $a^{\frac{n-1}{2}} \equiv 1 (mod\, n)$ га эга бўлинади. Шундай қилиб *n* сони эйлер псевдотуб сони бўлиши учун, *a* сони *n* модул бўйича квадрат чегирма бўлиши керак. Иккинчи ҳолдагидек $\left(\frac{a}{n}\right) = (-1)^k$ тенгликка эга бўламиз. 3-леммадан фойдаланган ҳолда ва олдинги ҳолдаги мулоҳазаларлан $n = 2^s r + 1 \equiv 1\ (mod\ 2^{j+1})$ ва
$1 \equiv n = p_1 p_2 \dots p_m \equiv (2^j + 1)^k \equiv k2^j + 1 (mod\ 2^{j+1})$ ларга эга бўлинади, $k \equiv 0\ (mod\ 2)$ келиб чиқади, яъни *k* тоқ сон ва $\left(\frac{a}{n}\right) = (-1)^k = 1$.

Шундай қилиб, агар *n* сони *a* асосага кўра кучли псевдотуб бўлса, у ҳолда *n* сони *a* асосга кўра эйлер псевдотуб сони бўлади. Агар *n* сони *a* асосга кўра эйлер псевдотуб сони бўлса, у ҳолда *n* сони *a* асосга кўра ҳам псевдотуб бўлади. Қуйида 2-жадвалда сонларни тубликка синаш алгоритмлари таҳлили келтирилган.

2-жадвал

Тубликка синаш алгоритмлари хусусиятлари

Тест	Тест тури	Қўлланиш қоҳаси
Ферма	Эҳтимолий	Катта сонларни тубликка синашда ишлатилади.
Рабби-Миллер	Эҳтимолий	Оқик калитли тизимларда узунлиги 512, 1024 ва 2048 битли туб калитларни ҳосил қилишда фойдаланилади.
Поклингтон	Детерминантланган	*n-1* ни маълум факторлаш орқали катта туб сонларга эга бўлиш.

Шундай қилиб катта туб сонларни генерация қилишда ҳамда уларни тубликка синашда алгоритмнинг математик ёндашувини инобатга олиш керак бўлади. Кўриб чиқилган алгоритмлар орасида Рабби-Миллер тести катта сонларни тубликка текширишда эҳтимолан ёндашиб якоби символи ҳамда лежандр хоссаларидан келиб чиқиб берилган сонни туб ёки мураккаб сонлигини бир неча мезонлар бўйича аниқлайди, бу эса унинг бардошлилигини таъминлаб беради.

II боб бўйича хулосалар

1. Очиқ калитли криптотизимларда бардошли калитлар туб сонларни ҳосил қилиш масалалари билан боғлиқлиги асосланди.

2. Мураккаблик даражаси катта бўлган туб сонларни генерация қилиш алгоритмлари тадқиқ этилди.

3. Ҳозирги кунда энг кўп қўлланиладиган сонларни тубликка синашнинг эҳтимолий алгоритмлари таҳлил қилинди.

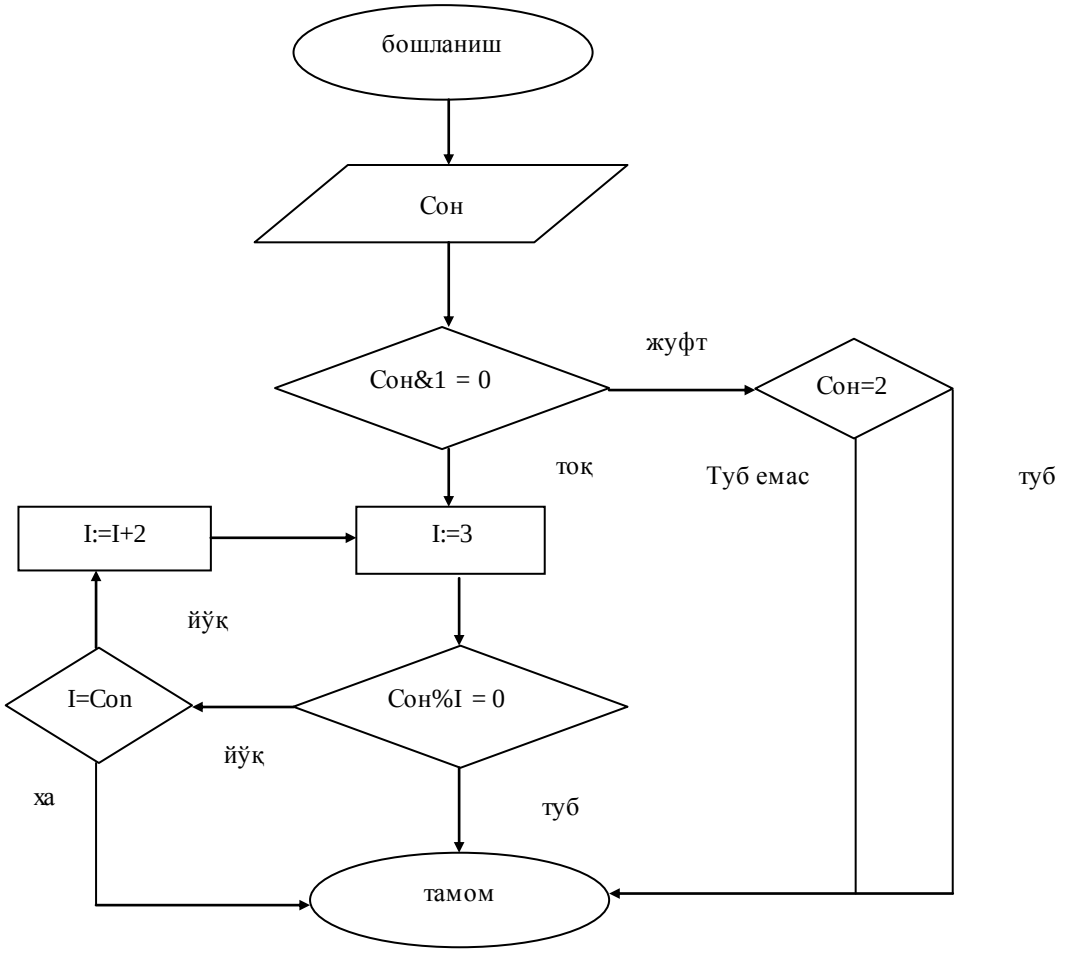
4. Мавжуд криптографик сонларни тубликка синаш алгоритмлари тахлил қилинди ва уларни тури, қўлланиш соҳаси бўйича тавсифланди.

Кучли туб сонларни ҳосил қилиш учун уларни мураккаб алгоритм бўйича генерация қилинган бўлса ҳам уларни тубликка синашда бир неча тубликка синаш тестларидан ўтказиш мақсадга мувофиқ бўлади ва бардошли калитларни ҳосил қилишда яхши самарага эришилади.

III боб. Бардошли калитларни генерация қилиш алгоритми ва унинг дастури

1. Бардошли калитларни генерация қилиш алгоритми

Криптографияда туб сонлар муҳим аҳамиятга эга. Масалан, носимметрик тизимларда факторлаш ва дискрет логарифмлаш мураккаблигига асосланган тизимлар кўплаб учрайди ва улар очиқ калитли тизимларнинг асоси ҳисобланади. Шуларни ҳисобга олган ҳолда фойдаланиялаётган катта узунликдаги туб сонларни тубликка текшириш муҳим аҳамиятга эга. Ушбу қисмда тубликка текширувчи тестлар (иккинчи бобда келтирилган) асосида яратилаётган туб сонларни текшириш ва уларни тублигини аниқлаш масаласи кўриб чиқилади.

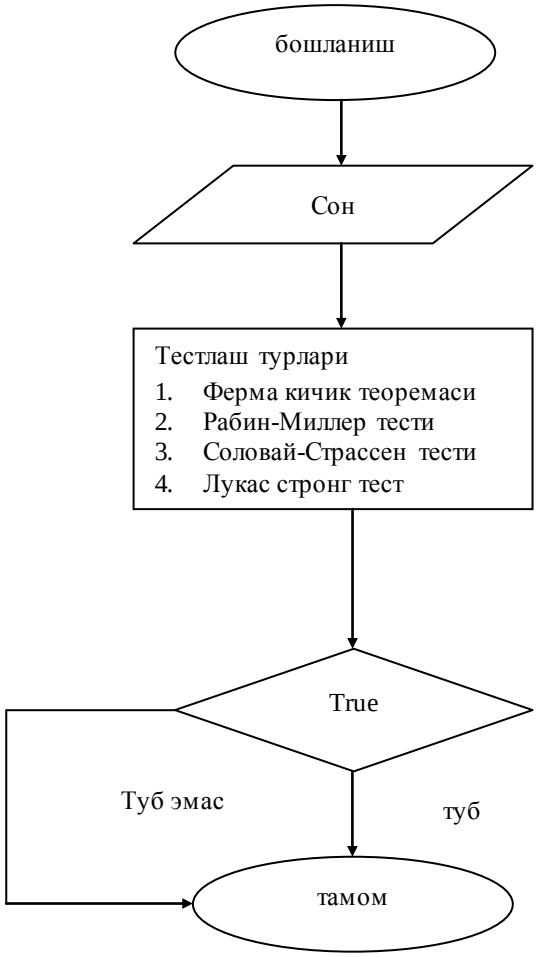


2- расм. Одатий туб сонларни ҳосил қилиш алгоритми

Одатий ҳолда фойдаланилган алгоритм 2-расмда кўрсатилган бўлиб, бунда, анаъвий усулдан фойдаланилган ҳолатда агар текширилаётган сон кичик бўлса вақтдан ютуқ беради, агар катта узунликка эга бўлганда дастурнинг ишлаш тезлиги пасайиб кетади. Бунда қуйидаги муаммо орқали жавоб бериш мумкин:

```
for (int i = 3; (i * i) <= candidate; i += 2)
      {
          if ((candidate % i) == 0)
          {
              return false;
          }
       }
```

Ушбу алгоритмдан кўриниб турибдики агар соннинг узунлиги оортиб борса, унда текширишлар сони кўпаяди ва натижада вақтдан ютқазилади.



3- расм. Туб сонларни ҳосил қилишнинг комбинациялашган алгоритми

Таклиф этилаётган комплекс тестлаш усуллари бўйича амалга оширилиб, бунда тестлаш усулларидан ихтиёрий миқдорда фойдаланиш мумкин. Тубликка текшириш тестлари сонининг ортиши билан сарфланадиган вақт ҳам ортиб боради.

Ушбу усулда тестлар мажмуи қуйидаги тестлардан ташкил топган:

- Ферманинг кичик теоремаси;
- Рабин-Миллер тести;
- Слован-Штрассет тести;
- Лукас стронг тести;

2. Бардошли калитларни генерация қилиш алгоритмининг дастури ва уни носимметрик тизимда қўллаш

Юқоридаги бўлимларда ассиметрик тизимларни қуришда асос қилинган мураккаблик турлари: этарли катта сонларни туб кўпайтувчиларга ёйиш, характеристикаси етарли катта бўлган чекли майдонларда дискрет логарифмларни ҳисоблаш масалаларини ечиш мураккабликлари билан боғлиқ бўлган тизимлар кўриб чиқилди. Замонавий криптографияда янги ҳисобланган, параметрли алгебра мураккабликларини криптографик тизимга тадбиқ этиш катта ютуқ беради.

Ушбу бўлимда бардошли туб сонлардан фойдаланган ҳолда параметрли алгебра мураккаблигига асосланган ассиметрик шифрлаш ва ЭРИ алгоритмларини дастури яратиш билан танишамиз.

Дастлаб парметрли алгебра амали ҳисобланган парметрли даражага ошириш ва параметрли кўпайтириш амаллари билан танишиб чиқсак. Қуйида p модуль бўйича R параметрли кўпайтириш ва даражага кўтаришнинг математик асоси келтирилган.

X ни Y га p модуль бўйича R параметрли кўпайтириш амали $X \circledR Y (mod\ p)$ кўринишда белгиланади ва қуйидаги кўринишда аниқланади[6]:

$$X \circledR Y (mod\ p) \equiv X + Y\,(1 + R\,X)\ (mod\ p).$$

Ушбу амал коммутатив ва ассоциатив амалдир.

X ўзгарувчини p модуль бўйича R параметрли тескарилаш амали $X^{\backslash -1}\ (mod\ p)$ шаклида белгиланади ва қуйидаги кўринишда аниқланади:

$$X^{\backslash -1}\ (mod\ p) \equiv -\,X\,(1 + R\,X)^{-1}\ (mod\ p),$$

бу ерда $X^{\backslash -1} \circledR X \equiv 0\ (mod\ p)$, 0 – параметрли группанинг бирлик элементидир.

Асос X ни p модуль бўйича R параметр билан d-даражага ошириш амали $X^{\backslash d}\ (mod\ p)$ кўринишида ифодаланади. Масалан, $d = 37$ бўлганда R параметр билан $X^{\backslash d}$ қуйидагича ҳисобланади:

$$X^{\backslash 37} \Rightarrow X^{\backslash 32+4+1}\ (mod\ p) \equiv ((((X^{\backslash 2})^{\backslash 2})^{\backslash 2})^{\backslash 2})^{\backslash 2} \circledR (X^{\backslash 2})^{\backslash 2} \circledR X\ (mod\ p),$$

$$\text{бу ерда: } X^{\backslash 2}\ (mod\ p) \equiv X\,(2 + X\,R)\ (mod\ p).$$

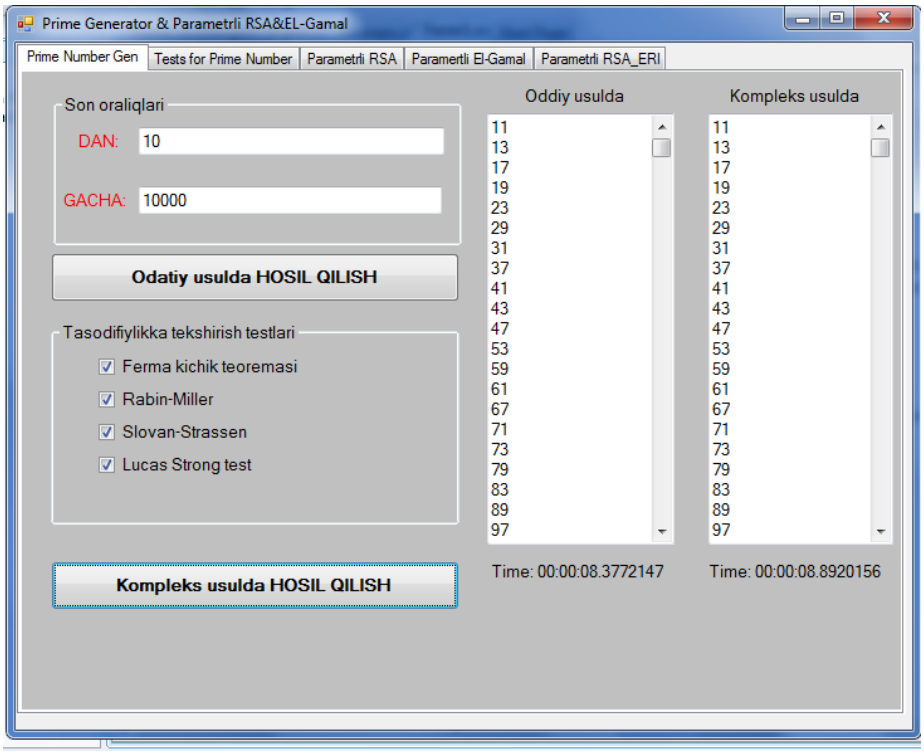
Ушбу криптографик дастурий восита Visual C# дастурлаш тилида яратилган бўлиб, ушбу дастур ишлаши учун .Net Framework 3.5 компонентасини ўрнатиш талаб этилади.

Ушбу дастур 5 та қисмдан иборат булар қуйидагилар:

- туб сонларни ҳосил қилиш генератори;
- сонларни тубликка текширувчи алгоритмлар;
- параметрли алгебрага асосланган RSA шифрлаш алгоритми;
- параметрли алгебрага асосланган El-Gamal шифрлаш алгоритми;
- параметрли алгебрага асосланган ERI (RSA асосида);

Ушбу амаллар дастурий кўринишда амалга оширилган бўлиб, дастур ойнасининг кўриниши қуйидагича.

Туб сонларни ҳосил қилиш генератори. Дастурниг ушбу қисмида оралиқлар бўйича туб сонлар ҳосил қилинади.



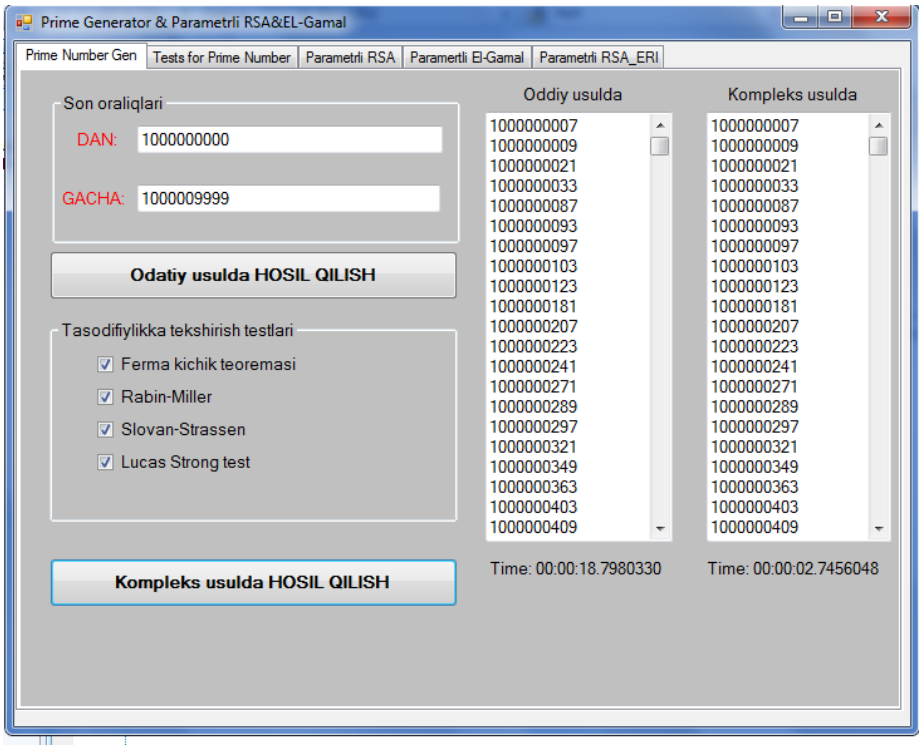
4-расм. Туб сон ҳосил қилиш ойнасининг кўриниши

Ушбу ойнадан кўриниб турибдики, одатий ҳосил қилинган ва комплекс ҳолда ҳосил қилинган туб сонлар генераторлари сарфлаган вақт бир-биридан катта фарқ қилмайди. Бошқа томондан тестлашдан ўтган туб сонлар бардошли саналиб, ундан фойдаланиш катта самара беради.

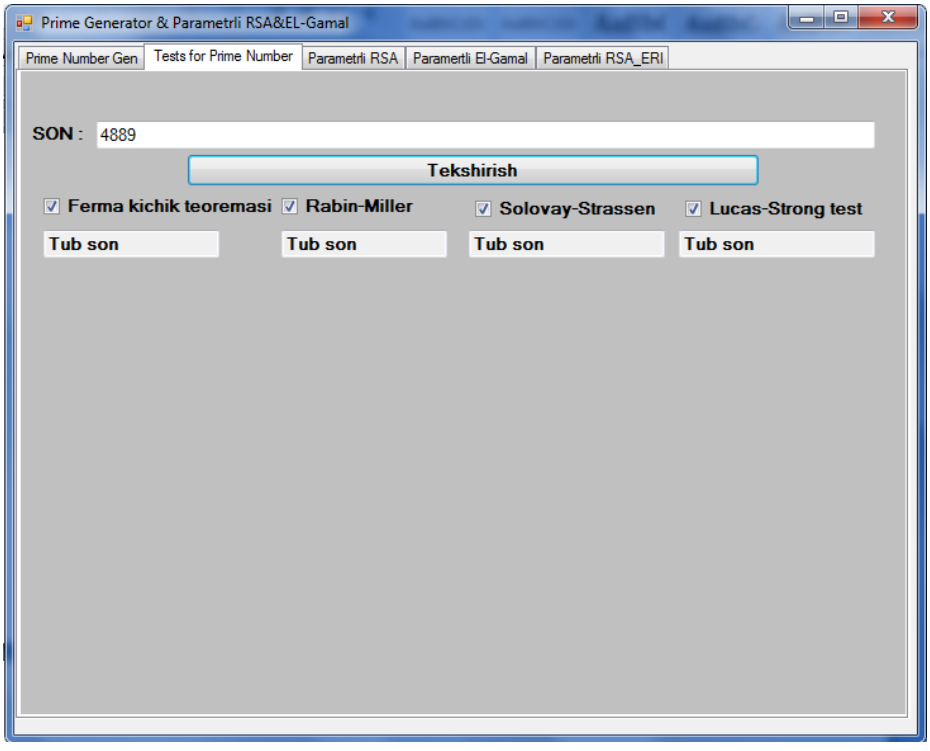
Агар алгоритмларда катта узунликдаги сонлар ҳосил қилинса, у ҳолда комплекс ҳолда ташкил этилган генератор вақтдан катта ютуқ беради. Ушбу кўрсаткичлар 5-расмда кўриниб турибди.

Сонларни тубликка текширувчи алгоритмлар. Ушбу қисмда тубликка текширувчи тестлар асосида сонларни текшириш дастури ишлаб чиқилган. Улар қуйидагилар:

- Ферманинг кичик теоремаси асосида;
- Робин-Миллер тести;
- Соловай-Страссен тести;
- Лукас стронг тест.



5-расм. Туб сон ҳосил қилиш ойнасининг кўриниши



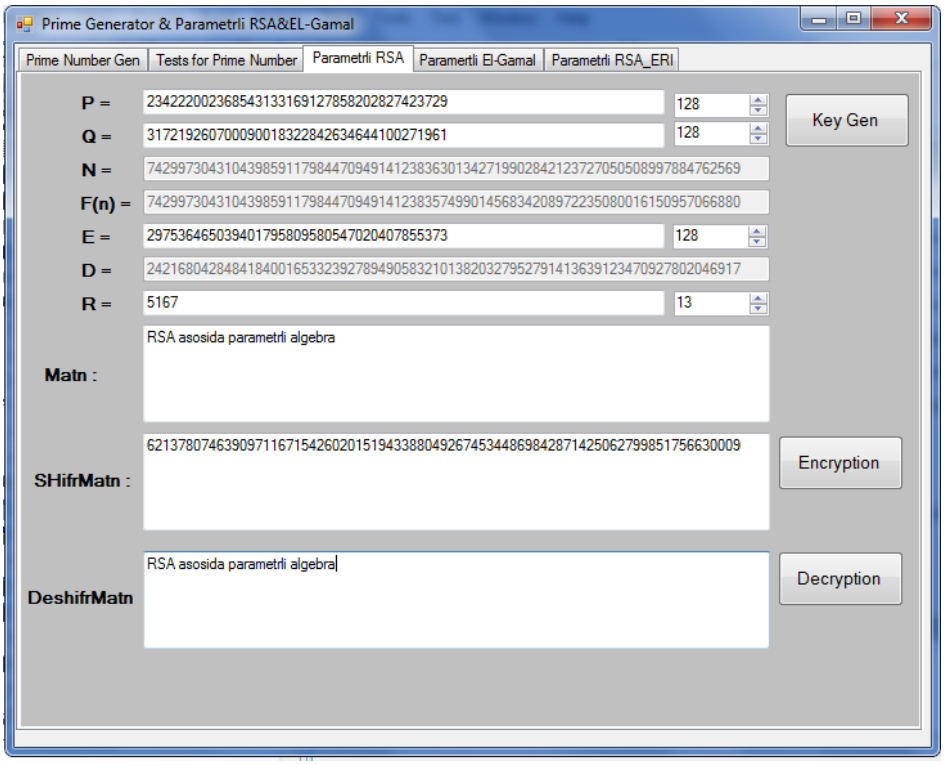
6-расм. Туб сонларни текшириш ойнаси

Ушбу тестлар алгоритми ҳақида иккинчи бўлимда айтиб ўтилди. Дастур ойнаси фойдаланишга қулай бўлиб, текширилаётган сон киритилади

ва тестлаш тури танланиб, текшириш тугмаси босилади. Натижада соннинг туб ёки туб эмаслигига қараб натижа ҳосил қилинади (6-расм).

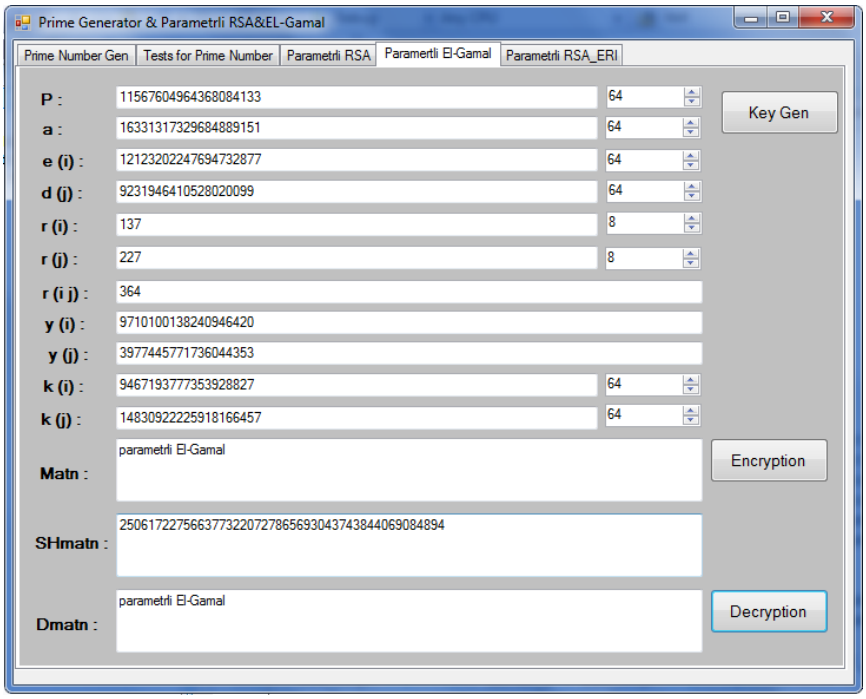
Дастурий воситанинг қолган уч қисми туб сонларни амалда, факторлаш ва дискрет логарифмлаш муаммосига асосланган носимметрик тизимларда қўллаш кўриб чиқилади.

Параметрли алгебрага асосланган RSA шифрлаш алгоритми. Ушбу дастур анаънавий RSA шифрлаш алгоритмининг параметр асосида ҳосил қилинган кўринишидир. Бунда ҳар бир параметр узунлиги 256-бит бўлиб, якуний n эса 512-битни ташкил этади. Ушбу дастурда фойдаланилган катта узунликдаги туб сонлар *BinInt* класси асосида ҳосил қилиниб, мавжуд тестлаш асосида текширилади. Текширишдан ўтган сонлар ушбу дастурда кирувчи параметр сифатида фойдаланилади. Ҳар бир параметр автоматик равишда ҳосил қилинади. Киритилаётган параметр узунлигини ихтиёрий равишда танлаш имконияти фойдаланувчига қулайлик яратиади.



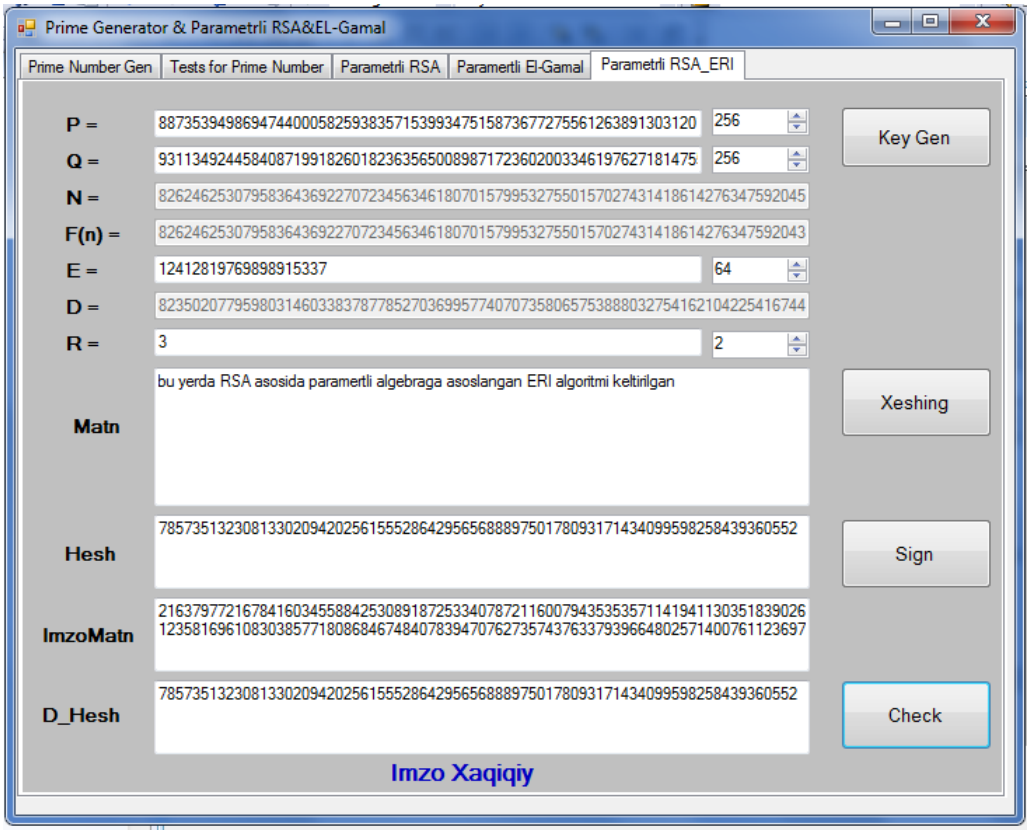
7-расм. Параметрли RSA шифрлаш дастури

Параметрли алгебрага асосланган El-Gamal шифрлаш алгоритми. Параметрли El-Gamal шифрлаш тизими дастури камида 64-бит узунликдаги P калит асосида ҳосил қилинади. Ҳар бир калит узунлигини ошиши билан дастурнинг бардошлиги ошади. *r(i)* ва *r(j)* калитларни узунлиги ортиши тизимни ишлаш тезлигига таъсир кўрсатади. *e(i)* ва *d(j)* каттиликлар камида 64-бит узунликка эга. *r(i)* ва *r(j)* махфий калитлар эса камида 2-битни ташкил этиб, тасодифий сонлар генератори асосида ташкил этилиб, тубликка текширувчи тестлар асосида тестланади ва шифрлашда фойдаланилади. Параметрлар узунлигини ортириш ихтиёрий танлаш асосида амалга оширилади.



8-расм. Параметрли El-Gamal шифрлаш дастури

Параметрли алгебрага асосланган ERI (RSA асосида). Ушбу дастурда анъанавий RSA шифрлаш алгоритмининг параметрли алгебрага ўтказилган шакли ишлаб чиқилган.



9-расм. Параметрли RSA асосида ЭРИ алгоритми дастури

Бунда қўшимча R параметр асосида даражага ошириш амалга оширилган бўлиб, бу параметр тизимнинг хавфсизлик даражасини яна бир параметрга боғлиқлигини исботлаб, уни махфий тутилиши асосида бардошлик таъминланади. Q ва P қийматлар камида 256-бит ўлчамда олиниб, параметр R камида 2-бит узунликка эга. Олинган ҳар бир параметр тасодифий ҳосил қилиниб, тубликка текширилади ва олинган сон шифрлашда фойдаланилади.

3. Ишлаб чиқилган дастурий криптографик модулни бардошлилигини баҳолаш

Ушбу амалий қисмда яратилган дастурий воситаларнинг бардошлигини баҳолаш ҳар бир дастурнинг яратилиш мақсади ва уни амалиётда берадиган фойдасига қараб амалга оширилади.

Шунга кўра яратилган туб сонларни ҳосил қилувчи генераторларнинг афзаллик ва камчиликларига тўхталиб ўтсак.

3-жадвал

Анаънавий ва комбинациялашган усулларнинг ўзаро таҳлили

Хусусиятлар	**Анаънавий**	**Комбинациялашган**
Камчиликлар	Ҳосил бўлаётган соннинг узунлиги ортиши билан унга кетадиган вақтни кўпайиши; Сонларни тубликка текшириш тестлари мавжуд эмаслиги ва бунинг натижасида сонларни қўшимча тубликка текшириш амалга оширилиши кераглиги	Кичик узунликда анаъвий усулга қараганда кўп вақт сарфланиши.
Ютуқлар	Кичик узунликда комбинациялашган усулга қараганда кам вақт сарфланиши.	Тўртта тестлаш туридан ихтиёрий фойдаланиш имконияти мавжудлиги. Катта узунликдаги туб сон ҳосил қилишда вақтни анаънавий усулга қараганда кам сарфланиши.

Туб сонларнинг амалиётда қўллаш учун яратилган дастурий воситанинг бардошлигини баҳолашда қуйидаги хусусиятларга этибор берилди:

- Яратилаётган туб сонларни ишончлигига;
- Носимметрик тизимда фойдаланилган параметрли алгебра мураккаблигига.

Яратилган носимметрик тизимлар параметрлари олдинги дастурда фойдаланилган тубликка текшириш тестлари асосида тесланиб, сўнгра фойдаланилди. Бу эса тизимда фойдаланилаётган параметрларнинг бардошлигини билдиради.

Носимметрик тизимларда киритилган қўшимча мураккаблик, даража параметри асосида амалга оширилади. Шу ўринда даража параметри муаммоси учта мураккаблик поғонаси билан фарқланиб, қуйидагича таърифланади:

1-таъриф. Агар параметрли алгебра $(F_n; ®)$ да ташувчи F_n нинг элементи y берилган бўлса, унда параметр R, даража кўрсаткичи e ва элемент a топилсин**,** бу ерда $F_n - n$ та бутун сонлардан тузилган чекли тўплам, $y \equiv a^{\backslash e} (mod\ n)$, $^{\backslash e} - a$ ни параметр R билан e-даражаси рамзи, элемент a $a^{\backslash \omega}\ (mod\ n) \equiv 0$ шартини фақат $\omega = q$ бўлгандагина қаноатлантиради**,** $q - \varphi(n)$ нинг бутун сонли бўлувчиси, $\varphi(n)$ – *Эйлер пи-функцияси* (мураккабликнинг учинчи поғонасига оид муаммо).

2-таъриф. Агар параметрли алгебра $(F_n; ®)$ да ташувчи F_n нинг элементлари y ва a берилган бўлса, унда параметр R ва даража кўрсаткичи e топилсин**,** бу ерда $F_n - n$ та бутун сонлардан тузилган чекли тўплам, $y \equiv a^{\backslash e} (mod\ n)$, $^{\backslash e} - a$ ни параметр R билан e-даражаси рамзи, элемент a $a^{\backslash \omega}\ (mod\ n) \equiv 0$ шартини фақат $\omega = q$ бўлгандагина қаноатлантиради, $q - \varphi(n)$ нинг бутун сонли бўлувчиси, $\varphi(n)$ – *Эйлер пи-функцияси* (мураккабликнинг иккинчи поғонасига оид муаммо).

3-таъриф. Агар параметрли алгебра $(F_n; ®)$ да ташувчи F_n нинг элементлари y, a ва даража кўрсаткичи e берилган бўлса, унда параметр R топилсин**,** бу ерда F_n – n та бутун сонлардан тузилган чекли тўплам, $y \equiv a^{\backslash e}(mod\ n)$, $^{\backslash e}$ – a ни параметр R билан e–даражаси рамзи, элемент a $a^{\backslash \omega}\ (mod\ n) \equiv 0$ шартини фақат $\omega = q$ бўлгандагина қаноатлантиради, q – $\varphi(n)$ нинг бутун сонли бўлувчиси, $\varphi(n)$ – *Эйлер пи-функцияси* (мураккабликнинг биринчи поғонасига оид муаммо).

Мазкур муаммоларнинг юзага чиқиши бир томонлама параметрли функциянинг қуйидаги хосса билан боғлиқ:

$$a^{\backslash e} \equiv a * \sum_{i=0}^{i=e-1} F^i\ (mod\ n)$$

бу ерда $F = 1 + R * a,\ n \in \{p,\ p_1 * p_2\}$.

4-таъриф. Агар параметрли алгебра $(F_p; ®)$ да ташувчи F_p нинг элементлари y ва R берилган бўлса, унда даража кўрсаткичи e ва элемент a топилсин**,** бу ерда F_p - n та бутун сонлардан тузилган чекли тўплам, $y \equiv a^{\backslash e}(mod\ p)$, $^{\backslash e}$ - a ни параметр R билан e-даражаси рамзи, элемент a $a^{\backslash \omega}\ (mod\ n) \equiv 0$ шартини фақат $\omega = q$ бўлгандагина қаноатлантиради**,** q - $\varphi()$ нинг бутун сонли бўлувчиси, $\varphi(n)$ - *Эйлер пи-функцияси*.

Яқоридаги тарифлардан келиб чиқиб параметрли RSA алгоритми учун қуйидагиларни келтириш мумкин:

- Ушбу алгоритми одатий ҳолда факторлаш муаммосига асосланганлиги ва қўшимча тарзда параметр муаммосини киритилиши бунга дискрет логарифмлаш муаамосини киритади.
- Агар ички томондан R параметр маълум бўлган ҳолда ҳам алгоритм ўзининг бардошлигини камида факторлаш муаммоси даражасида ушлаб туради.

Ушбу дастурдан фойдаланишда бардошлиликка эришишда қуйидагиларга аҳамият бериш шарт:

- R параметрни этарли даражада катта узунликда танланиши ($2^{256} > R$, $R^{-1} \geq 2^{160}$ шартни бажариши);
- Кирувчи параметрларни 2048-битдан кам бўлмаган ҳолда танланиши (p^{160} учун R параметрни топиш имконияти амалий йўқлиги);

El-Gamal шифрлаш тизимида ҳам шинга ўхшаш қуйидаги афзалликлар мавжуд:

- Дискрет логарифмлаш муаммосининг қўшимча параметр муаммоси асосида ортирилиши ва бунинг натижасида икки марта дискрет логарифмлаш муаммомини вужудга келтириш.
- Махфий параметр R аниқланганда ҳам тизим ўзининг кучуни бутунлай ёқотмаслиги.

Бу тизим учун ҳам RSA тизимига келтирилган шартлар ўринлидир. Умумий ҳолда синалган туб сонларни амалиётда қўллаш носимметрик тизим учун фойдали бўлиб, бунда тизим бардошлиги туб сон ишончлилик даражаси ва узунлигига боғлиқ бўлади.

3 боб бўйича хулосалар

Ушбу бўлимда катта узунликдаги туб сонлардан фойдаланган ҳолда мавжуд носимметрик тизимларда параметрли алгебра муаммоларини қўллаб алгоритмлар яратилиб, дастурий воситаси яратилди.

Катта узунликдаги туб сонларни ҳосил қилиш бу тизимларда муҳим аҳамият касб этади. Шунинг учун дастурнинг биринчи қисмида катта узунликдаги туб сонларни ҳисоблаш дастури яратилди. Ушбу яратилган дастурнинг амалий бардошлиги исботланди.

Яратилган туб сонларни тубликка текшириш дастурнинг иккинчи қисмида амалга оширилиб, бунда тубликка тестлаш усулларидан фойдаланилди.

Ушбу яратилган икки дастурий восита асосида, RSA ва El-Gamal алгоритмларининг параметрли алгебрага ўтказиш амали асосида янги бардошли носимметрик тизим ишлаб чиқилди ва унинг анаънавий шаклларига қараганда бардошлиги исботланди.

Параметрли алгебра муаммоси носимметрик тизимларда қўшимча қўшилган мураккаблик тури бўлиб, қўшимча R параметр узунлиги ортиши билан яратилган тизим бардошлиги одатий тизимга қараганда ортиб боради. Шунинг учун янги киритилган параметр $2^{256} > R$, $R^{-1} \geq 2^{16}$ шартни қаноатлантириши талаб этилади.

Хулоса

Магистрлик диссертацияси ишини бажариш жараёнида қуйидаги асосий натижалар олинди:

1. Носсиметрик криптотизимларда калитларни генерация қилишда алгоритмларнинг мураккаблик даражасига боғлиқлиги асосланиб, муаммо тури бўйича муҳим аҳамият касб этадиган, кенг қўлланиладиган алгоритмлар тадқиқ этилди.

2. Носсиметрик шифрлаш ва электрон рақамли имзо алгоритмлари тадқиқ этилиб, бир неча ҳусусиятлари бўйича тавсифи келтирилиб, калитларни ҳосил қилишда туб сонларга асосланганлиги изоҳланди.

3. Криптографик алгоритм хавфсизлигини тавсифлайдиган хусусиятлар етарли даражада кўп бўлиб, калитларни турли ҳужумларга бардошлиги хусусияти хавфсизлик талабларини шаклланишига олиб келади. Диссертация ишида калитларни хавфсизлигига оид асосий талаблар тадқиқ этилди.

4. Тадқиқ этиш натижалари шуни кўрсатдики, калитларни ҳосил қилишда уларни бардошлилиги туб сонларга асосланганлиги, катта бардошли туб сонларни танлашда уларни тубликка текшириш тестидан ўтказиш керак бўлади.

5. Кўзланган мақсадни амалга ошириш учун коплекс тестлаш усули таклиф қилиниб, бунда тестлаш усулидан иҳтиёрий миқдорда фойдаланиш мумкин бўлади.

6. Параметрли алгебра мураккаблигини криптотизимга тадбиқ этиш катта самара беради. Шу боис бардошли туб сонлар билан бирга параметрли алгебрадан фойдаланиб носсиметрик криптотизимлар учун дастури яратилди.

Адабиётлар рўйхати

1. «Ахборотлаштириш тўғрисида»ги Ўзбекистон Республикаси Қонуни. 11.12.2003 й. №560-II.

2. «Ўзбекистон Республикасида ахборотнинг криптографик муҳофазасини ташкил этишга доир чора-тадбирлари тўғрисида» ги Ўзбекистон Республикаси Президентининг ПҚ-614-сон қарори. – Тошкент, 3 апрел 2007 йил.

3. Ғаниев С.К., Каримов М.М., Ташев К.А. Ахборот хавфсизлиги. Ахборот-коммуникацион тизимлар хавфсизлиги. Ўқув қўлланма. Т., “Aloqachi”. 2008. – 382 б.

4. Акбаров Д.Е. «Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши» - Т.: «Ўзбекистон маркаси», 2009. - 424 б.

5. Ахмедова О.П. Параметрлар алгебраси асосида носимметрик криптотизимлар яратиш усули ва алгоритмлари // Номзодлик диссертация иши, Тошкент-2007.

6. Хасанов Хислат ПўлатовичТакомиллашган диаматрицалар алгебралари ва параметрли алгебра асосида криптотизимлар яратиш усуллари ва алгоритмлари – Тошкент, 2008 – 204 бет

7. К.Э. Шенон. Теория связи в секретных системах. В кн.: К.Э. Шенон. Работы по теории информации и кибернетике. М.: ИЛ, 1963, том 2. -С. 243-332.

8. Денисов Т.А, Е.Н. Клитина, О.Ю. Самарин. Теоретико-числовые методы в криптографии. Бумага офсетная. 10 п.л. Тираж 1000 экз. 25.01.2006

9. Алгоритм RSA. «Комплексное обеспечение информационной безопасности автоматизированных систем» О. Н. Жданов, И. А. Лубкин ; Сиб. гос. аэрокосмич. ун-т. – Красноярск, 2007. –38 с.

10. US Patent, Rivest R., Shamir A. and Adleman L.: Cryptographic Communications System and Method. 4,405,829, 1983.

11. Diffie, W., Hellman, M.E. New directions in cryptography // IEEE Transactionson Information Theory, vol. IT-22, 1976. – Pp. 644-654.

12. Диффи У. Первые десять лет криптографии с открытым ключом // Перевод с англ. Защита информации. Малый тематический выпуск ТИИЭР. – Москва, 1988. – т.76, №5. – С. 54-74.

13. Шеннон К. Работы по теории информации и кибернетике. М.ИЛ, 1963. - С.333-369 (Теория свяди в секретных системах).

14. Beeler M., Gosper R., Schroeppel R. HACKMEM: Tech. Rep. AIM 239: MTI, 1972.

15. Brent R. P. An improved monte-carlo factorization algorithm // BIT._1980._ Vol. 20._ Pp. 176–184.

16. Brillhart M. M. . J. A method of factoring and the factorization of f_7. //Mathematics Of Computation._ 1975._ Vol. 29._ Pp. 183–205.

17. Carmichael R. The Theory Of Numbers._ New York: J. Willey & Sons,1914._ P. 95.

18. Cohen H. A Course In Computational Algebraic Number Theory._ 3rd edition._ New York: Springer, 1996._ P. 545.

19. 1969._ Vol. 1 of The Art of Computer Programming. Garner H. The residue number system // IRE Transactions on Electronic Computers._ 1957._ Vol. EC-8, no. 2._ Pp. 140–147.

20. Knuth D. E. Seminumerical Algorithms._ Addison-Wesley Professional,1969._ Vol. 2 of The Art of Computer Programming.

21. Lehman S. Factoring large integers // Mathematics Of Computation.1974._ Vol. 28, no. 126._ Pp. 637–646.

22. Lehmer D., Powers R. On factoring large numbers // Bulletin Of the American Mathematical Society._ 1931._ Vol. 37, no. 9._ Pp. 770–Шеннон К. Теория и связи в секретных системах. Работы по теории информации и кибернетике. – М.: Иностранная лит. 1963. – 243 б.

23. Kraitchik M. Th´eorie des Nombres. Tome I et II._ Paris: Gauthier-Villars, 1926.Винокуров А. Современность практической криптографии // Системы безопасности связи и телекоммуникаций. – 2003. – №10. – С. 218-221.

24. Бабаш А.В., Шанкин Г.П. История криптографии. Часть I. - Изд.: Лори Гелиос АРВ, 2002.- 240 с.

25. Diffie, W., Hellman, M.New directions in cryptography // IEEE Transactionson Information Theory, vol. IT-22, 1976. – Pp. 644-654.

26. Чмора А.Л. Современная прикладная криптография. Изд.:Гелиос, 2001.- 256 с.

27. Koblitz N. and Vanstone S. The state of elliptic curve cryptography // Designs, Codes and Cryptography, 19 (2000). – Pp. 173-193.

28. Koblitz N. Elliptic Curve Cryptosystems // Mathematics of Computation, 48, 1987. – Pp. 203-209.

29. Voorhoeve M. Factorization algorithms of exponential order // Computational methods in number theory. V. 1 / H.W. Lenstra and R. Tijdeman, editors. Amsterdam, 1982. P. 79—88.

30. Лунин А.В., Сальников А.А. Перспективы развития и использования асимметричных алгоритмов в криптографии. http: //www.ssl.stu.neva.ru.Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. - Изд.:Лори Гелиос АРВ, 2005.- 192 с.

31. US Patent, Hellman, et al. Cryptographic apparatus and method, 4.200.770, April 29,1980.

32. US Patent, Rivest R., Shamir A. and Adleman L.: Cryptographic Communications System and Method. 4,405,829, 1983.

33. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. Учебное пособие. - Изд.:Лори Горячая Линия - Телеком, 2002.- 175 с.

34. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. – Изд.:МЦНМО, 2003. – 328 с.

35. Hankerson D., Menezes A., VanstoneS. GuidetoEllipticCurve Cryptography. Springer-Verlag New York, Inc. 2004.-456 pp.

36. Коробейников А.Г., Гатчин Ю.А. Математические основы криптологии. Учебное пособие. - Санкт-Петербург, 2004. – 106 с.

37. Масленников М., Практическая криптография. - М.:Лори BHV - Санкт - Петербург, 2003.- 464 с.

38. Шнайер Б. Слабые места криптографических систем // Открытые системы. – 1999, № 1. – С. 31-36.

39. BihamE., ShamirA. DifferentialcryptanalysisofDES-likecryptosystems // AdvancesinCryptology — CRYPTO ’90. LNCS. Springer–Verlag. 1991. V. 537. P.

40. Authentication by using pseudo-random numbers. Arziyeva J.T., Xudoyqulov Z.T., Mardiyev U.R. International Scientific and Practical Conference “INNOVATION-2012”.

41. Носсимметрик криптотизимларга асосланган калитларни генерация қилиш алгоритмлари тадқиқи. Гуломов Ш.Р., Мардиев У.Р0., Республиканиский семинар: «Информационная безопастность в сфере связи и информатизации. Проблемы и пути их решения». Ташкент 30 октября 2012 г.

Илова

Дастур коди

```
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.Security.Cryptography;

namespace GENERATOR_PRIME
{
    public partial class Form1 : Form
    {
        public Form1()
        {
            InitializeComponent();
        }
        ASCIIEncoding encoding = new ASCIIEncoding();
        ASCIIEncoding decoding = new ASCIIEncoding();

        RSA_Sign.BigInteger p;
        RSA_Sign.BigInteger q;
        RSA_Sign.BigInteger n;
        RSA_Sign.BigInteger fn;
        RSA_Sign.BigInteger param;
        RSA_Sign.BigInteger E;
        RSA_Sign.BigInteger D;
        private bool prime_1(RSA_Sign.BigInteger candidate)
        {
            if ((candidate & 1) == 0)
            {
                if (candidate == 2)
                {
                    return true;
                }
                else
                {
                    return false;
                }
            }
            for (int i = 3; (i * i) <= candidate; i += 2)
            {
                if ((candidate % i) == 0)
                {
                    return false;
                }
            }
            return candidate != 1;
        }
        private bool testlash(int test_id, RSA_Sign.BigInteger son)
        {
            RSA_Sign.BigInteger bg = new RSA_Sign.BigInteger();
            if (test_id ==0)
            {
                return bg.FermatLittleTest(1, son.ToString());
```

```
        }
        if (test_id == 1)
        {
            return bg.RabinMillerTest1(1, son.ToString());
        }
        if (test_id == 2)
        {
            return bg.SolovayStrassenTest(1, son.ToString());
        }
        return false;
    }
    private void button2_Click(object sender, EventArgs e)
    {
        RSA_Sign.BigInteger dann = new RSA_Sign.BigInteger(textBox6.Text, 10);
        RSA_Sign.BigInteger gacha = new RSA_Sign.BigInteger(textBox7.Text, 10);
        if (comboBox1.Visible)
            {
                for (RSA_Sign.BigInteger i = dann; i < gacha; i++)
                {
                    if (testlash(comboBox1.SelectedIndex, i))
                    {
                        textBox8.Text += i.ToString() + Environment.NewLine;
                    }
                }
            }
            else
            {
                for (RSA_Sign.BigInteger i = dann; i < gacha; i++)
                {
                    if (prime_1(i))
                    {
                        textBox8.Text += i.ToString() + Environment.NewLine;
                    }
                }
            }
        }
    private void button1_Click(object sender, EventArgs e)
    {
        RSA_Sign.BigInteger bg=new RSA_Sign.BigInteger();
        string son = textBox1.Text;
        if (checkBox1.Checked)
        {
            bool natija=bg.FermatLittleTest(10,son);
            if (natija)
            {
                textBox2.Text = "Tub son";
            }
            else
            {
                textBox2.Text = "Murakkab son";
            }
        }
        if (checkBox2.Checked)
        {
            bool natija = bg.RabinMillerTest1(10, son);
            if (natija)
            {
                textBox3.Text = "Tub son";
            }
            else
```

```
        {
            textBox3.Text = "Murakkab son";
        }
    }
    if (checkBox3.Checked)
    {
        bool natija = bg.SolovayStrassenTest(10, son);
        if (natija)
        {
            textBox4.Text = "Tub son";
        }
        else
        {
            textBox4.Text = "Murakkab son";
        }
    }
}

private void checkBox10_CheckedChanged(object sender, EventArgs e)
{
    if (checkBox10.Checked)
    {
        comboBox1.Visible = true;
    }
    else
    {
        comboBox1.Visible = false;
    }
}

private void tabPage1_Click(object sender, EventArgs e)
{

}

private void button6_Click(object sender, EventArgs e)
{

}

private void button5_Click(object sender, EventArgs e)
{
    Random ran = new Random();
    p = RSA_Sign.BigInteger.genPseudoPrime(256, 13, ran);
    q = RSA_Sign.BigInteger.genPseudoPrime(256, 13, ran);
    E = RSA_Sign.BigInteger.genPseudoPrime(256, 13, ran);
    param = RSA_Sign.BigInteger.genPseudoPrime(13, 13, ran);
    n = p * q;
    fn = (p - 1) * (q - 1);
    D = RSA_Sign.BigInteger.Inverse(E, fn);
    textBox18.Text = p.ToString();
    textBox17.Text = q.ToString();
    textBox16.Text = n.ToString();
    textBox15.Text = fn.ToString();
    textBox14.Text = E.ToString();
    textBox13.Text = D.ToString();
    textBox11.Text = param.ToString();

}
```

```
        private void button3_Click(object sender, EventArgs e)
        {
            RSA_Sign.BigInteger xesh = new RSA_Sign.BigInteger(textBox5.Text, 10);
            textBox9.Text = (xesh.modPowpar(E, n, param)).ToString();

        }

        private void textBox12_TextChanged(object sender, EventArgs e)
        {
            if (textBox12.Text.Length != 0)
            {
                RSA_Sign.BigInteger heshqiymat = new
RSA_Sign.BigInteger(SHA512hash(encoding.GetBytes(textBox12.Text)));
                textBox5.Text = heshqiymat.ToString();
            }
        }
        private static byte[] SHA512hash(byte[] data)
        {
            SHA512 sha512 = new SHA512CryptoServiceProvider();
            return sha512.ComputeHash(data);
        }

        private void button4_Click(object sender, EventArgs e)
        {
            RSA_Sign.BigInteger Dxesh = new RSA_Sign.BigInteger(textBox9.Text, 10);
            textBox10.Text = (Dxesh.modPowpar(D, n, param)).ToString();
            label11.Visible = true;
            if (textBox5.Text == textBox10.Text)
                label11.Text = "Imzo Xaqiqiy";
            else
                label11.Text = "Imzo Xaqiqiy emas";

        }

        private void button6_Click_1(object sender, EventArgs e)
        {
            Random ran = new Random();
            p = RSA_Sign.BigInteger.genPseudoPrime(256, 13, ran);
            q = RSA_Sign.BigInteger.genPseudoPrime(256, 13, ran);
            E = RSA_Sign.BigInteger.genPseudoPrime(256, 13, ran);
            param = RSA_Sign.BigInteger.genPseudoPrime(13, 13, ran);
            n = p * q;
            fn = (p - 1) * (q - 1);
            D = RSA_Sign.BigInteger.Inverse(E, fn);
            textBox26.Text = p.ToString();
            textBox25.Text = q.ToString();
            textBox24.Text = n.ToString();
            textBox23.Text = fn.ToString();
            textBox22.Text = E.ToString();
            textBox21.Text = D.ToString();
            textBox19.Text = param.ToString();
        }

        private void textBox20_TextChanged(object sender, EventArgs e)
        {

        }

        private void button7_Click(object sender, EventArgs e)
        {
```

```
            RSA_Sign.BigInteger matn = new
RSA_Sign.BigInteger((encoding.GetBytes(textBox20.Text)));
            //RSA_Sign.BigInteger xesh = new RSA_Sign.BigInteger(textBox5.Text, 10);
            textBox27.Text = (matn.modPowpar(E, n, param)).ToString();

        }

        private void button8_Click(object sender, EventArgs e)
        {
           // RSA_Sign.BigInteger matn = new
RSA_Sign.BigInteger((encoding.GetBytes(textBox20.Text)));
            RSA_Sign.BigInteger xesh = new RSA_Sign.BigInteger(textBox27.Text, 10);
            RSA_Sign.BigInteger desh =new RSA_Sign.BigInteger((xesh.modPowpar(D, n,
param)).ToString(),10);
            byte[] ss = desh.getBytes();
            textBox28.Text = decoding.GetString(ss);
        }
        RSA_Sign.BigInteger p_elgamal;
        RSA_Sign.BigInteger a_elgamal;
        RSA_Sign.BigInteger e_el;
        RSA_Sign.BigInteger d_el;
        RSA_Sign.BigInteger r_i;
        RSA_Sign.BigInteger r_j;
        RSA_Sign.BigInteger k_i;
        RSA_Sign.BigInteger k_j;
        RSA_Sign.BigInteger y_i;
        RSA_Sign.BigInteger y_j;
        RSA_Sign.BigInteger r_i_j;
        RSA_Sign.BigInteger s_1j;
        RSA_Sign.BigInteger s_2j;
        private void button9_Click(object sender, EventArgs e)
        {
            Random ran = new Random();
            p_elgamal = RSA_Sign.BigInteger.genPseudoPrime(256, 13, ran);
            a_elgamal = RSA_Sign.BigInteger.genPseudoPrime(192, 13, ran);
            e_el = RSA_Sign.BigInteger.genPseudoPrime(192, 13, ran);
            d_el = RSA_Sign.BigInteger.genPseudoPrime(192, 13, ran);
            r_i = RSA_Sign.BigInteger.genPseudoPrime(8, 13, ran);
            r_j = RSA_Sign.BigInteger.genPseudoPrime(8, 13, ran);
            r_i_j = (r_i + r_j) % p_elgamal;
            //MessageBox.Show(r_i_j.ToString());
            k_i = RSA_Sign.BigInteger.genPseudoPrime(192, 13, ran);
            k_j = RSA_Sign.BigInteger.genPseudoPrime(192, 13, ran);
            RSA_Sign.BigInteger rs=new RSA_Sign.BigInteger();
            RSA_Sign.BigInteger inver_i = RSA_Sign.BigInteger.Inverse(r_i,
p_elgamal)*a_elgamal;
            RSA_Sign.BigInteger inver_j = RSA_Sign.BigInteger.Inverse(r_j, p_elgamal) *
a_elgamal;
            y_i = inver_i.modPowpar(e_el, p_elgamal, r_i);
            y_j = inver_j.modPowpar(d_el, p_elgamal, r_j);
            textBox29.Text = p_elgamal.ToString();
            textBox33.Text = a_elgamal.ToString();
            textBox32.Text = e_el.ToString();
            textBox31.Text = d_el.ToString();
            textBox30.Text = r_i.ToString();
            textBox34.Text = r_j.ToString();
            textBox35.Text = r_i_j.ToString();
            textBox36.Text = y_i.ToString();
            textBox37.Text = y_j.ToString();
            textBox41.Text = k_i.ToString();
```

```
            textBox42.Text = k_j.ToString();
        }
        public RSA_Sign.BigInteger fff(RSA_Sign.BigInteger bi1,RSA_Sign.BigInteger bi2)
        {
           RSA_Sign.BigInteger result = new RSA_Sign.BigInteger();

            int len = (bi1.dataLength > bi2.dataLength) ? bi1.dataLength : bi2.dataLength;

            for (int i = 0; i < len; i++)
            {
                uint sum = (uint)(bi1.data[i] ^ bi2.data[i]);
                result.data[i] = sum;
            }
            result.dataLength = 70;

            while (result.dataLength > 1 && result.data[result.dataLength - 1] == 0)
                result.dataLength--;

            return result;
        }
        private void button10_Click(object sender, EventArgs e)
        {
            RSA_Sign.BigInteger qism = RSA_Sign.BigInteger.Inverse(r_j,
p_elgamal)*a_elgamal;
            s_1j = qism.modPowpar(k_j, p_elgamal, r_j);
            RSA_Sign.BigInteger R=r_j*(r_i_j-r_j);
            ASCIIEncoding encon = new ASCIIEncoding();
            RSA_Sign.BigInteger matn = new
RSA_Sign.BigInteger(encon.GetBytes(textBox38.Text));
            RSA_Sign.BigInteger qism1 = RSA_Sign.BigInteger.Inverse(r_j, p_elgamal) * y_i;
            RSA_Sign.BigInteger rr = qism1.modPowpar(k_j, p_elgamal, R);
            s_2j = fff(matn, rr);
            textBox39.Text = s_2j.ToString();
        }

        private void button11_Click(object sender, EventArgs e)
        {
            RSA_Sign.BigInteger R = r_i * (r_i_j - r_i);
            RSA_Sign.BigInteger qism1 = RSA_Sign.BigInteger.Inverse(r_i, p_elgamal) *
s_1j;
            RSA_Sign.BigInteger rr = qism1.modPowpar(e_el, p_elgamal, R);
            RSA_Sign.BigInteger matn=fff(s_2j,rr);
            byte[] ss = matn.getBytes();
            ASCIIEncoding decod = new ASCIIEncoding();
            textBox40.Text = decod.GetString(ss);
        }

        private void tabPage2_Click(object sender, EventArgs e)
        {

        }
    }
}
```