ЎЗБЕКИСТОН АЛОҚА ВА АХБОРОТЛАШТИРИШ АГЕНТЛИГИ

«UNICON.UZ» - Фан-техника ва маркетинг тадқиқотлари маркази
давлат унитар корхонаси

# КРИПТОТАҲЛИЛ ВА УНИНГ МАХСУС УСУЛЛАРИ

Ўқув қўлланма

Тошкент 2010

УЎТ 681.3

**Хасанов Пўлат Фаттохович, Хасанов Хислат Пўлатович, Ахмедова Ойдин Пўлатовна, Давлатов Алишер Бахтиёрович**

*(т.ф.д., профессор П.Ф. Хасанов таҳрири остида)*

***Криптотаҳлил ва унинг махсус усуллари*** – Тошкент, 2010 – 175 бет

Ушбу ўқув қўлланмада криптотаҳлил асослари, криптотаҳлил объекти, криптографик алгоритмлар бардошлилиги, мураккаблик назарияси ҳамда симметрик ва носимметрик криптотизимлар бардошлилигини таъминловчи тамойиллар ва муаммолар баён этилган.

Ўқув қўлланмада ошкора калитли криптотизимларни криптотаҳлиллашнинг универсал усуллари ва уларнинг таснифи ҳамда электрон рақамли имзо алгоритмларини криптотаҳлиллашнинг параметрлар группаси усули келтирилган.

Ушбу ўқув қўлланма ахборот хавфсизлиги ва криптография йўналишида таълим олаётган магистрлар учун мўлжалланган. Шунингдек ушбу ўқув қўлланмадан ахборот хавфсизлиги йўналишида бакалаврлар тайёрлаш жараёнида ҳамда криптография йўналишида илмий-тадқиқот олиб бораётган аспирант-тадқиқотчилар, илмий ходимлар ва соҳа мутахассислари фойдаланишлари мумкин.

**МУНДАРИЖА**

**ҚИСҚАРТМАЛАР**

| | | |
|---|---|---|
| 1. | AES (Advanced Encryption Standard) – | АҚШнинг маълумотларни шифрлаш стандарти. |
| 2. | АҚШ – | Америка Қўшма штатлари. |
| 3. | АНФ – | Алгебраик нормал форма. |
| 4. | БФ – | Буль функция. |
| 5. | ГОСТ 28147-89 – | Россия Федерациясининг маълумотларни шифрлаш стандарти. |
| 6. | ГОСТ Р 34.10–94 – | Россия Федерациясининг дискрет логарифмлашга асосланган электрон рақамли имзо стандарти. |
| 7. | ГОСТ Р 34.10-2001 – | Россия Федерациясининг эллиптик эгри чизиқда дискрет логарифмлашга асосланган электрон рақамли имзо стандарти. |
| 8. | DES (Data Encryption Standard) – | АҚШнинг маълумотларни шифрлаш стандарти. |
| 9. | DLP (Discrete Logarithm Problem) – | Дискрет логарифм муаммоси. |
| 10. | DHP (Diffi Hellman Problem) – | Диффи-Хеллман муаммоси. |
| 11. | DSA (Digital Signature Algorithm) – | АҚШнинг дискрет логарифмлашга асосланган электрон рақамли имзо алгоритми. |
| 12. | ДНФ – | Дизъюнктив нормал форма. |
| 13. | ДСТУ 4145-2002 – | Украинанинг эллиптик эгри чизиқда дискрет логарифмлашга асосланган электрон рақамли имзо стандарти. |
| 14. | GDLP (General Discrete Logarithm Problem) – | Умумлашган дискрет логарифм муаммоси. |
| 15. | GDHP (General Diffi Hellman Problem) – | Умумлашган Диффи-Хеллман муаммоси. |

| | | |
|---|---|---|
| 16. | GNFS (General Number Field Sieve) – | Умумлашган сонли майдон ғалвири усули. |
| 17. | ECDLP (Elliptic Curve Discrete Logarithm Problem) – | Эллиптик эгри чизиқда дискрет логарифмлаш муаммоси. |
| 18. | EC-DSA-2000 (Elliptic Curve Digital Signature Algorithm) – | АҚШнинг эллиптик эгри чизиқда дискрет логарифмлашга асосланган электрон рақамли имзо алгоритми. |
| 19. | EC-KCDSA – | Кореянинг эллиптик эгри чизиқда дискрет логарифмлашга асосланган электрон рақамли имзо алгоритми. |
| 20. | EC-GDSA – | Германия Федератив Республикасининг эллиптик эгри чизиқда дискрет логарифмлашга асосланган электрон рақамли имзо алгоритми. |
| 21. | ESIGN – | Япониянинг электрон рақамли имзо алгоритми. |
| 22. | EKUB – | Энг катта умумий бўлувчи. |
| 23. | FEAL (Fast Data Encryption Algorithm)– | Япония маълумотларни шифрлаш алгоритми. |
| 24. | IDEA (International Data Encryption Algorithm) – | Халқаро маълумотларни шифрлаш алгоритми. |
| 25. | КИ – | Корреляцион иммунлик. |
| 26. | КРОМ – | Калитларни рўйхатга олиш маркази. |
| 27. | НСКУ – | Назорат сеанс калити усули. |
| 28. | МША – | Маълумотларни шифрлаш алгоритми. |
| 29. | NFS (Number Field Sieve) – | Сонли майдон ғалвири усули. |
| 30. | МБ – | Маълумотлар базаси. |
| 31. | *“O”* – | Ҳисоблаш мураккаблиги қийматининг тартибини кўрсатувчи белги. |
| 32. | PGP (Pretty Good Privacy) – | Бинойидек пинҳоналик деб номланган дастур. |

| | | |
|---|---|---|
| 33. | RSA – | Райвест-Шамир-Адлеман алгоритми. |
| 34. | RSAP – | RSA муаммоси. |
| 35. | СТП – | Статистик таснифлаш процедураси. |
| 36. | СНТ – | Сунъий нейрон тўри. |
| 37. | S – | Ҳисоблаш қурилмаси хотирасининг ҳажми билан боғлиқ бўлган мураккаблик. |
| 38. | SQROOT – | *n* модули бўйича квадрат илдиз. |
| 39. | SUBSET-SUM – | Қисм тўплам-йиғиндиси. |
| 40. | SNFS (Special Number Field Sieve) – | Махсус кўринишдаги сонларни (масалан, Ферма сонларини) факторлаш усули. |
| 41. | УАА – | Уолш-Адамар акслантириши. |
| 42. | Т – | Вақт билан аниқланадиган мураккаблик. |
| 43. | ТТ – | Тарқалиш тамойили. |
| 44. | XOR – | 2 модул бўйича қўшиш. |
| 45. | O’z DSt 1092:2005, O’z DSt 1092:2009 – | Ўзбекистоннинг даража параметри муаммоларининг мураккаблигига асосланган электрон рақамли имзо бўйича давлат стандартлари. |
| 46. | QRP – | Квадратик чегирма муаммоси. |
| 47. | ҚҚЎСТ – | Қатъий кескин ўзгариш самарадорлик тамойили. |
| 48. | ЭРИ – | Электрон рақамли имзо. |
| 49. | ЭЭЧ – | Эллиптик эгри чизиқ. |

# КИРИШ

Ҳозирги кунда ҳар қандай ривожланган давлатда ахборот ва телекоммуникация технологияларининг жамиятда эгаллаган ўрни тобора юксалиб бормоқда. Ўзбекистон Республикаси ҳам мустақиллик йиллари ахборотлаштириш соҳасида инқилобий ўзгаришлар даврини бошдан кечирмоқда. Ўзбекистон Республикасининг «Телекоммуникациялар тўғрисида»ги қонуни ва Ўзбекистон Республикаси Президентининг 2002 йил 30 майдаги «Компьютерлаштиришни янада ривожлантириш ва ахборот-коммуникация технологияларини жорий этиш тўғрисида»ги Фармони бу борада муҳим аҳамият касб этди. Телекоммуникациялар ва маълумотлар узатишнинг миллий тармоғини ривожлантириш, давлат бошқарувига электрон технологияларни жорий этиш, электрон тижоратни ривожлантириш каби фармонда белгиланган чора-тадбирларнинг амалга оширилиши Ўзбекистон Республикасининг бу соҳада буюк давлатлар қаторидан муносиб ўрин эгаллашига катта ишонч пайдо қилди.

Замонавий ахборот-коммуникация технологиялари қулайликлар яратиш билан бир қаторда янги муаммоларни ўртага қўймоқда. Ахборот базаларида сақланадиган ва телекоммуникация тизимларида айланаётган ахборот хавфсизлигига таҳдид кескин ошмоқда. Айниқса, Интернет пайдо бўлгандан бошлаб, ахборот ўғирлаш, ахборот мазмунини эгасидан изнсиз ўзгартириб ва бузиб қўйиш, тармоқ ва серверлардан берухсат фойдаланиш каби ҳоллар дунё миқёсида кўпайди [1-9]. Ахборот хавфсизлиги муаммоси Ўзбекистон Республикаси учун ҳам долзарб муаммога айланди. Республикамизда сўнгги йилларда ахборот хавфсизлигини таъминлашга, чет элдан валютага сотиб олинаётган дастурий ва аппарат-дастурий воситаларнинг маҳаллийлаштиришга давлатимиз раҳбарияти томонидан катта аҳамият берилмоқда. Бунга қабул қилинган бир нечта қонун ва норматив ҳужжатлар, жумладан, “Ахборотлаштириш тўғрисида»ги, «Электрон ҳужжат айланиши тўғрисида»ги, «Электрон рақамли имзо тўғрисида»ги қонунлар мисол бўлиши мумкин.

Шуни таъкидлаш лозимки, Ўзбекистон Республикаси Президенти И.А. Каримовнинг «Жаҳон молиявий иқтисодий инқирози. Ўзбекистон

шароитида уни бартараф этишнинг йўллари ва чоралари» [11] номли асарида Ўзбекистон учун инқирозни бартараф этиш ва жаҳон бозорида янги марраларга чиқишнинг ишончли йўлларидан бири инновацион технологияларни кенг жорий этиш эканлиги кўрсатиб ўтилган. Ҳозирги кунда ахборот хавфсизлигини таъминлашга қаратилган воситаларнинг аксарияти чет элдан сотиб олинади. Шунинг учун, ахборот хавфсизлигини таъминловчи воситаларни республикамизда ишлаб чиқаришни йўлга қўйиш, янги технологиялар яратиш, бунинг ҳисобига валютани иқтисод қилиш муҳим вазифалардан ҳисобланади.

Ҳозирги кунга қадар ахборот хавфсизлигини таъминлашда энг ишончли воситалардан бири ахборотни криптографик ҳимоя қилиш воситалари ҳисобланади. Шу боис бу соҳа мутахассисларига фаоллик кўрсатиш учун шарт-шароитлар яратиб берилмоқда. 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. Мазкур қарорнинг асосий вазифаларидан бири ахборотнинг криптографик муҳофазаси соҳасида юқори малакали кадрларни тайёрлашдан иборат. Бунинг учун криптография йўналишида давлат тилида таълим олаётган талабалар, аспирант-тадқиқотчилар ва илмий ходимлар учун мўлжалланган ўқув қўлланмалар, дарсликлар, услубий қўлланмалар ва китоблар ишлаб чиқиш муҳим аҳамият касб этади.

Тақдим этилаётган ўқув қўлланма ахборот хавфсизлиги ва криптография йўналишида таълим олаётган магистрлар учун мўлжалланган. Шунингдек ушбу ўқув қўлланмадан ахборот хавфсизлиги йўналишида бакалаврлар тайёрлаш жараёнида ҳамда криптография йўналишида илмий-тадқиқот олиб бораётган аспирант-тадқиқотчилар, илмий ходимлар ва соҳа мутахассислари фойдаланишлари мумкин. Ушбу ўқув қўлланма “Криптография ва криптотаҳлил” мутахассислигининг ўқув таълим стандарти ва ўқув дастурига мувофиқ ишлаб чиқилди.

# 1. КРИПТОТАҲЛИЛ АСОСЛАРИ

## 1.1. Асосий тушунчалар ва таърифлар

Ҳар қандай соҳа ва йўналиш ҳақида тўлиқ маълумотга эга бўлиш учун дастлаб шу соҳа ва йўналишнинг асосий тушунчалари билан танишмоқ лозим [11]. Криптология ҳақида тўлиқроқ маълумотга эга бўлиш учун қуйидаги келтирилган атамалар ва уларнинг таърифлари муҳим аҳамиятга эга.

*Алгоритм* деганда масалани чекланган қадамларда ечиш учун аниқ белгиланган қоидаларнинг тартибланган чекли тўплами тушунилади [11].

Ахборотни сохталаштириш имкониятини йўққа чиқариш ва ундан рухсат этилмаган тарзда фойдаланишдан муҳофаза қилиш мақсадида ахборотни алмаштиришнинг математик алгоритми *криптографик алгоритм* деб аталади [11].

Аниқ сонлар тўпламидан берилган тўпламнинг ҳар бир элементи бир хил эҳтимоллик билан танлаб олиниши мумкин бўлган сон *тасодифий сон* деб аталади.

Маълум бир натижага эришиш мақсадида икки ва ундан кўп субъект томонидан берилган кетма-кетликда бажариладиган ҳаракатлар (йўриқномалар, буйруқлар, ҳисоблашлар, алгоритмлар) тўплами *протокол (баённома)* дейилади.

Криптоалгоритмдан ва шифрлаш калитларидан фойдаланишни белгилаб берадиган қоидалар ва процедуралар тўплами *криптографик баённома (криптографик протокол)* деб аталади [11].

Ахборотнинг, унга бўладиган табиий ёки сунъий тусдаги таҳдидларнинг таъсири шароитида унинг яхлитлигини, конфиденциаллигини, ишончлилигини, ҳақиқийлигини ва ундан фойдалана олишни таъминловчи усуллар ва воситаларнинг жами *ахборотни муҳофаза қилиш* дейилади [11].

*Криптотаҳлил* шифрни ёки ҳар қандай бошқа шаклдаги криптография объектининг сирини очиш санъати ва илми бўлиб, калитни билмасдан туриб шифрланган матндан дастлабки матнни олиш ёки дастлабки матн ва шифрланган матн бўйича калитни ҳисоблаш жараёнидир.

Криптотаҳлил билан шуғулланувчи мутахассис криптотаҳлилчи деб аталади.

Криптоалгоритмнинг криптотаҳлилга бардошлилиги, яъни криптотизимнинг турли ҳужумларга дош бера олиш қобилияти *криптобардошлилик* деб аталади [11].

Ахборотни муҳофаза қилиш тизимининг бир қисмини ёки бутун тизимни бузишга бўлган муваффақиятли ёки муваффақиятсиз уриниш *ҳужум* деб аталади [11].

Ҳужумнинг қуйидаги турлари мавжуд:

*1. Актив (фаол) ҳужум* - тизимга ёлғон ахборот ўрнаштириш ёки мавжуд ахборотни ўзгартириш йўли билан қилинадиган ҳужум.

*2. Луғат бўйича ҳужум* - тўғридан-тўғри қилинадиган турли кўринишли ҳужумнинг бири бўлиб, бу ҳужум пайтида махфий сўз (парол)лар қайта сараланади ва/ёки олдиндан тузилган махфий сўзлар рўйхатига мурожаат этилади.

*3. Фақат шифрланган матн бўйича ҳужум* - фақат берилган шифрматнга асосланган криптотаҳлил усули.

*4. Қўпол куч ҳужуми, тўлиқ танлаш* - мумкин бўлган қийматларнинг барчасини ёки салмоқли миқдорини ҳақиқий қиймат топилгунча танлашга асосланган ҳужум.

Ёлғон хабарлар ўрнаштиришга, хабарларни тутиб олиш ва ўзгартиришга, маълумотлар базасидан фойдаланишга, ўз ваколатини кенгайтиришга, ёлғон очиқ калитни ўрнаштиришга, сохта ҳужжатлар тайёрлашга, имзодан бош тортишга ва шу кабиларга уринаётган бузғунчи *актив (фаол) бузғунчи* ҳисобланади [11].

Криптографик баённомани издан чиқариш бўйича ҳаракат қилмайдиган бузғунчи *пассив (суст) бузғунчи* дейилади.

Ахборотни узатишда, сақлашда ёки қайта ишлашда, рақобатчи олдида муайян фойда олиш ёки унга зиён етказиш мақсадида атайлаб, ахборотни рухсат этилмаган тарзда ўзгартириш *ахборотни сохталаштириш* дейилади.

Дастлабки матнни шифрланган матндан шифрлаш калитини билмасдан туриб тиклаш билан тугайдиган криптотаҳлил жараёни *шифрни калитсиз очиш (кенг маънода дешифрлаш)* деб аталади.

*Криптотизимни бузиш* деганда маъқул бўлган вақтда замонавий ҳисоблаш воситаларидан фойдаланиб криптотаҳлил масалаларини ҳал этиш усулини топиш тушунилади.

## 1.2. Криптотаҳлилнинг зарурати

### 1.2.1. Криптотаҳлилнинг илмий фан сифатида шаклланиши

Кейинги ўн йилликлар криптологиянинг барча масалалари бўйича очиқ нашрий ишларнинг кескин ўсиб бориши билан характерланади. Ҳозирги кунда криптотаҳлил энг фаол ривожланаётган тадқиқот соҳаларидан бирига айланиб бормоқда. Бардошлилиги шубҳа остига олинмаган кўплаб криптотизимлар очиб ташланди. Криптотаҳлилчи учун катта қизиқиш уйғотадиган математик усулларнинг катта арсенали [6] яратилди.

1970 йиллар бошида фақат симметрик криптотизим маълум эди. Лекин бу мавзу бўйича очиқ эълон қилинган ишлар жуда кам эди [12]. Унга қизиқишнинг пастлиги қатор сабаблар билан белгиланади.

Биринчидан, тижорат учун мўлжалланган криптотизимларга қаттиқ талаб сезиларли даражада эмас эди.

Иккинчидан, асосий ишлар кўлами ёпиқ эканлиги янги натижа олишни истаган кўплаб тадқиқотчи олимларга қийинчилик туғдирар эди.

Учинчидан, энг аҳамиятли омил шуки, криптотаҳлил илмий фан сифатида шаклланмаган бўлиб, жиддий математик тамойиллар билан

бирлашмаган тарқоқ усул ("трюк") лар мажмуи эди холос.

1970 йилларда вазият тамоман ўзгарди. Биринчидан, алоқа тармоқларининг ривожланиши ва компьютерларнинг кундалик ҳаётга кириб бориши туфайли ахборотни криптографик муҳофаза қилиш заруратини жамиятнинг тобора кўпроқ табақалари тушуна бошлади.

Иккинчидан, Диффи-Хеллман томонидан 1976 йилда ошкора (очиқ) калитли криптографиянинг [12-13] ихтиро этилиши махфийликка бўлган тижорат талабларини қондириш учун замин яратди. Бу билан классик криптографиянинг камчилигини белгиловчи асрлар давомида ечилмай келган калитларни тарқатиш муаммоси ҳал бўлди. Аслида бу ихтиро илмий ҳамжамиятга катта туртки бўлиб, сифат жиҳатдан янги тадқиқ этилмаган соҳани очиб берди. Бу соҳа тез суръатлар билан ривожланиб бораётган ҳисоблаш мураккаблиги назариясига оид янги илмий натижаларни ишлаб чиқишга замин яратди ва бунинг оқибатида жиддий математикавий тамойилларга асосланган *криптотаҳлил йўналиши илмий фан сифатида* шаклланди.

Шифрлаш криптоалгоритмларига қўйиладиган асосий (биринчи) талабнинг моҳияти шундаки, алоқа канали орқали узатилаётган бирор ахборотнинг маъносини очиш худди шу калит билан шифрланган бошқа ахборотнинг маъносини очишга имкон туғдирмаслиги лозим.

Иккинчи талаб шифрлаш ва дешифрлаш аппаратурасини ишлатиш хусусиятларини назарда тутиш ва оператор ёки махфийлаштирилган ахборотни шакллантиришга аралашиш имкони бор шахслар томонидан йўл қўйиладиган баъзи эркинликларни эътиборга олади.

Криптотаҳлил умумий математик натижалардан фойдаланишга ҳам (масалан, катта сонларни туб кўпайтувчиларга ажратиш RSA криптотизимини очиш учун, дискрет логарифмлаш Эль Гамал [14-18] тизимини очиш учун), муайян криптоалгоритм учун олинган хусусий ҳол бўйича натижаларга ҳам таяниши мумкин. Қоида тарзида, криптотаҳлил алгоритмлари эҳтимоллик алгоритмларидир.

Қуйидаги 1-жадвалда криптотаҳлилчида мавжуд бўлган ахборотга боғлиқ ҳолда амалга оширилиши мумкин бўлган криптотаҳлил турларининг умумлашган рўйхати келтирилган [6, 19].

1-жадвал

**Криптотаҳлил турлари**

| **Криптотаҳлил тури** | **Криптотаҳлилчига маълум маълумотлар** |
|---|---|
| Фақат шифрматн бўйича таҳлил | • Шифрлаш алгоритми<br>• Дешифрлаш лозим бўлган шифрматн |
| Маълум очиқ матн бўйича таҳлил | • Шифрлаш алгоритми<br>• Дешифрлаш лозим бўлган шифрматн<br>• Битта махфий калит билан ҳосил қилинган очиқ (дастлабки, асл) матн ва шифрматнлар мос қисмларининг бир ёки бир нечта жуфтлиги |
| Танлаб олинган очиқ матн асосидаги таҳлил | • Шифрлаш алгоритми<br>• Дешифрлаш лозим бўлган шифрматн<br>• Криптотаҳлилчи танлаган очиқ матн ва унга мос, махфий калит ёрдамида яратилган шифрматн |
| Танланган шифрматн бўйича таҳлил | • Шифрлаш алгоритми<br>• Дешифрлаш лозим бўлган шифрматн<br>• Криптотаҳлилчи танлаган шифрматн ва унга мос махфий калит ёрдамида шифри очилган очиқ матн. |
| Танланган матн бўйича таҳлил | • Шифрлаш алгоритми<br>• Дешифрлаш лозим бўлган шифрматн<br>• Криптотаҳлилчи танлаган очиқ матн ва унга мос, махфий калит ёрдамида яратилган шифрматн<br>• Криптотаҳлилчи танлаган шифрматн ва унга мос махфий калит ёрдамида шифри очилган очиқ матн. |

Бу жадвалдаги танланган шифрматн  ва танланган матн бўйича таҳлил криптотаҳлилчилар томонидан кам ишлатиладиган таҳлил турлари сирасига киради.

### 1.2.2. Криптотаҳлилнинг мақсади ва объекти

Криптотаҳлилдан мақсад, махфий калитни билмаган ҳолда, шифрни очиб, шифрматннинг аслини тиклаш ёки шифрланган сигналларни аслига мос деб қабул қилинадаган бошқа мазмун бериб, сохталаштиришдир. Криптотаҳлилда одатда биринчидан шифрматн, иккинчидан махфий калитдан бошқа шифрлашнинг барча алгоритми ва протоколлари маълум деб ҳисобланади. Шифрматнни шу ҳол учун етарли даражада бардошли қилиб ҳосил қилиш криптографнинг асосий вазифасидир. Агар криптограф буларга қўшимча тарзда, рақиб томон криптотаҳлилчисига шифрматнга тегишли асл матннинг ўзи ёки унинг бир неча парчаси маълум деб саналган ҳол учун етарли бардошлиликка эга бўлган криптотизим ҳосил этса, бундай тизим *асл матн асосида таҳлилга нисбатан бардошли тизим* деб аталади.

Кўпчилик замонавий шифр яратувчилар тизим бардошлилигини танланган асл матн асосида криптотаҳлилга нисбатан бардошлилик (бунда шифр матни ҳам маълумлиги назарда тутилади) билан белгилайдилар.

Ошкора калитли криптотизим криптотаҳлилчисининг асосий мақсади, унинг нияти бузуқ бўлса, махфий (шахсий) калитни билмаган ҳолда ошкора калит ва ҳимояланмаган алоқа каналидан жўнатилган ошкора ахборотдан фойдаланган ҳолда жўнатилган ахборотни сохталаштириб, бу ахборотни ошкора калит эгасига тегишли эканига ахборот қабул қилувчида тўла ишонч ҳосил бўлишига эришишдир. Бу мақсадга нияти бузуқ криптотаҳлилчи икки йўлдан бирини танлаган ҳолда эришиши мумкин: хэш-функцияда (у барча учун ошкора) коллизия топа олса ёки факторлаш, дискрет логарифм ёки ЭЭЧда дискрет логарифмлаш муаммоларидан бирини ечишга етарли вақт ва ҳисоблаш ресурсларига эга бўлса.

ЭРИ ва аутентификация муаммоларини ечишда криптограф

тизимнинг хавфсизлигини таъминлашда очиқ матн ва шифрланган матнга қўшимча хэш-функциянинг ҳам маълумлигини эътиборга олиши лозим, чунки хэш–функция криптотизимнинг шифрлаш ва дешифрлашга оид барча механизмлари сифатида криптотаҳлилчига маълум ҳисобланади ва муҳим ҳужум объекти саналади.

Хэш-функция [20-22] ахборотни бир томонлама ўзгартиришдир. Унинг алоҳида томони шундаки, $y=H(x)$ осон ҳисобланади. Лекин, унинг тескариси $x= H(y)$ ни ҳисоблаш мушкул.

Криптотизим яратувчиси криптотаҳлилчига нималар маълум бўлиш эҳтимолини қанчалик кўп эътиборга олган бўлса, тизим шунчалик бардошлироқ бўлиб чиқади.

Хэш-функцияларнинг типик қўлланиши шундаки, берилган матннинг шундай зичлаштирилган образи яратилсинки, унинг аслини ҳисоблаб топиш асосида тиклашнинг имконияти бўлмасин.

Криптотизимлар қандай таҳлил объектига нисбатан бардошлилигига кўра қуйидаги синфларга бўлинадилар. Булар:

1. Шифрланган матн асосида криптотаҳлилга нисбатан бардошли.
2. Очиқ (асл) матн асосида таҳлилга нисбатан бардошли.
3. Танланган асл матн асосида таҳлилга нисбатан бардошли.
4. Танланган шифрматн асосида таҳлилга нисбатан бардошли.
5. Очиқ калит асосида криптотаҳлилга нисбатан бардошли (ошкора криптотизимлар учун).
6. Имзо асосида криптотаҳлилга нисбатан бардошли (аутентификация ва ЭРИ учун).
7. Хэш-функция асосида таҳлилга нисбатан бардошли (аутентификация ва ЭРИ учун).

Криптотаҳлил усуллари ҳам таҳлил объекти синфларига мос тарзда қуйидаги синфларга бўлинади:

1. Шифрланган матн асосида криптотаҳлил.
2. Очиқ матн асосида криптотаҳлил

3. Танланган очиқ матн асосида криптотаҳлил.
4. Танланган шифрматн асосида криптотаҳлил.
5. Очиқ калит асосида криптотаҳлил (ошкора криптотизимлар учун).
6. Имзо асосида криптотаҳлил (аутентификация ва ЭРИ учун).
7. Хэш-функция асосида криптотаҳлил.

Бундан ташқари криптотаҳлил усуллари криптотизимнинг бардошлилигини таъминловчи муаммо [1-2, 6, 9] турига қараб ҳам фарқланадилар.

## 1.3. Криптографик алгоритмлар бардошлилиги тушунчаси

### 1.3.1. Криптографик бардошлилик

Криптобардошлилик (бардошлилик) деб - криптотизимнинг ҳужумларга қарши тура олиш қобилиятига айтилади [11]. Миқдорий жиҳатдан криптобардошлилик етарли эҳтимоллик билан криптотаҳлилчини муваффақиятга элтадиган энг яхши криптотаҳлил алгоритмининг мураккаблиги билан ўлчанади [6].

Криптоалгоритмлар улар хавфсизлигининг исботлана олувчанлик даражаси билан фарқланадилар.

Сўзсиз бардошли, исботланарли бардошли ва фараз бўйича бардошли криптоалгоритмлар мавжуд. Сўзсиз бардошли криптоалгоритмларнинг хавфсизлиги калитни очиш мумкин эмаслигини исботловчи теоремаларга асосланади. Масалан, Вернам шифри (бир марта фойдаланиладиган калитли) сўзсиз бардошлидир.

Исботланарли бардошли криптотизимларнинг бардошлилиги барча томонидан мураккаблиги тан олинган ва кўплаб математиклар ечишга уриниб еча олмаган яхши маълум математика масаласи (муаммо)нинг ечиш мураккаблиги билан аниқланади. Масалан, Диффи-Хеллман ёки Райвест-Шамир-Адлеман (RSA) алгоритмлари шу синфга оид. Буларнинг бардошлилиги дискрет логарифмлаш ва бутун сонни туб кўпайтувчиларга

ажратиш масалаларининг мураккаблиги билан белгиланади.

Фараз бўйича бардошли криптоалгоритмлар бир ёки бир неча киши уриниб кўрган ва яхши ўрганилган масалаларга келтирилмайдиган хусусий математика масалаларига асосланади. Лекин, уларга катта эпчиллик хос бўлиб, криптоалгоритмлардан бўш жойлар пайқалганда улардан воз кечмай буни ҳисобга олиб яна қўшимча ишлаш кўп вақтни олмайди. Масалан, DES, ГОСТ 28147-89, FEAL, IDEA ва бошқалар [14-16]. Афсуски, сўзсиз бардошли криптотизимлар амалиётда ноқулайдир.

Исботланарли бардошли криптоалгоритмларнинг хавфсизлиги улар асосига олинган масалаларнинг яхши ўрганилганлигидадир. Камчилиги зарурат туғилганда криптоалгоритмни тезкор тарзда қайта қуриш имконияти йўқлигидадир. Улар "қаттиқ" тизимлар бўлиб, уларнинг бардошлилигини оширишга математика масаласи ўлчамларини ошириш ёки алмаштириш орқали эришилади. Бу албатта, шифрланган аппаратдагина эмас, балки унга қўшни жиҳозларда ҳам ўзгаришлар занжирини юзага келтиради.

Фараз бўйича бардошли криптоалгоритмлар тегишли математика масалаларининг нисбатан кам ўрганилганлиги билан характерланади.

Калит бардошлилиги, калитсиз ўқишга бардошлилик, имитобардошлилик (тақлидга бардошлилик) ва ёлғон ахборотни тиқиштириш тушунчаларини фарқлаш лозим.

Калит бардошлилиги - бу энг яхши маълум алгоритм билан калитни топиш мураккаблигидир.

Имитобардошлилик - бу энг яхши маълум алгоритм ёрдамида ёлғон ахборотни рўкач қилишдир.

Шунга ўхшаш, криптоалгоритмнинг ўз бардошлилиги, протокол бардошлилиги, калитлар ҳосил қилиш алгоритми ва тарқатиш бардошлилиги фарқланади.

Бардошлилик сатҳи криптотаҳлилчининг имкониятларига ва фойдаланувчига боғлиқ.

Калитлар бардошлилиги  сатҳлари берилган криптотизим учун

қуйидаги тартибга бўйсунади:

Калитнинг матнлар асосида таҳлилга нисбатан бардошлилиги $Б_{тм}$ асл (очиқ) матн асосида таҳлил $Б_{м}$ дан, $Б_{м}$ эса шифрланган матн асосида таҳлилдаги калит бардошлилиги $Б_{шм}$ дан оша олмайди:

$$Б_{тм} \le Б_{м} \le Б_{шм}.$$

Айрим ҳолларда криптограф ҳатто рақиб томон криптотаҳлилчиси криптотизимга аралашиши, яъни "ўзиники" бўлиши мумкин деб ҳисоблаган ҳол учун ҳам яроқли бардоши етарли криптотизим ярата олади.

Одатда яратиладиган криптоалгоритмлар махсус танланган асл матнларга асосланган криптотаҳлилга нисбатан бардошли қилиб яратилади. Бардошлилик таърифида калитни топишдаги "энг яхши" алгоритм тушунчаси конструктив бўлмагани учун унинг талқини субъективдир. Қайсидир криптоалгоритмни энг яхши алгоритм сифатида қарашда калитни оддий қараб чиқиш орқали топишга солиштирилади.

Фойдаланилаётган бирорта криптоалгоритм учун калит топишнинг энг яхши алгоритми аниқланмаган, зеро бундай энг яхши алгоритмни топиш фавқулодда мураккаб масаладир. Шу туфайли амалиётда бардошлиликни баҳолашда энг яхши маълум ёки тадқиқотлар давомида аниқланган топиб очиш алгоритмидан фойдаланилади. Шундай қилиб, амалиёт қобилиятли криптотаҳлилчига янги, самаралироқ таҳлил усулини ўйлаб топиб бардошлилик баҳосини камайтиришга ҳалал бера олмайди.

Калитни топишнинг янги самарали усулини яратиш ёки криптоалгоритмни заифлаштиришнинг бошқа усулини яратиш мазкур криптоалгоритмдан фойдаланувчиларга зарар келтириши борасида катта имкониятлар яратади, бундай тадқиқотларни эълон қилиш ёки яшириш жамиятнинг очиқлик даражасига ҳам боғлиқ. Оддий фойдаланувчи бузғунчининг калитни бузиб очишига ҳеч қандай қаршилик қила олмайди.

Маълумки, «энг яхши маълум» алгоритм тушунчаси мутлақ эмас. Эртага бузиб очишлик янги самарали алгоритмини яратилмаслигига ҳеч ким кафолат бера олмайди. Бунда криптоалгоритм истеъмолдан чиқади.

Математика фанининг ва ҳисоблаш техникасининг тараққиёти ошиб борган сари криптоалгоритмнинг бардошлилиги камайиб бораверади. Криптоалгоритмни ўз вақтида алмаштирмасликдан мумкин бўлган зарарнинг олдини олиш учун криптоалгоритм бардошлилигини даврий тарзда қайта текшириб бориш мақсадга мувофиқдир. Янгидан ишлаб чиқилган криптоалгоритмнинг башорат қилиб бўлмайдиган *нураб кетиши* эҳтимолини пасайтириш учун криптографик тадқиқотлар олиб бориш зарурдир.

Айтилганлардан келиб чиқадики, криптотизим бардошлилиги кўп қирралидир. Бардошлилик нафақат ишлаб чиқувчидан, бошқарув ва алоқа тизимида мазкур криптоалгоритмдан фойдаланиш хусусиятларига, криптотизимнинг физикавий амалга оширилишига ҳамда математика ва ҳисоблаш техникасининг келажакдаги ютуқларига боғлиқ. Ахир криптотизим кўп йиллар давомида ишлатилиши мумкин, авваллари очиқ алоқа каналлари орқали узатилган ахборотни сир сақлаш зарурати фан ва техника тараққиётини ўнлаб йиллар учун олдиндан башорат қилиш заруратини туғдиради.

Кўп тизимларнинг бардошлилиги ишончли суръатда кўплаб яхши маълум масалаларнинг ечила олмаслигига суянади ва балки вақт ўтиши билан баъзи криптотизимларнинг бузиб очилиши принципиал мумкин эмаслигини исботлаш мумкин бўлар.

Аммо криптография масалаларини яхши ўрганилган математик масалаларга келтириш орқали исботланадиган бардошлиликка эришиш умидлари оқланмади, қайтага бунинг акси юз берди. Худди шу криптография масалаларини жозибали математика масаласига келтириш кўп криптотизимларни очиб ташлашга олиб келди. Ҳозирги кунда анъанавий бир марта ишлатиш лентаси ягона сўзсиз бардошли шифрлаш тизими бўлиб қолмоқда.

Идеал тарзда бирор ошкора калитли криптотизимнинг бардошлилигини исботлаш учун бу тизимни очишнинг ҳисобга олишга арзийдиган очиш эҳтимолига эга бўлган ҳар қандай алгоритми амалга

ошириб бўлмайдиган катта ҳисоблашлар билан боғлиқлигини исботлашга келтирилиши кифоя. Бирорта ҳам маълум бўлган ошкора калитли криптотизим бу кучли бардошлилик мезонини қаноатлантирмаса ҳам вазиятни мутлақо умидсиз деб баҳолаш ўринсиз. Кўплаб ишлаб чиқилган тизимларга нисбатан уларнинг бардошлилиги айрим аҳамиятли ва деярли барча томонидан жуда мураккаб деб тан олинган масалани ечиш мураккаблигига эквивалентлиги исботланган. Бутун сонларни туб кўпайтувчиларга ажратиш ва дискрет логарифмлаш масалалари шулар жумласидандир. Шунинг учун ҳам DH калит тарқатиш тизими, RSA ва Эль Гамал [17-18] криптотизимлари бардошлилиги исботланадиган криптотизимлар синфига мансубдир. Кейинги ўн йилликлар давомида криптография ва ҳисоблаш мураккаблиги назарияси соҳасида олиб борилган тадқиқотлар замонавий криптотаҳлилчига у ишлаб чиққан криптотизимни бардошлилигини нима пасайтириши сабабларини чуқурроқ тушунишга ёрдам беради.

Кўпдан бери мавжуд бўлган ва яқинда юзага келган криптотизимлар учун криптотаҳлил олиб бориш жуда долзарб масаладир. Чунки шундагина берилган криптотизимнинг бардошли эмаслиги ҳақида ўз вақтида фикр билдириш мумкин бўлиб, уни яхшилаш ёки бошқасига алмаштириш имкони туғилади. Бардошсиз криптотизимларни ўз вақтида пайқаш учун эса ҳар доим маълум бўлган криптотаҳлил усулларини мукаммаллаштириш ва янгиларини топиш лозим бўлади.

### 1.3.2. Симметрик ва носимметрик криптотизимлар бардошлилигини таъминловчи тамойиллар ва муаммолар

Маълумки, 1975 йилгача криптографияда симметрик криптотизимлардан фойдаланилган. Шу йилдан бошлаб носимметрик криптотизимлар юзага келгач, аутентификация, яъни ахборот муаллифининг асли ким эканлигини ахборот қабул қилувчи ва ундан бошқалар учун

тасдиқлаш имконияти туғилди. Шундан бошлаб криптография мақсадларидан яна бири аутентификация бўлиб қолди.

Илмий криптография даврининг муҳим муваффақиятлари рўйхати бошида Клод Эльвуд Шенноннинг 1949 йилда яратилган ***«Махфий тизимларда алоқа назарияси»*** асари туради [9, 12, 23-24]. Унда ахборот муҳофазасининг назарий тамойиллари шакллантириб берилган.

К.Э. Шеннон томонидан қилинган бундай кашфиёт у яратган ахборот назарияси фани туфайли юзага келган эди. К.Э. Шеннон нафақат Вернамнинг тасодифий шифрини бузиб очиб бўлмаслигини, балки ҳимояланган канал орқали узатиладиган махфий калит миқдори (битлар сони) чегараларини ҳам аниқ кўрсатиб берди. У чекланмаган ресурсларга эга бўлган криптотаҳлилчи бирор «тасодифий шифр»ни очишида махфий калитни топиши учун зарур бўлган шифрланган матндаги белгилар сони $S$ қуйидагича ифодаланишини кўрсатди:

$$S = H(k)/(r*Log\ n).$$

Бу ерда: $H(k)$ - калит энтропияси, яъни калитнинг ҳар битта белгисига тўғри келадиган ахборот миқдори, $r$ - очиқ матннинг сериборалиги, $n$ - алифбо ҳажми.

Келтирилган ифода шифрланадиган матннинг сериборалиги нолгача пасайтирилса, криптотаҳлилчи кичик калит билан шифрланган матнни ҳам оча олмаслигини кўрсатади. Демак, шифрлаш олдидан ахборотни статистик кодлаш (зичлаштириш, архивлаш) лозим. Бунда ахборотнинг ҳажми ва сериборалиги камаяди, энтропияси ошади.

К. Шеннон криптотизимларнинг бардошлилигини ***назарий*** ва ***амалий*** турларга ажратади. Назарий бардошлилик деганда рақиб томоннинг таҳлилчиси у қўлга туширган криптограммаларни таҳлиллашда чекланмаган вақтга ва барча зарур воситаларга эга бўлган ҳолда криптотизимнинг бардошлилиги тушунилади. Амалий бардошлилик деганда криптотаҳлилчининг вақти ва ҳисоблаш имкониятлари чекланган ҳолга оид бардошлилик тушунилади. К. Шеннон амалий шифрларда ишлатиладиган

икки тамойилни ажратади. Булар ***ёйиш ва аралаштиришдир***. Ёйиш деганда, очиқ матннинг битта белгисини шифрланган матннинг кўп белгиларига таъсир этиши тушунилади. Бу очиқ матннинг статистик хоссаларини яширишга имкон беради. Бу тамойил калит белгиларига нисбатан ҳам қўлланилади. Аралаштириш деганда, К. Шеннон шифрланадиган ва шифрланган матнларнинг статистик хоссаларининг бир-бирига боғланишини тиклашни қийинлаштирувчи шифрлашга оид ўзгартиришларни назарда тутган.

К. Шенноннинг «яхши» шифр яратиш муаммоси маълум шартларни қондирувчи энг мураккаб масалаларни топишга келтирилади. «Бизнинг шифримизни шундай тузиш мумкинки, уни бузиб очиш ечилиши катта ҳажмдаги ишларни талаб қилиши маълум бўлган муаммони ўз ичига олсин ёки унга эквивалент бўлсин» деган луқмаси эътиборга лойиқдир.

Симметрик криптотизимга оид бошқа тамойиллар ҳам мавжуд. Булар зарурий бардошлиликни таъминловчи криптографик хоссалар, шартлар ва мезонлар бўлиб, улар билан кейинги бўлимда танишилади.

Мавжуд носимметрик криптотизимлар бардошлилигини таъминлашга асос бўлган мураккаб муаммо (масала) тури бўйича қуйидагича таснифланади (2-жадвал):

- факторлаш муаммосининг мураккаблигига асосланган криптотизимлар;
- дискрет логарифм муаммосининг мураккаблигига асосланган криптотизимлар;
- эллиптик эгри чизиқда дискрет логарифм муаммосининг мураккаблигига асосланган криптотизимлар;
- бошқа муаммоларга асосланган криптотизимлар [2].

2-жадвал

**Муаммо тури бўйича носимметрик криптотизимлар таснифи**

| **Муаммо** | **Баёни** |
|---|---|
| Факторлаш | Бутун факторлаш муаммоси: бутун мусбат *n* берилган, унинг Туб факторларини топиш керак: яъни, $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ кўринишда ёзиш керак, бу ерда $p^i$ - турли туб сонлар ва ҳар бири $e_i \geq 1$. |
| RSA муаммоси (RSAP) | RSA муаммоси (RSA инверсия каби маълум): иккита турли *p* ва *q* тоқ сонларнинг кўпайтмаси бўлган бутун мусбат *n* сони, *EKUB (e, (p-1)(q-1))=1* га тенг бўлган бутун мусбат *e* сони ва бутун *c* берилган, шундай бутун *m* ни топиш керакки, унда $m^e \equiv c \pmod{n}$ бўлсин. |
| Квадратик чегирма муаммоси (QRP) | Квадратик чегирма муаммоси: тоқ мураккаб бутун *n* ва $\left(\frac{a}{n}\right) = 1$ Якоби белгисига эга бўлган бутун *a* сони берилган, *a* сони *n* модуль бўйича квадратик чегирма эканлиги ёки чегирма эмаслиги аниқлансин. |
| *n* модули бўйича квадрат илдиз (SQROOT) | *n* модули бўйича квадрат илдиз: мураккаб бутун *n* сони ва $a \in Q_n$ (*n* модули бўйича квадратик чегирма тўплами) берилган, *n* модули бўйича *a* дан шундай бутун квадратик илдиз *x* топилсинки, унда $x^2 = a \pmod n$ бўлсин. |
| Дискрет логарифм муаммоси (DLP) | Дискрет логарифм муаммоси: Туб сон *p* учун, чекли майдон $Z_{p*}$ да ҳосил қилувчи (генератор) элемент $\alpha$ ҳамда $\beta \in Z_{p*}$ берилган бўлса, шундай $0 \leq x \leq p-2$ бўлган бутун *x* сон топилсинки, унда $\alpha^x \equiv \beta \pmod p$ бўлсин, бу ерда *x* – даража кўрсаткичи. |

| **Муаммо** | **Баёни** |
|---|---|
| Умумлашган дискрет логарифм муаммоси (GDLP) | Умумлашган дискрет логарифм муаммоси: *n* тартибли чекли циклик группа *G, G* нинг ҳосил қилувчиси $\alpha$ ва $\beta \in G$ элемент берилган, шундай $0 \le x \le n-1$ бўлган бутун *x* сони топилсинки, унда $\alpha^x = \beta$ бўлсин. |
| Диффи-Хеллман муаммоси (DHP) | Диффи-Хеллман муаммоси: туб сон *p, Zp** ҳосил қилувчиси - $\alpha$ ва $\alpha^a \ (mod\ p)$ ва $\alpha^b \ (mod\ p)$ элементлари берилган, $\alpha^{ab} \ (mod\ p)$ топилсин. |
| Умумлашган Диффи-Хеллман муаммоси (GDHP) | Умумлашган Диффи-Хеллман муаммоси: чекли циклик группа *G, G* ҳосил қилувчиси - $\alpha$ ва группа элементлари $\alpha^a$ ва $\alpha^b$ лар берилган, $\alpha^{ab}$ топилсин. |
| Қисм тўплам - йиғиндиси (SUBSET-SUM) | Қисм тўплам-йиғиндиси муаммоси: бутун мусбат сонлар тўплами $\{a_1, a_2, ..., a_n\}$ ва бутун мусбат сон *S* берилган, йиғиндиси *S* га тенг бўлган $a_j$ қисм тўплам мавжудми ёки йўқми аниқлансин. |
| Эллиптик эгри чизиқда дискрет логарифм муаммоси (ECDLP) | Эллиптик эгри чизиқли дискрет логарифм муаммоси: *K* чекли майдон ва *G* нуқтада тартиби *n* бўлган *G* нуқта, $Q \in E(K)$ нуқтада *E* ЭЭЧ берилган. $Q=[d]G$ шартни қаноатлантирувчи *d*, $0 \le d \le n-1$ бутун сонни топиш талаб этилади, агарда у мавжуд бўлса. |

| Муаммо | Баёни |
|---|---|
| Даража параметри муаммоси | 1-таъриф. Агар параметрли группа $(F_n; ®)$ да ташувчи $F_n$ нинг элементи $y$ берилган бўлса, унда параметр $R$, даража кўрсаткичи $e$ ва элемент $a$ топилсин.<br>2-таъриф. Агар параметрли группа $(F_n; ®)$ да ташувчи $F_n$ нинг элементлари $y$ ва $a$ берилган бўлса, унда параметр $R$ ва даража кўрсаткичи $e$ топилсин.<br>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, $\varphi(n)>R>1$, 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, $n \in \{p, p_1 * p_2\}$, $p$, $p_1$, $p_2$ – туб сонлар. |

Мавжуд носимметрик криптоалгоритмлар орасида халқаро ва давлат стандартлари мақомига эга бўлган ЭРИ алгоритмларининг кўпчилиги факторлаш (RSA, ESIGN), дискрет логарифмлаш (DSA, ГОСТ Р 34.10–94), ЭЭЧда дискрет логарифмлаш (ГОСТ Р 34.10-2001, EC-DSA-2000, EC-KCDSA, EC-GDSA ва ДСТУ 4145-2002) ва даража параметри (O'z DSt 1092:2005, O'z DSt 1092:2009) муаммоларининг мураккаблигига асосланган алгоритмлардир.

Симметрик криптотизимлар учун шифрлаш калитини очиқ канал бўйича тақсимлаш алгоритмлари асосида Диффи-Хеллман муаммосининг мураккаблиги ётади. Шу боис, факторлаш, дискрет логарифмлаш, ЭЭЧда дискрет логарифмлаш, Диффи-Хеллман ва даража параметри муаммоларини ҳал этиш кўпчилик криптотаҳлилчиларнинг эътиборини ўзига тортади.

## Назорат саволлари

1. Протокол ва криптографик протоколга таъриф беринг. Бу тушунчаларнинг фарқи нимада?

2. Ахборотни муҳофаза қилиш деганда нимани тушунасиз?

3. Криптотаҳлил ва криптотаҳлилчи деганда нимани тушунасиз, криптотаҳлилчининг мақсади нима?

4. Криптотаҳлилчи учун таҳлиллаш объекти нима?

5. Алгоритм, протокол, тизим криптобардошлилиги деганда нималарни тушунасиз?

6. Актив ва қўпол куч ҳужумлари орасида қандай фарқ мавжуд? Яна қандай ҳужум турларини биласиз?

7. Ахборотни сохталаштириш, криптотизимни бузиш деганда нимани тушунасиз?

8. Криптотаҳлил йўналиши илмий фан сифатида қачон шаклланган, бунга қандай омиллар сабаб бўлган?

9. Шифрлаш криптоалгоритмларига қандай асосий талаблар қўйилади?

10. Криптоалгоритмлар бардошлилиги деганда нимани тушунасиз? Назарий ва амалий бардошлиликларнинг фарқи нимада?

11. Сўзсиз бардошли, исботланарли бардошли ва фараз бўйича бардошли криптоалгоритмларнинг бир биридан фарқи нимада?

12. Калит бардошлилиги, калитсиз ўқишга бардошлилик, имитобардошлилик ва ёлғон ахборотни тиқиштириш тушунчаларининг фарқлари нимада?

13. Қандай криптотаҳлил турларини биласиз?

14. Калитлар бардошлилиги сатҳлари берилган криптотизим учун қандай тартибга бўйсунади?

15. Қандай криптотаҳлил йуналишларини биласиз? Криптоалгоритм, танланган асл матнлар асосида криптотаҳлилга нисбатан бардошли бўлиши етарлими?

16. Криптотизимлар таҳлил объектига нисбатан бардошлилигига кўра қандай синфларга бўлинадилар?

17. Криптотаҳлил усуллари қандай синфларга бўлинади?

18. К. Шеннон криптотаҳлилчи бирор «тасодифий шифр»ни очишда махфий калитни топиши учун зарур бўлган шифрланган матндаги белгилар сони $S$ ни қандай ифодалар орқали берган?

19. К. Шеннон амалий шифрларда ишлатиладиган қандай тамойилларни ажратган, бу тамойиллар ҳақида қандай тушунчага эгасиз?

20. Мавжуд носимметрик криптотизимлар бардошлилигини таъминлашга асос бўлган мураккаб муаммолардан қайси турларини биласиз? Уларнинг қайсилари кўпчилик носимметрик криптотизимлар яратишга асос бўлган?

21. Дискрет логарифм ва факторлаш муаммоларига таъриф беринг?

22. Эллиптик эгри чизиқда дискрет логарифмлаш муаммосига таъриф беринг?

23. Даража параметри муаммосига таъриф беринг?

## 2. КРИПТОТАҲЛИЛНИНГ УНИВЕРСАЛ УСУЛЛАРИ

Охирги йигирма йил ичида криптотаҳлил фаол ривожланаётган тадқиқот соҳаларидан бирига айланди. Криптотаҳлилчиларда қизиқиш уйғотадиган математик усулларнинг бутун бир арсенали пайдо бўлди. Бундан ташқари, ҳисоблаш техникаси самарадорлиги ошиши натижасида аввал мавжуд бўлмаган ҳужум турларининг пайдо бўлишига олиб келди [25]. Қуйидаги 1-расмда криптотаҳлил усулларининг пайдо бўлиши вақт бўйича ва турли хил криптотизимларни бузишда қўлланилиши бўйича тизимлаштирилган маълумот келтирилган.

| | | | |
|---|---|---|---|
| **Хэш-функция** | | **5, 8** | |
| **Носимметрик шифр** | | **1, 2, 3, 4** | **9** |
| **Симметрик шифр** | **1, 2** | **3, 6, 7** | **9** |
| | **Кеча** | **Бугун** | **Келажакда** |

1-расм. Криптотаҳлил усуллари

Бу ерда:

1 - Калитларни тўлиқ танлаш усули.

2 - Частотавий таҳлил усули.

3 - Калит генератори таҳлили.

4 – Поллард усули.

5 - «Ўртада учрашиш» усули.

6 - Дифференциал таҳлил усули.

7 - Чизиқли таҳлил усули.

8 - Коллизия усули.

9 - Қўшимча каналлар бўйича таҳлил усули.

1-расмда келтирилган криптотаҳлил усуллари бўйича маълумотлар кейинги бўлим ва параграфларда баён этилган.

Ҳар қандай криптотизимнинг бардошлилиги криптоалгоритмга ва калитнинг хоссаларига эга бўлиши билан бир қаторда ишончли пухта протоколга ҳам эга бўлиши шарт. Пухта математик асосга эга бўлиб, мукаммал баённомага эга бўлмаган криптотизим заиф ва бардошсиз бўлиши мумкин.

Криптотизимларни криптотаҳлиллашнинг универсал усуллари қаторига ҳозирги кунда қўлланиб келинаётган ва самарали натижа берадиган тўлиқ танлаш, частотавий таҳлил, ўртада учрашиш, Поллард, калит бўйича ҳужум ва хэш-функция коллизияси усулларини [1, 6, 9, 25] ҳамда қўшимча каналлардан фойдаланишга асосланган криптотаҳлил усулларини [25-26] киритиш мумкин.

### 2.1. Тўлиқ танлаш усули

Тўлиқ танлаш, яъни калитларнинг *барча мумкин бўлган вариантларини танлаш усули,* криптотаҳлилчининг носимметрик криптотизим алгоритмини ва ошкора калитни билган ҳолда барча мумкин бўлган калитларни танлаш ва синаб кўришга асосланади. Симметрик криптотизимларда ҳам шифрматн ва очиқ матн асосида тўлиқ танлаш усули қўлланилади. Криптотаҳлилчилар кўпинча компьютер ёрдамида калитларни тўлиқ танлаш усулидан фойдаланиб шифрларни ошкор этадилар. Криптотаҳлил жараёнида миллиард калитларни секундига минглаб калит тезликда танлашга тўғри келади.

Фараз қилинсин, бузғунчи учун бир ёки бир неча *(x, y)* жуфтлик маълум бўлсин. Осонлик учун ҳар қандай жуфтлик *(x, y)* учун $E_k(x)=y$ муносабатни қаноатлантирувчи ягона $k$ калит мавжуд бўлсин. Мумкин бўлган калитлар тўпламини тартибга солинади ва $K$ даги калитларни кетма-кет равишда $E_k(x)=y$ тенглик бажарилишига текшириб чиқилади. Агар $k \in K$

калитнинг бир вариантини текшириш бир амал ёрдамида ҳисобланса, унда калитларни тўлиқ танлаш учун $|K|$ амал талаб этилади. Бунда $|K|$ - тўпламдаги элементлар сони. Шифрлаш схемасида калит тасодифий ва тенг эҳтимоллик билан $K$ тўпламдан танланган бўлсин. Бунда калит $1/|K|$ эҳтимоллик билан билан топилади ва тўлиқ танлаш усулининг иш ҳажми $1$ га тенг бўлади [25].

Мисол учун шахсий калит узунлиги $100$ бит бўлса, унда барча шахсий калитлар сони $2^{100}$ га тенг, яъни калитлар тўплами қуввати $|K|=2^{100}$. Шахсий калит узунлиги $56$ бит бўлганда, барча мумкин бўлган шахсий калитлар сони $|K|=2^{56}\approx 0.5*10^{17}$ га тенг. Бунда, агар ҳисоблаш қурилмаси ҳар битта махфий калитга мос ошкора калитни ҳисоблаш ва уни ҳеч қийинчиликсиз таққослаш учун $10^{-6}$ секунд вақт сарфласа, $24$ соатда барча калитларни синаб чиқиш учун $5.787*10^{5}$ та ЭҲМ керак бўлади [1].

Шунинг учун ҳам шахсий ва шифрлашда фойдаланиладиган калитни топишни мураккаблаштириш мақсадида шахсий калитлар узунлиги $127$-$159$ битдан катта бўлган узунликда генерацияланади.

### 2.2. Калит бўйича ҳужум

Криптотаҳлилчининг махфий калитни топишга қаратилган хатти-ҳаракатлари *криптоҳужум* деб аталади.

Криптоҳужумдан мақсад калитни билмаган ҳолда шифрматнни очишдир. Криптотизимга ҳужум қилиш учун криптотаҳлилчи зарурий криптотаҳлил воситаларига эга бўлиши керак. Бу воситалар криптоҳужум қўлланиладиган шифрлаш алгоритмининг акслантиришлари хусусиятларини ҳисобга олиб, шифрматнни шифрлаш алгоритми калитини билмаган ҳолатда шифрматнни очиш мақсадида математик моделлаштириш усулларини қўллаш асосида яратилади [1, 25].

Криптотизимнинг ишончсизлиги сабабларидан бири тизимда кучсиз калитлардан фойдаланиш ҳисобланади, чунки кучсиз калитлар етарли даражада ҳимоялаш даражасини таъминлай олмайди. Шу сабабли

калитларни ҳосил қилиш жараёнида уларни яроқсизга чиқариш учун барча кучсиз калитлар аввалдан маълум бўлиши лозим. Тасодифий сон генераторлари криптографик тизимларнинг бардошлилиги учун яна бир хавф манбаидир. Агар калитларни генерациялашда кучсиз криптографик алгоритмлардан фойдаланилса, фойдаланилган шифрдан қатъий назар бутун тизим бардошсиз ҳисобланади.

Симметрик криптотизимларда фойдаланиш учун мўлжалланган сифатли калит тасодифий иккилик тўпламини ифодалайди. Агар $n$ разрядли калит талаб этилса, калитни генерациялаш жараёнида мумкин бўлган $2^n$ вариантлардан бир хил эҳтимоллик билан танлаб олиш керак.

Носимметрик криптотизимларда фойдаланиш учун мўлжалланган сифатли калитларни генерациялаш эса анча қийин жараён бўлиб, юқорида айтилганидек бу тизимда фойдаланиладиган калитлар муайян математик хоссаларга эга бўлиши лозим. Масалан, RSA тизимида шифрлаш модули иккита катта туб сонларнинг кўпайтмаси кўринишида бўлади.

Псевдотасодифий генераторлар ёрдамида бардошли криптотизимларни яратиш мумкин. Яхши тасодифий сон генераторлари ишлаб чиқишда мураккаб бўлиб, уларнинг ишончлилиги аппарат ва дастурий таъминотнинг афзаллигига боғлиқ бўлади. Шу сабабдан турли криптографик қарашлар асосида самарали псевдотасодифий генераторлар яратиш бўйича тадқиқотлар амалга оширилмоқда.

### 2.3. Частотавий таҳлил усули

Частотавий, яъни статистик характеристикалар усулида симметрик ёки носимметрик криптотизим криптотаҳлилчиси шифрматндаги белгилар, ҳарфлар, сўзларнинг такрорланишлари сонини (частоталарини) ҳисоблаб, очиқ матн қайси тилда ёзилганини аниқлайди. Сўнгра эса, шифрматн шифр белгилари параметрларини очиқ матн қайси тилда ёзилган бўлса, шу тилнинг параметрлари билан солиштиради. Масалан, инглиз тилида **E** ҳарфи частотаси юқори, шифрматнда **L** ҳарфи частотаси юқори. Шифрматндаги **L**

ҳарфини **E** ҳарфи билан алмаштирилади, яъни шифрматн ва очиқ матн ёзилган тил частоталарини камайиш тартибида ёзиб, тартиби тўғри келган белгилар ўзаро алмаштирилади. Кейин шифрматн биграмма, триграмма ва *k*-граммаларининг такрорланишлар сонини топиб, очиқ матн ёзилган тил биграмма, триграмма ва *k*-граммалари билан мос ҳолда алмаштиради. Биграмма, триграмма, *k*-грамма деганда, матнда иккита, учта ва *k*-та белгининг кетма-кет келиши тушунилади. Масалан, инглиз тилида **th**, **in**, **is**, **er**, **he**, **en**, биграммалари, рус тилида **ст**, **но**, **ен**, **то**, **на** биграммалари, **сто**, **ено**, **нов**, **тов**, **ова** триграммалари кўп учрайди [1, 25]. Қуйидаги 3-жадвалда [25] рус тили ҳарфларининг пайдо бўлишининг нисбий частотаси келтирилган

3-жадвал

**Рус тили ҳарфларининг пайдо бўлишининг нисбий частотаси**

| **Ҳарф** | **Частота** | **Ҳарф** | **Частота** | **Ҳарф** | **Частота** | **Ҳарф** | **Частота** |
|---|---|---|---|---|---|---|---|
| о | 0.09 | о | 0.038 | о | 0.016 | о | 0.007 |
| е,ё | 0.072 | л | 0.035 | ы | 0.016 | ш | 0.006 |
| а | 0.062 | к | 0.028 | б | 0.014 | ю | 0.006 |
| и | 0.062 | м | 0.026 | ь,ъ | 0.014 | ц | 0.004 |
| н | 0.053 | д | 0.025 | г | 0.013 | щ | 0.003 |
| т | 0.053 | п | 0.023 | ч | 0.012 | э | 0.003 |
| с | 0.045 | у | 0.021 | й | 0.01 | ф | 0.002 |
| р | 0.04 | я | 0.018 | х | 0.009 | | |

Юқорида айтиб ўтилган принциплар ҳозирги кунда кенг тарқалган паролларни танлаш бўйича дастурларда қўлланилади. Паролларни танлаш бўйича дастур аввало эҳтимоллиги катта бўлган паролларни танлайди. эҳтимоллиги кичик бўлган паролларни кейинга олиб қўяди. Бунда паролларни танлаш жараёни ўн ва юз мартталаб камаяди. Қуйидаги 4-жадвалда паролларни танлашда олинган қатор натижалар келтирилган.

4-жадвал

**Паролларни танлаш натижалари**

| Танлаш мураккаблиги | Танлаш вақти | Процессор тури |
|---|---|---|
| $2{,}08 \cdot 10^{11}$ | 15 минут | 486DX/4-100 |
| $5{,}68 \cdot 10^{10}$ | 8 соат | Pentium-120 |

### 2.4. Поллард усули

Поллард усули график шаклда "ўртада учрашиш" усулига бироз ўхшашдир. Унда "тасодифий акслантириш графида учрашиш" масаласи ечилади. Бу ерда ҳам иккита графнинг бошланғич тугунларидан чиқиб токи илдиз тугунидан ўтувчи цикл ҳосил бўлгунча қарама-қарши йўналишда ҳаракат давом этади. Учрашиш мураккаблиги $0{,}5\varphi(p/8)\#M$, якуний мураккаблик $6{,}5\varphi(p/8)\#M$.

Поллард усули циклик группада дискрет логарифм масаласини ечиш учун қисман эквивалент калитларни топишда қўлланилади. Булар бир хил хэш-функция берувчи икки аргументни топишда ҳам асқотади.

Дискрет логарифмлаш масаласига тадбиқан бу усул аввалги "ўртада учрашиш" усулига нисбатан катта хотирадан воз кечиш имконини яратади. МБни сортлаш зарурати ҳам йўқолади. Шу туфайли вақт бўйича мураккаблик *0(log#M)* марта кам бўлиб, мураккаблик $O(\varphi\#M)$ қадам, хотира ҳажми *O(1)* блокдан иборат [1, 6].

### 2.5. «Ўртада учрашиш» усули

Агар криптоалгоритмнинг махфий калитлар тўплами композиция амалига нисбатан берк бўлса, яъни ҳар қандай икки калит $z_i$ ва $z_j$ учун шундай калит $z_k$ топилсинки, ҳар қандай матни кетма-кет $z_i$ ва $z_j$ калитларида шифрлаш натижаси шу матнни $z_k$ билан шифрланган матнга айнан бўлсин, яъни

$$F(z_j, F(z_i, x))=F(z_k, x).$$

Унда бу хоссадан фойдаланиб, шифрлаш калитини топиш мумкин, яъни $z_k$ ни топиш учун эквивалент жуфтлик $< z_i, \ z_j >$ ни топиш кифоя. Бу усул "туғилган кунлар парадокси"га асосланади. Маълумки, туғилган кунлар текис тақсимланган деб ҳисобланса, 24 кишилик гуруҳда $p=0,5$ эҳтимоллик билан икки кишининг туғилган куни бир хил чиқади.

Умумий ҳолда бу парадокс қуйидагича ифодаланади: агар $a \in n$ предметлар $n$ та предмет орасидан қайтарилиш билан танланса, икки предметнинг бир хил бўлиш эҳтимоли

$$\mathrm{p} = 1 - \mathrm{e}^{-\mathrm{a}^2/2}.$$

Фараз қилинсинки, очиқ матн $x$ ва $y$ нинг шифрограммаси $y$ маълум. $x$ учун тасодифий тарзда калитлар тўплами $z_l$ ва шифрограммалар $w=F(z_l, x)$ тўпламини сақловчи маълумотлар базаси (МБ) тузамиз ва шифрограммаларни $w$ бўйича тартибга соламиз. МБ ҳажмини $0((p\#\{z\})$ га тенг қилиб оламиз.

Сўнгра тасодифан $z_{ll}$ калитни олиб, $y$ шифрматнни очамиз ва натижа $v=F(z_{ll},y)$ ни МБ билан таққослаймиз. Агар $v$ бирор $w$ билан тенг чиқса, калит $z_{ll}$ изланган калит $z$ га эквивалент.

Вақт бўйича усул мураккаблиги

$$O(\varphi\#\{z\}\log\#\{z\}).$$

Кўпайтувчи $log\#\{z\}$ саралаш мураккаблигини ҳисобга олади.

Зарур хотира $0((p\ \#\{z\}log\#\{z\})$ бит ёки $0((p\ \#\{z\})$ блокдан иборат. Блок узунлиги ва калит узунлиги чекланган доимийга фарқ қилади деб фараз қилинади.

Бу усул калитлар тўплами яримгруппа бўлган қисм тўпламни ўз ичига олган бўлса ҳам қўлланилиши мумкин. Бу усулнинг бошқа қўлланилишини тўплам яримгруппа бўлмаган ҳол учун хэш-функциялар мисолида намойиш этиш мумкин.

Масалан, ЭРИни сохталаштириш учун битта хэш-образга эга икки матн топиш лозим. Ундан сўнг имзоланган хабарни бошқа ўша хэш-образга

эга бўлган хабар билан алмаштириб қўйиш мумкин. Бундай икки хабарни топишни "ўзаро учрашиш" усулида амалга оширилса, излаш мураккаблиги

$0((p\ \#\{z\})$ бўлади.

Бунда $\#\{z\}$ мумкин бўлган хэш-образлар сони. Америкалик математик Д. Шенкс томонидан таклиф этилтан [1, 6, 25] бу алгоритм эҳтимоллик алгоритмидир.

### 2.6. Хэш-функция коллизияси усули

Криптографияда хэш-функциялар қуйидаги масалаларни ҳал қилиш учун ишлатилади:

- маълумотни узатишда ёки сақлашда унинг тўлалигини назорат қилиш учун;

- маълумотнинг манбасини аутентификация қилиш учун.

Маълумотни узатишда ёки сақлашда унинг тўлалигини назорат қилиш учун ҳар бир маълумотнинг хэш-қиймати ҳисобланади ва бу қиймат маълумот билан бирга сақланади ёки узатилади. Маълумотни қабул қилган фойдаланувчи маълумотнинг хэш-қийматини ҳисоблайди ва мавжуд бўлган назорат қиймати билан солиштиради. Агар таққослашда бу қийматлар мос келмаса, маълумот ўзгарганлигини билдиради.

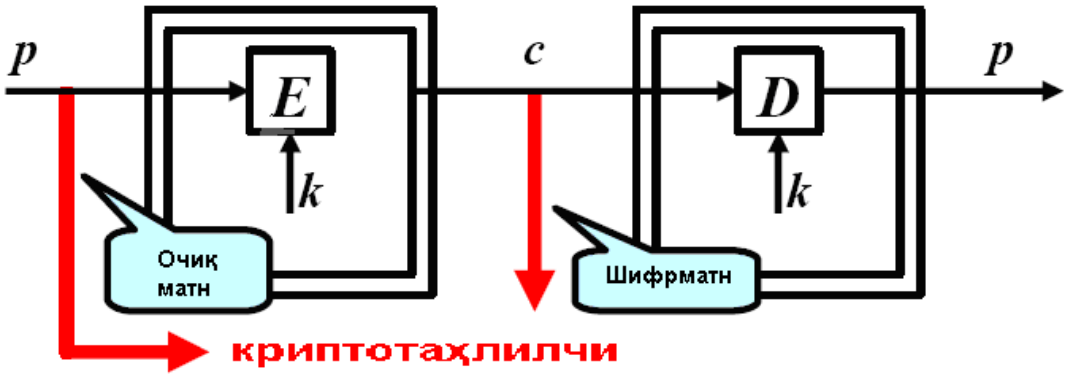
Хэш-функцияларга қилинадиган асосий ҳужум бу коллизияни ҳосил қилишдир. Қўлга тушган $x$ ва $y\neq x$ матнлар учун $H(x)\neq H(y)$ бўлиши - коллизияга бардошлилик хоссасидир.

“Туғилган кун парадокси”га асосланган криптоҳужум хэш-функцияларда коллизияларни топиш учун ишлатиладиган асосий криптоҳужумлардан биридир. Бу криптоҳужумга асосан хэш-қиймат берилганда унга мос бўлган маълумотни танлашнинг мураккаблиги $O(2^n)$ катталик билан, маълумот ва унинг хэш-қиймати берилганда, хэш-қиймати шунга тенг бўладиган бошқа маълумотни танлашнинг мураккаблиги $O(2^{n/2})$ катталик билан баҳоланади [1, 6, 25]. $H(x)=H(y)$ кўринишдаги иккита

маълумотни “ўртада учрашиш” ёки Поллард усулидан фойдаланиб топиш мумкин.

### 2.7. Қўшимча каналлардан фойдаланишга асосланган криптотаҳлил усуллари

Бошқа томонлар ва қўшимча каналлар орқали ҳужум – бу криптографик ҳужум тури бўлиб бошқа томонлар ва қўшимча каналлардан олинган ахборотлардан фойдаланишга асосланган [1, 25]. Қўшимча каналлардан олинган ахборот деганда шифрлаш қурилмасидан олиниши мумкин бўлган ахборот тушунилади, бунда у очиқ ёки шифрматн ҳисобланмайди (2-расм).




2-расм. Қўшимча каналлар орқали ҳужум

Қўшимча каналлар орқали ҳужум қуйидаги уч тур буйича таснифланади.

- ҳисоблаш жараёнини назорат қилиш бўйича: фаол ва суст;

- модулдан фойдаланиш усули бўйича: агрессив, ярим агрессив ва ноагрессив;

- таҳлил жараёнида қўлланиладиган услуб бўйича: оддий ва турлича.

Қўшимча каналлар орқали қилинадиган ҳужумларда криптографик алгоритм ва протоколларни реализация қилишда олинган ахборотлардан фойдаланилади. Бу маълумотлар вақт ўлчови бўйича, қувват ёки электромагнит нурланиш сарфи бўйича бўлиши мумкин. Қўшимча

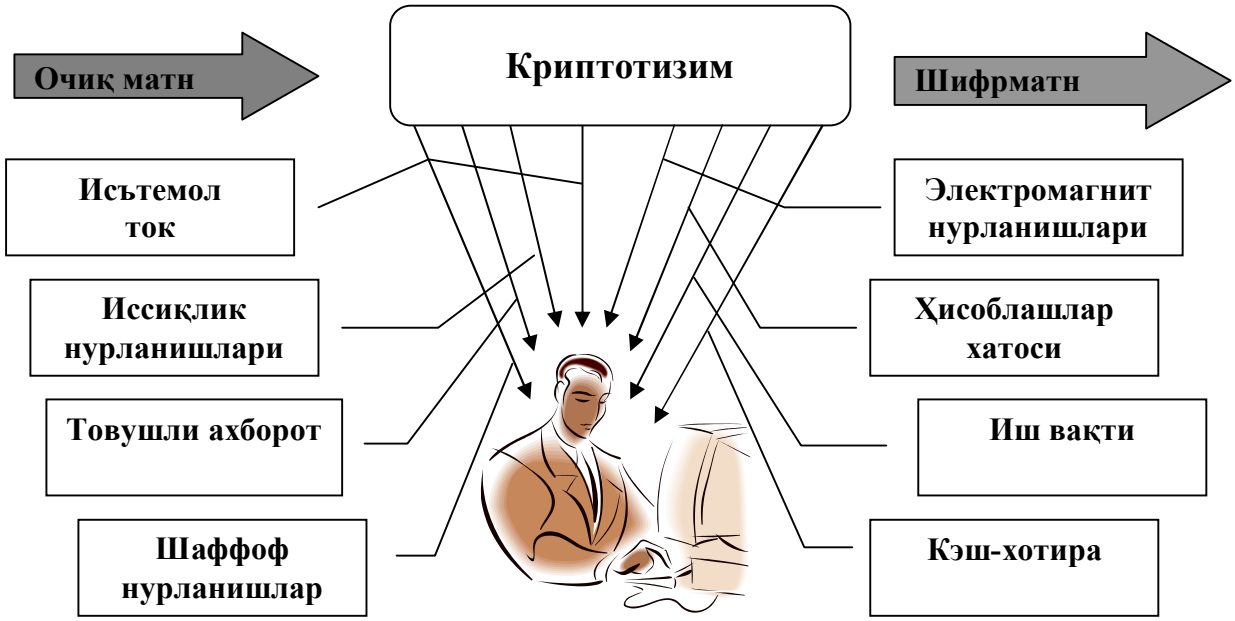
каналлардан олинадиган ахборотларнинг бошқа шакли сифатида дастурий ёки аппарат хатоларини ҳисоблаш натижалари бўлиши мумкин.

Бундан криптографик алгоритмларни дастурий ёки аппаратли реализациясини аниқ амалга ошириш хавфсизлик учун жуда муҳимлиги келиб чиқади. Кичкина бир хатолик хавфсизликда катта фарқни келтириб чиқаради.

Ҳозирги кунда ўндан ошиқ қўшимча каналлар фарқланади [25]. Қуйидаги 3-расмда баъзи қўшимча каналлар келтирилган.

Ҳужумлар фойдаланиладиган қўшимча каналлар кўринишига қараб ажратилади. Қуйида қўшимча каналлар орқали қилинадиган машҳур ҳужумларни санаб ўтамиз.

1. Вақт бўйича ҳужум.
2. Қувват бўйича оддий ҳужум.
3. Қувватлар фарқи бўйича ҳужум.
4. Ҳисоблашлар хатоси бўйича ҳужум.
5. Электромагнит нурланишлар бўйича ҳужум.
6. Шаффоф нурланишлар бўйича ҳужум.
7. Акустик ҳужум.
8. Кэшга ҳужум.




3-расм. Қўшимча каналлар

Қўшимча каналлар орқали қилинган *вақт бўйича ҳужум* даставвал фуқаролар уруши даврида пайдо бўлган. Криптографик алгоритмларни амалга оширишдаги ҳисоблашлар турли вақт оралиқларида бажарилади. Бу вақт ичида махфий параметрлар ҳақида баъзи ахборотларга эга бўлиш мумкин ва агар ҳужумни аниқ амалга ошириш бўйича етарли билимга эга бўлса, унда статистик таҳлил мазкур махфий параметрларни тўлиқ тиклаши мумкин бўлади. Вақт бўйича ҳужум шифрлаш жараёнини бажариш учун зарур бўлган шифрлаш модулини топиш вақтини аниқ ўлчашга асосланган. Бу ахборот махфий калитни очиш имконини беради [1, 25, 27].

*Қувват бўйича ҳужум*дан, асосан, криптотизимлар аппарат кўринишда амалга оширилганда, фойдаланилади. Қувват бўйича ҳужум айниқса махфий калит сақланадиган смарт-карта ва бошқа тизимларга ҳужумда муваффақиятли бўлади. Қувватлар фарқи бўйича ҳужум эса истеъмол қилинадиган қувватни таҳлил этиш натижасида амалга оширилади. Смарт-карталарга қувват бўйича оддий ҳужум одатда бир неча секундни,

қувватлар фарқи бўйича ҳужум эса бир неча соатни талаб этади. Қувватлар фарқи бўйича ҳужум энг кам сарфни талаб этади.

*Ҳисоблашлар хатоси бўйича ҳужум* аппарат таъминотидаги тасодифий хатоликларга қаратилган бўлиб, унинг хавфсизлигига жиддий таъсир кўрсатади. Бу хатоликлар ёки хато чиқиш маълумотларининг муҳим қўшимча каналга айланишини, ҳатто баъзида криптотаҳлил учун шифрнинг заифлигини сезиларли ошириб юборади.

Ҳисоблаш амалларини компьютерларда амалга ошириш электромагнит нурланишларни юзага келтиради. Бу нурланишларни ўлчаш ва таҳлиллаш натижасида криптотаҳлилчи бажарилаётган ҳисоблашлар ва фойдаланилаётган маълумотлар тўғрисида аҳамиятга молик ахборотга эга бўлади. *Электромагнит нурланишлар бўйича ҳужум* билан бирга шаффоф нурланишлар бўйича ҳужумдан ҳам фойдаланилади. Бунда компьютер мониторидан чиққан нурланишнинг девордаги акси чиқиш сигналларини тиклашга ёрдам бериши мумкин. Бу ҳужумнинг афзаллиги шундаки, бунда қурилмадан фойдаланиш талаб этилмайди [1, 25, 27].

Ҳозирги вақтда қўшимча каналларни тадқиқ этиш асосан энергия истеъмолини таҳлил этиш бўйича ҳужумга йўналтирилган бўлса ҳам, *акустик ҳужум* хавфи мавжуддир. Процессорнинг товуши билан унда бажариладиган ҳисоблашлар орасида боғлиқлиқ борлигини криптотаҳлилчи Шамир исботлаб берган.

Агар процессор кэш-хотирада сақланмаётган маълумотлардан фойдаланишни амалга оширса, зарурий маълумотлар кэш-хотирадаги асосий хотирадан юкланмагунча ҳисоблашларда қандайдир тўхтаб қолиш содир бўлади. Бундай тўхтаб қолиш бузғунчи учун кэш-хотирани тўлиш частотасини аниқлаш имконини беради. Худди шу ердан қўшимча каналга ахборот сизиб чиқиши юзага келади.

Кейинги бўлимда тўлиқ ошкор этиш синфига мансуб факторлаш, ё дискрет логарифмлаш ва ЭЭЧда дискрет логарифмлаш каби мураккаб муаммоларни ечишга йўналтирилган тажовузларга ошкора калитли

криптотизим алгоритмларининг криптотаҳлиллаш усуллари ҳамда RSA криптотизими протоколининг заиф томонларидан фойдаланиб ҳужум уюштириш сценарийлари баён этилган.

## Назорат саволлари

1. Криптотизимларни криптотаҳлиллашнинг универсал усуллари қаторига самарали натижа бераётган қайси усулларни кирита оласиз?

2. Тўлиқ танлаш, частотавий таҳлил, ўртада учрашиш, Поллард криптотаҳлил усулларидан ҳар бирининг моҳиятини ўхшаш ва фарқли томонларини тушунтиринг?

3. Калит бўйича ҳужум ва хэш-функция коллизияси усулларини ҳамда қўшимча каналлардан фойдаланишга асосланган криптотаҳлил усулларидан ҳар бирининг моҳиятини ўхшаш ва фарқли томонларини тушунтиринг?

4. Қўшимча каналлар орқали қилинадиган ҳужумлардан вақт, қувват, қувватлар фарқи ва ҳисоблашлар хатоси бўйича ҳужумларнинг моҳияти ва уларнинг юзага келиш сабабларини тушунтиринг?

5. Қўшимча каналлар орқали қилинадиган ҳужумлардан электромагнит нурланишлар, шаффоф нурланишлар, акустик ҳужумлар ва кэшга ҳужумларнинг моҳияти ва уларнинг юзага келиш сабабларини тушунтиринг?

# 3. НОСИММЕТРИК КРИПТОТИЗИМЛАРНИ КРИПТОТАҲЛИЛЛАШ УСУЛЛАРИ

Маълумки, энг кўп фойдаланиб келинган носимметрик тизимларга бардошлилиги учта муаммонинг, яъни факторлаш, дискрет логарифмлаш ва ЭЭЧ группасида дискрет логарифмлаш мураккаблиги муаммоларидан бири билан белгиланадиган криптотизимлар киради. Булар билан бир қаторда қўшимча махфийликка эга бўлган носимметрик криптотизимлар ҳам юзага келмоқда. Улар криптотизим яратувчи криптографлар учун ҳам, криптотизимни қўпоришни ёки ҳужум учун бардошлиликни баҳолашни мақсад қилган субъектларга криптотаҳлил объекти бўлиб хизмат қилади.

## 3.1. Дискрет логарифмлаш муаммосининг мураккаблигига асосланган носимметрик криптотизимлар криптотаҳлили

Дискрет логарифмлаш усуллари ва кейинги параграфда кўриладиган факторлаш усуллари орасида параллеллик - ўзига хос изоморфизм мавжуд. Масалан, Диксон алгоритми билан индексли ҳисоблаш алгоритмлари бир-бирига жуда ўхшаш, иккала алгоритмда ҳам тенгламалар системасини тузиш ва чизиқли алгебрадан фойдаланиш босқичлари ўхшаш. Лекин, дискрет логарифмлаш муаммоси факторлаш муаммосига нисбатан мураккаброқдир. Агар дискрет логарифмлашнинг полиномиал алгоритми яратилса, унда факторлаш муаммоси ҳам осон ҳал бўлади.

Ҳозирги кунда энг самарали ҳисобланган криптотаҳлил алгоритмлари субэкспоненциал мураккабликка эгадир. Бу алгоритмлар “index-calculus” (индексли ҳисоблаш) алгоритмлари бўлиб, фактор базасини қуришга асосланган.

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 [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 $c\approx 1,92$ [1, 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

$$\sum^m_{i=1} log_a x_i \equiv \sum^m_{j=1} log_a y_j\ mod\ (p-1).$$

Охирги таққосламалардан бир қанчасини ҳосил қилингач, $log_a x_i$ ва $log_a y_j$ 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 $log_a g$ 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.

## 3.2. 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 [1, 31].

Факторлаш муаммосини ҳал этишга бағишланган адабиётлар [1, 30, 32] 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 $r$ -, $\lambda$ - усули номлари остида такомиллаштирилди. $r$ - $\lambda$ - 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 [1, 25, 31].

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 [1].

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.

Ўқув қўлланманинг 1-иловасида ўқув машғулотларида фойдаланиш учун *(p-1)* Поллард, *(p+1)* Вильямс ва Ленстра алгоритмлари мажмуасига

асосланган Си тилидаги дастури келтирилган. Дастур MIRACL математик библиотекаси асосида шакллантирилган.

Ўқув қўлланманинг 2-иловасида шахсий компьютер факторлаган RSA модуллари ва факторлашга кетган вақт сарфлари келтирилган.

Факторлашга оид мисоллар математик библиотека MIRACL ўрнатилган қуйида келтирилган конфигурацияга эга бўлган шахсий компьютерда 1-иловада келтирилган дастур асосида ҳисобланган.

Фойдаланилган шахсий компьютер конфигурацияси қуйидагича:

Операцион тизим: Microsoft Windows XP Professional Service Pack 3 [version 1.5 May 2008], Процессор: Intel™ Core™2 Duo CPU E4600 @ 2.40GHz, ОЗУ: 1 ГБ.

Қуйида субэкспоненциал алгоритмлар синфига оид Диксон, квадратик ғалвир ва сонли майдон ғалвир усулларининг асослари билан танишилади.

### 3.2.1. Диксон усули

Фараз қилинсинки, $n$ ни факторлаш лозим бўлсин. Агар Лежандр эътибор қаратган $x^2 \equiv y^2 \pmod n$ таққосламани, яъни $n$ га каррали бўлган, $x$ ва $y$ $k \neq 0$ учун $x^2 - y^2 = kn$, унда $(x-y)(x+y)=kn$ бўлади. Агар кичик эҳтимоллик билан $x-y=k$ ва $x+y=n$ ҳосил қилинса, камида ½ эҳтимоллик билан $n$ ни факторлаш мумкин бўлади. Агар $EKUB(n, x-y)$ ва $EKUB(n, x+y)$ бўлса, унда булар $n$ нинг фош этилган факторлари бўлади [1].

Масалан, $100=9 \pmod{91}$, унда $10^2=3^2 \pmod{91}$,

$(10-3)(10+3) = (7)(13) =0 \pmod{91}$, демак, $7*13=91$.

Умумий ҳолда факторлар $EKUB(n, x-y)$ ва $EKUB(n, x+y)$ ларни ҳисоблаш орқали топилади. $EKUB$ дан фойдаланиш зарурлигини кўриш учун фараз қилинсинки, $x=34$, $y=8$, булар $34^2=8^2 \pmod{91}$ таққосламани қаноатлантиради, чунки $34^2 \pmod{91}=64$ дир. Бу мисолда $x-y=26$ ва $x+y=42$, бинобарин, $EKUB(91,26)=13$, $EKUB(91,42)=7$.

EKUB $O(\log a)^2$ дан кичик мураккабликка эга бўлган Евклид алгоритми асосида осон ҳисобланади, аммо $x^2 \equiv y^2 \pmod n$ таққосламани қаноатлантирувчи ўзгарувчилар жуфтини топиш мураккаб масаладир. Бу масалани ечишни осонлаштириш учун таққосламани қаноатлантириш шартларини бироз ўзгартириш кифоя.

Масалан, $41^2=32 \pmod{1649}$ ва $43^2=200 \pmod{1649}$ бўлсин, бу ерда $32$ ҳам, $200$ ҳам квадратик чегирма эмас.

Бироқ, иккала тенгламадан кутилган таққослама $(41*43)^2=80^2 \pmod{1649}$ берувчи $41^2 43^2=32*200=6400 \pmod{1649}$ топилади.

Бу масалани ечиш учун фойдаланиладиган субэкспоненциал мураккабликка эга бўлган алгоритмларда силлиқлик хусусиятига эга бўлган сонлардан фойдаланилади. Алгоритмлар мураккаблиги бу хусусиятдан фойдаланишга бўлган ёндашув билан фарқланади.

Факторлаш масаласини ечишда икки босқичда ҳисоблашлар амалга оширилади:

- биринчи, тайёрланиш босқичида бирор чегара B танланади ва фактор базаси ҳамда бу база асосида тенгламалар системаси шакллантирилади. Фактор базаси деганда $2 \le p_i \le L^n$ шартини қаноатлантирувчи $k$ та туб сон $p_i$ тушунилади, бу ерда $L=e^{\sqrt{\log n \log\log n}}$ ва базанинг $m^2 \pmod n$ синфида энг кичик номанфий чегирмаси $Q(m)$ билан белгиланади;

- иккинчи босқичда тенгламалар системасининг ечими топилади.

Одатда бошланғич ҳисоблашлар бир марта амалга оширилади, сўнгра факторлар топилади. Шундай қилиб, факторлаш тенгламалар системасини ечишга ўтилади.

Алгоритмнинг биринчи босқичини амалга оширишда, фактор базасини шакллантиришда $1<m_i<n$ шартини қаноатлантирувчи $m_1 \dots m_{k+1}$ сонлар тасодифий тарзда изланади ва $Q(m_i)=p_i^{\alpha I,1} \dots p_k^{\alpha I,k}$ $(i=1,\underline{k+1})$ кўринишдаги сонлар шакллантирилади. Бу ерда $m_i^2 = Q(m_i) \pmod n$ *силлиқ* сонлар (B-силлиқлик муносабати билан боғланган сонлар)дир, чунки улар унча катта бўлмаган туб сонларнинг кўпайтмаси сифатида ифодаланади.

$Q(m_i)$ кўрсаткичлари векторини $v_i\uparrow=(\alpha_{I,1}\dots\alpha_{I,k})\in Z^k$ билан белгиланади, бу ерда $Z^k$ – $k$ узунликка эга бўлган вектор фазоси.

$k$ ўлчамли Буль фазоси $Z^k_2$ да $x_1 v_i\uparrow+\dots+ x_1 v_i\uparrow\equiv 0\uparrow$ $(mod\ 2)$ кўринишдаги тенгламалар системасини ечиб, $x_{1\dots} x_{k+1}\in\{0.1\}$ топилади, бу ерда $x_{1\dots} x_{k+1}$ вектори нолга тенг вектордан фарқли. Бундай ечим мавжуд, чунки тенгламалар сони номаълумлар сонидан кичик.

Ҳисобланган қийматлар $x_{1\dots} x_{k+1}$ учун, қуйидаги таққослама ўринлидир:

$$(m_1^{x1} *** m_1^{xk+1})^2\equiv p_1^{c1} *** p_k^{ck}\ (mod\ n),$$

бу ерда $c_1=\sum^{k+1}_{i=1}x_i\alpha_{i,1}$, $c_k=\sum^{k+1}_{i=1}x_i\alpha_{i,k}$,

$X=m_1^{x1} *** m_1^{xk+1}$, $Y=\prod^{k}_{j=1} p_j^{ck/2}$, $c_k$ - $x_i$ таърифга кўра бутун сон.

Натижада $X^2\equiv Y^2(mod\ n)$ таққосламасига эга бўлинади. Сўнгра $1<EKUB\ (X\pm Y,n)<n$ текширилади, шарт бажарилса факторлар топилган бўлади, акс ҳолда алгоритм бошига қайтилади ва токи қониқарли ечим топилмагунча, бошқа $m_i$ лар билан юқоридаги амаллар бажарилади.

### 3.2.2. Квадратик ғалвир усули асослари

Факторлашнинг квадратик ғалвир усули Диксон усулига жуда ўхшаш. Иккала алгоритмда ҳам чизиқли алгебра асосларидан бир хил тарзда фойдаланилган. Яъни, аввало чегара $B$ танланади ва $B$ дан катта бўлмаган туб сонлардан фактор базаси шакллантирилади. Шаклланган база етарли миқдорда $B$-силлиқ сонларни ўз ичига олиши шарт [1].

Кейин кўпҳад $Q(x)=(\lfloor\sqrt{n}\rfloor+x)^2+n$ аниқланади. Бу кўпҳад квадратик бўлиб, база элементларини $B$-силлиққа текшириш учун фойдаланилади. Усул номида “квадратик” атамаси қатнашиши кўпҳад квадратик бўлганидан келиб чиққан.

Силлиқлик муносабатига эга бўлган сонларни танлаш учун $0$ сонини ўз ичига олган интервал, масалан, $[-M;\ M]$ дан ҳар бир бутун сон $x\in[-M;M]$ учун $y=Q(x)$ ҳисобланади. Сўнгра $n$ модуль бўйича $y=\underline{x}^2$

ҳисобланади, бу ерда $\underline{x}=\lfloor\sqrt{n}\rfloor+x$ . Натижада Диксон алгоритмидаги каби $y$ $B$-силлиқми ёки йўқлиги аниқланади. Агар $y$ силлиқ бўлса, унда чизиқли тенгламалар системасини ечиш босқичи учун *2* модуль бўйича экспонента сифатида сақлаб қўйилади. Квадратик ғалвир усулининг Диксон усулига нисбатан устунлиги [1, 33] да баён этилган ғалвир тузиш усули билан белгиланади. Ғалвир тузиш фактор базасини шакллантириш ишини осонлаштиради.

Қуйида квадратик ғалвир усулининг 1991 йилда таклиф этилган такомиллаштирилган Померанц усулининг асосий ғояси ҳақида тўхталамиз.

Фактор базаси сифатида қандайдир параметр билан чекланган $s$ та шундай туб сон $p_i$ лар танланадики, $(n/p_i)=1$ бўлсин, бу ерда $(n/p_i)$ Якоби белгиси.

$m=\lfloor\sqrt{n}\rfloor$, $Q(t)=(t+m)^2-n=H(t)^2$, бу ерда $H=t+\lfloor\sqrt{n}\rfloor$. $t$ нинг деярли кичик қийматларида $Q(t)$ нинг қиймати ҳам катта бўлмайди. Кейинги қадамда, $t$ сонларини кўриб чиқиш ва $Q(t)$ ларни кўпайтувчиларга ажратиш ўрнига, алгоритм биратўла "кераксиз" $t$ ларни чиқариб ташлайди ва фактор базаси орасида фақат $Q(t)$ нинг бўлувчилари мавжуд бўлганларини қолдиради, яъни

$$A=Q(t)=\prod_{j=1}^{s} p_j^{\gamma_j},$$

$Q(t)$ фактор базасида ажратилади. Унда $B=H(t)$ белгилаш орқали $B^2 \equiv A^2 \pmod n$ таққосламага эга бўлинади ва бундай таққосламаларни тўплаб, ўзгарувчиларни сафдан чиқариш орқали Диксон алгоритмидагидек $X^2 \equiv Y^2 \pmod n$ таққосламасига эга бўлинади, оқибатда факторлар топилади.

Бугунги кунда сонли майдон ғалвири усули ва Померанцнинг такомиллашган квадратик ғалвир усули энг тезкор усуллардир.

### 3.2.3. Сонли майдон ғалвири усули асослари

Дастлабки Поллард тезкор факторлаш усули [1] томонидан таклиф этилган бўлиб, махсус кўринишдаги сонларни (масалан, Ферма

сонларини) факторлаш (SNFS) учун мўлжалланган. SNFS усулида энг катта факторланган натурал сон *227* ўнли хонали рақамларда берилган сондир. Аммо RSA-модуллари махсус кўринишга эга бўлмаганлиги боис, уларни умумлашган сонли майдон ғалвири (GNFS) усули асосида факторлаш мумкин. Ҳозиргача эришилган рекорд натижалар *155* ўнли хонали (*512* бит) сонлар учун эришилган. Бу сонни факторлаш учун *8400 mips-йил* сарф бўлган [29, 33].

Ҳозирги кунда сонли майдон ғалвири усули асосида *110* ва ундан ортиқ ўнли хонали узунликдаги модулларни факторлаш учун энг тезкор алгоритмлар ишлаб чиқилган. Квадратик ғалвир усули нисбатан тўппа-тўғри мақсадга элтишга етарли бўлса ҳам, сонли майдон ғалвири усули такомиллашган математик асосларга таяниши билан истиқболлироқдир. Тушунишга қулай бўлган сонли майдон ғалвири усулининг баёни [29, 33] да келтирилган. Сонли майдон ғалвири  ўз моҳияти бўйича алгоритм эмас, балки бир неча босқичдан таркиб топган алгоритмлар мажмуасидир [1, 29-30].

Квадратик ғалвир алгоритмининг мураккаблиги $C_1=O(\exp( (\ln p)^{1/2} (\ln \ln p)^{1/2}))$ амал билан баҳоланса, сонли майдон ғалвири усулининг мураккаблиги $C_2=O(\exp(c(\ln p)^{1/3} (\ln \ln p)^{2/3}))$ амал билан баҳоланади, бу ерда $c\approx1,9223$. Сўнги ифодада $(\ln p)^{1/2}$ ҳади $(\ln p)^{1/3}$ га айланган, аммо $C_2$ да нисбатан катта $c$ нинг қатнашиши квадратик ғалвир алгоритми узунлиги *110* ўнли хонали бўлган модуллар қулайлигига сабаб бўлади [1, 29].

$n$ нинг бинар узунлиги $x=\log n$ га тенг олиниши келтирилган усул мураккаблилигини симметрик криптотизимлар калит узунлиги бўйича мураккаблиги билан таққослаш имконини беради.

Қуйида келтирилган 5-жадвалнинг биринчи устунида усуллар, иккинчи устунида факторлаш учун амаллар сарфи $f(x)$, учинчи устунида $\log_2 f(x)$ келтирилган.

5-жадвал

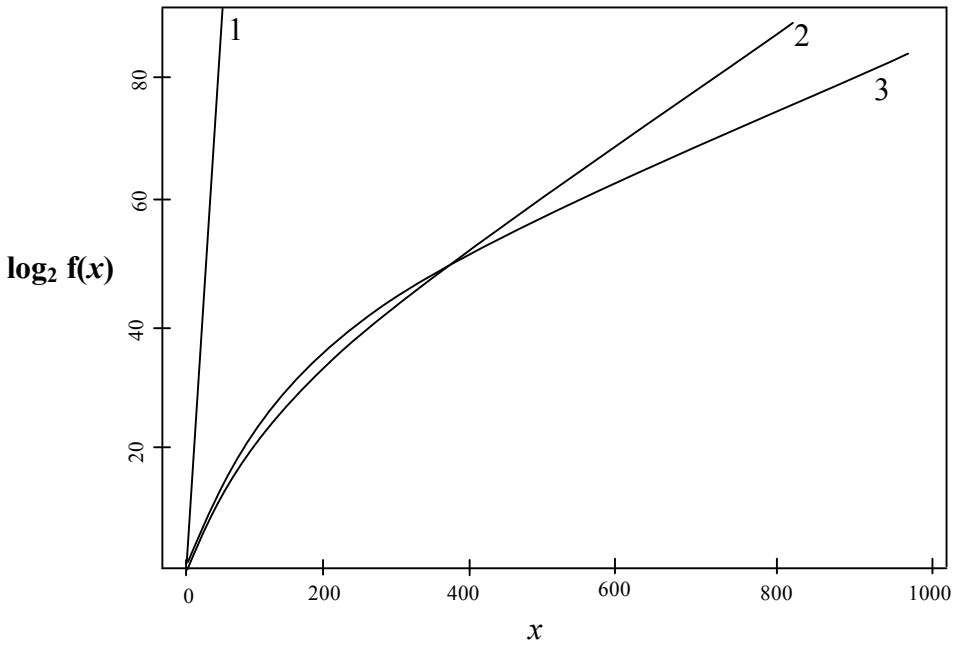
**Усуллар мураккаблиги**

| Усуллар | $f(x)$ | $\log_2 f(x)$ |
|---|---|---|
| Танлаб бўлиш | $2^x/x$ | $x - \log_2 x$ |
| Квадратик ғалвир | $2^c (\log_2 x)^{1/2}$, бу ерда $c=x^{1/2}$ | $x^{1/2} (\log_2 x)^{1/2}$ |
| Сонли майдон ғалвири | $2^{1.9223d} (\log_2 x)^{2/3}$, бу ерда $d=x^{1/3}$ | $1.9223\, x^{1/3} (\log_2 x)^{2/3}$ |

Келтирилган жадвалдан субэкспоненциал мураккабликка эга бўлган квадратик ғалвир ва сонли майдон ғалвири усуллари асимптотик мураккаблик нуқтаи назаридан экспоненциал мураккабликка эга бўлган алгоритмлардан устунлиги билан белгиланиши, бироқ полиномиал мураккабликка эга алгоритмлар билан рақобатлаша олмаслиги аён бўлади.

4-расмда танлаб бўлиш (1), квадратик ғалвир (2) ва сонли майдон ғалвири (3) усуллари бўйича тузилган алгоритмлар мураккабликларининг *x,* яъни модуль бинар узунлигига нисбатан ўзгариш графиги келтирилган.

Шуни қайд этиш лозимки, квадратик ғалвир усули сонли майдон ғалвири усулидан *390* битли модулларни факторлашда мураккаблик бўйича устунликка эга. Шунингдек, 4-расм асосида симметрик алгоритмлар шифрлаш калити узунлигига мос факторлаш мураккаблигини берувчи RSA алгоритми модулининг битлар сонини аниқлаш мумкин. Масалан, *390* битли RSA-модулни факторлаш *60* битли симметрик тизим шифрлаш калитини топиш мураккаблигига тенг [1, 29-30].




4-расм. Факторлаш алгоритмлари мураккабликларини таққослаш

Бу усул барча ҳозиргача маълум бўлган бошқа криптотаҳлил усулларини сиқиб чиқарган. NFC усули асосида криптотаҳлил учун зарур амаллар бажариш вақти қуйидаги ифода бўйича аниқланади:

$T = e^c$,

бу ерда

$C=((1.923+O(1)*(Ln(n))^{1/3}*(Ln(Ln(n)))^{2/3}$.

Ҳисоблашлар тезлиги $10^6$ бўлган компьютердан фойдаланиб амалга оширилганда $C$ ифодасида $O(1)=1$ учун амаллар бажариш вақти $1$ *мс* га тенг. NFC усулининг истиқболдаги тараққиёти $1.923$ доимийсини камайиши йўналишида юз бериши башорат қилинган. Кўпгина махсус тузилмали сонлар, масалан, Ферма сонлари учун доимий $1.5$ гача камайиши маълум. Ҳозирги кунда қўлланиладиган факторлаш қийин бўлган модуллар криптоалгоритм яратиш жараёнида аниқ белгилаб қўйилган талабларга жавоб бериши шарт. Бу талаблар жумласига махфий даража кўрсаткичи $d$ нинг катта сон бўлиши, ошкора калит қисми $e > 3$ шартига жавоб бериши, махфий туб модуллар учун $p-1$ ва $q-1$ ларнинг факторлари катта туб сон бўлиши ва шунга ўхшаш. Агар бундай модуллар учун ҳам доимийни $1.5$ га

камайтириш йўли топилса, унда *1024* битли сонларни ҳам мавжуд ҳисоблаш техникаси даражасида факторлаш мумкин бўлар эди. Доимийни камайтириш усулларидан бири бўлиб кўпҳад кўринишидаги сонларни кичик коэффициентлар орқали ифодалаш усулини топиш ҳисобланади. Ҳозирча адабиётларда бундай усул мавжудлиги ҳақида ахборот берилмаган.

### 3.3. Эллиптик эгри чизиқ группасида дискрет логарифмлаш масаласининг мураккаблигига асосланган тизимларнинг криптотаҳлил усуллари

ЭЭЧда нуқталарни қўшиш амали аниқланган [1, 34-39]. *E(K)* ЭЭЧ нуқталар тўплами нуқталарни қўшиш амалига нисбатан чекли коммутатив (Абель) группасини ҳосил қилади.

*Таъриф*. *({O,(x,y)∈E(K)}; "+")* жуфтлиги кўринишидаги алгебраик структурани ЭЭЧ нуқталари группаси деб аталади.

ЭЭЧга асосланган кўпчилик криптографик алгоритмларнинг бардошлилиги ЭЭЧда дискрет логарифмлаш масаласини ечиш мураккаблиги (ECDLP) билан белгиланади.

Бугунги кунда ECDLP масаласини ечишнинг энг яхши алгоритми, ЭЭЧда нуқталарни $\sqrt{\pi n/2}$ тартибли қўшишни талаб этувчи Поллардниг $\rho$-усулидир.

ЭЭЧ нуқталари тартиби ЭРИ бардошлилигини белгилаб берувчи муҳим параметрларидан биридир. *F(q)* чекли майдонда ЭЭЧ тартиби *#E(F(q))* деб белгиланувчи *E(F(q))* нуқталар сонига айтилади. Модомики Вейерштрасс тенгламаси барча $x \in F(q)$ учун иккидан ортиқ ечимга эга эмас экан, $\#E(F(q)) \in [1,\ 2q+1]$ бўлади. Тартиб қиймати интервали чегараси машҳур Хассе теоремасига [1, 39-41] мувофиқ қуйидагича аниқланади:

$$q+1-2\sqrt{q} \le \#E(F(q)) \le q+1+2\sqrt{q}.$$

Криптографик алгоритмларга бўладиган барча маълум ҳужумларга қаршилик қилиш учун криптотизим параметрлари қуйидаги шартларни қаноатлантириши шарт:

- $q$ тартиб катта туб сонга тенг ёки $2$ нинг катта даражаси шаклида бўлиши;

- ЭЭЧ нуқталари сони $\#E(K) = nh$, бу ерда туб сон $n > 2^{160}$ , $h \le 8$, $\#E(K) \neq q$;

- $n$ барча $1 \le k \le B$ учун $q^k - 1$ га бўлинмаслиги шарт.

Одатда амалиётда ANSI X9.62-1998 [42] да тавсия қилинганидек $B \ge 20$, танланади. ГОСТ Р 34.10-2001да $B$ сон $B \ge 31$ тенгсизликни қаноатлантиради, Германия Федератив Республикаси стандартида [34, 43] $B$ учун қуйи чегара қилиб $B \ge 10^4$ танланган.

[20] да белгиланганидек [41] интернет саҳифаларида EC-DSA-2000 даги мавжуд хатоликлар туфайли имзоланган ҳужжатни алмаштириб қўйиш эҳтимоллиги баён этилган. А.В. Кобец фикрича бу хатоликни, ЭЭЧ $x$ координатасининг қарама-қарши нуқтаси билан тенглиги $G_x == -G_x$ келтириб чиқаради ва қуйидаги айнанликка олиб келади:

$$r_1 = [k]G == r_2 = [(q-1)k]G == r.$$

Агар криптотаҳлилчига ҳар хил ҳужжатларнинг $e_1$ ва $e_2$ хэш-қийматлари учун ЭРИни ҳисоблаш (танлаб олиш) зарур бўлса, у ҳолда иккала тенгламанинг тенглигидан $s$ компонента учун, у асосида ҳар хил ҳужжат учун бир хил ЭРИни шакллантирувчи шахсий калит $d$ ни аниқлашнинг ўзи етарлидир. Лекин бу хатоликни тузатиш мураккаб эмас. Масалан, шахсий калит далилий генерациясини етарли даражада таъминлаш етарлидир.

Турли хилдаги ҳужумларга бардошли, махсус ишлаб чиқилган ЭРИни шакллантириш ва текшириш алгоритми схемалари катта қизиқиш уйғотади. Бундай алгоритмлар гуруҳига ЭЭЧда ЭРИ халқаро стандарти даражасидаги Германия ва Корея миллий алгоритмларини киритишимиз мумкин.

ЭРИ алгоритми маълум турдаги ҳужумларга етарли даражада бардошлиликка эга бўлмоғи лозим. Ҳар қандай ҳужум аниқ мақсадга етиш учун йўналтирилади. Шуни ҳисобга олган ҳолда ЭЭЧдаги ЭРИ схемаларига бўлган хавфларни хатарлилиги ошиб бориш тартибида қуйидаги турларга ажратиш мумкин [1]:

- бадният криптотаҳлилчининг қўлга киритганидан фарқланадиган, баъзи маъносиз маълумотлар учун ЭРИ ҳосил қилишига олиб келувчи экзистенциал сохталаштириш;

- олдиндан танланган маълумот учун ЭРИни яратишга олиб келувчи селектив сохталаштириш;

- фойдаланилаётганига функционал эквивалент бўлувчи самарали ЭРИ алгоритмини яратиш билан тугалланувчи универсал сохталаштириш;

- очиқ калитга мос ЭРИ эгасининг шахсий калитидан фарқли бўлиши мумкин бўлган махфий калитни ҳисоблаб топувчи тўлиқ очиш.

Ҳужумлардан энг кучлисига асосланган энг кучсиз таҳдидга бардошлиси ЭРИ алгоритмларининг энг ишончли схемаси ҳисобланади, яъни имзоланган маълумотларни танлаб олишли ҳужумга асосланган экзистенциал сохталаштиришга [1].

Тизимли параметрлар Полиг-Хеллман, Шенкснинг “кичкина ва катта қадамлар” $\rho$-Поллард мураккаб логарифми, индексни ҳисоблаб топишга ва шу каби бошқа ҳужумларга бардошлиликни таъминлаши лозим.

Полиг-Хеллман алгоритми асосида базавий (генератор) нуқталар тартиби факторлаш масаласи ётади. Алгоритм факторлаш натижасида ҳар бир модуль бўйича олинган дискрет логарифм ечими эвазига калитни топиш мураккаблигини пасайтиради. Калитни топишда қолдиқни топиш ҳақидаги хитойча теоремадан фойдаланилади.

“Кичкина ва катта қадамлар” алгоритми тезкорлик ва хотирадан фойдаланиш ўртасидаги ўзаро мосликни таъминлайди [1, 44].

ЭЭЧда дискрет логарифмлаш масаласини ечишниг маълум

усулларидан энг машҳури Поллардннинг $\rho$- ва $\lambda$- усулларидир [1, 45]. ЭЭЧ нуқталарини қўшиш билан аниқланувчи Поллардннинг $\rho$-усули мураккаблигини қуйидаги ифода орқали баҳолаш мумкин:

$$Ip=\sqrt{\pi q}/2,$$

бу ерда $q$ – ЭЭЧ базавий нуқталари тартиби.

[45]да Поллард $\rho$-усули тезлигини $\sqrt{2}$ мартага ошириш мумкинлиги кўрсатилган. У ҳолда усул мураккаблиги $I_p=\sqrt{\pi q}/4$ билан баҳоланади.

Поллард $\rho$-усулининг афзаллик томонларидан бири криптотаҳлил жараёнини мустақил бир нечта параллел жараёнларга ажратишдир. Бу ҳолда ҳар бир жараённи амалга ошириш мураккаблиги $I_p=\sqrt{\pi q}/2r^2$ ва $I_p=\sqrt{\pi q}/4\ r^2$ билан баҳоланади.

Поллард $\lambda$-усули мураккаблиги $I_\lambda=2\sqrt{q}$ билан ва параллеллашда $I_\lambda=2r^{-1}\sqrt{q}$ билан баҳоланади.

Поллардннинг иккала усулининг қиёсий таҳлили Поллард $\lambda$-усули Поллард $\rho$-усулига нисбатан мураккаброқлигини кўрсатади.

2004 йилда Поллард параллелланган алгоритми асосида “бузилган” ЭЭЧ калитининг энг катта узунлиги *109* битни ташкил этди [46].

6-жадвалда ЭЭЧда дискрет логарифмлаш масаласини ечишнинг ҳисоблаш мураккаблигини баҳолари келтирилган [1, 45].

ЭЭЧда дискрет логарифмлаш масаласини Поллард $\rho$-усулидан фойдаланиб ечиш мураккаблигига тааллуқли келтирилган маълумотлар шуни кўрсатадики, ЭРИ алгоритмларида базавий нуқтаси $q\geq 2^{256}$ тартибли ЭЭЧ қўлланиши ЭЭЧ базасидаги ЭРИ зарур бардошлилигининг келажакдаги истиқболини таъминлайди. Бу ГОСТ Р 34.10-2001нинг 10 йил давомида муваффақиятли эксплуатацияси ва калитни очиш мураккаблиги $3*10^{38}$ арифметик амалдан иборатлиги билан ҳам асосланади.

6-жадвал

**ЭРИни бузиш мураккаблиги**

| Базавий нуқта *G* тартиби (узунлик битларда) | Группадаги амаллар сони |
|---|---|
| 128 | $1{,}63480*10^{19}$ |
| 192 | $7{,}02141*10^{28}$ |
| 256 | $3{,}01567*10^{38}$ |
| 320 | $1{,}29522*10^{48}$ |
| 352 | $8{,}48836*10^{52}$ |
| 384 | $5{,}56293*10^{57}$ |
| 416 | $3{,}64572*10^{62}$ |
| 448 | $2{,}38926*10^{67}$ |
| 480 | $1{,}56583*10^{72}$ |
| 512 | $1{,}02618*10^{77}$ |
| 1024 | $1{,}18824*10^{154}$ |

Кейинги параграфда даража параметри муаммосининг мураккаблигига асосланган криптотизимларни криптотаҳлиллаш йўналишлари баён этилган.

### 3.4. Даража параметри муаммосининг мураккаблигига асосланган криптотизимларни криптотаҳлиллаш йўналишлари

Параметрли функциядан фойдаланишга асосланган криптотизимларнинг анъанавий бир томонлама функцияларидан фойдаланишга асосланган криптотизимлардан асосий фарқи шундаки, уларда параметр *R* дан, параметрли ЭЭЧга асосланган тизимларда эса *R, a, B* дан фойдаланилади. Бунда параметр $R \geq 2^{160}$ қонуний томонлар учун маълум бўлса, ноқонуний томонлар учун номаълумдир. Бу албатта криптографик модуллар дастурий ва аппарат-дастурий кўринишда ишлаб чиқилган ҳолга

тегишлидир. Агар криптографик модуллар ***махсус аппаратли модуль*** турига мансуб бўлса, унда махфий параметрлар ваколатга эга субъект, масалан, КРОМ ёки банк маъсул ходими томонидан ўрнатилиб криптографик модуль параметр *R, a, B* ҳақидаги ахборот ошкор бўлишидан муҳофаза қилиш механизмлари билан таъминланган бўлади. Тармоқ фойдаланувчилари, махфий параметрларни билмаган тарзда криптографик модуллардан фойдаланганликлари туфайли, криптографик модулнинг бардошлилиги ва тезкорлиги нисбатан кичик $(p \sim 2^{256})$ модулларда ҳам қонуний ва ноқонуний томонлар учун етарлича юқори бўлади. Бундай махсус аппаратли модуллар Ўзбекистон алоқа ва ахборотлаштириш агентлиги қошидаги «UNICON.UZ» - Фан-техника ва маркетинг тадқиқотлари маркази Давлат унитар корхонаси ходимлари томонидан ишлаб чиқилмоқда. Қуйида, асосан ***дастурий*** криптографик модуллар устида сўз боради [1, 9].

Даража параметри муаммосининг мураккаблигига асосланган криптотизимларда параметр *R* маълум бўлганда, бундай муаммоларни дискрет логарифм муаммосига келтириш мумкин бўлгани боис, бундай криптотизимларнинг криптобардошлилиги дискрет логарифм муаммосининг мураккаблигига асосланган криптотизимлар криптобардошлилигига яқин, лекин ундан кам бўлмайди. Демак, қонуний фойдаланувчи томонлардан бири дискрет логарифм муаммосини ечиш учун етарли ресурсларга эга бўлсагина, криптотизимни обрўсизлантириш имконияти пайдо бўлади. Яъни, қонуний фойдаланувчи томонлар орасида ўзаро ишонч бўлгандагина, даража параметри муаммосининг мураккаблигига асосланган криптотизимларнинг дискрет логарифм муаммосининг мураккаблигига асосланган криптотизимларнинг криптобардошлилигидан кескин даражада юқори бўлади. Яъни, бунда криптотизимлар, асосан, ташқи бадният бузғунчиларга нисбатан криптобардошлиликни кескин даражада оширишга хизмат қилади.

Параметрли функциядан фойдаланишга асосланган криптотизимларда *ноқонуний томонлар* учун махфий саналган параметр *R* ни ҳисоблаб топиш

учун энг қуйи – биринчи поғона мураккаблигига оид даража параметри муаммосини ҳал этиш учун қуйидаги хоссага биноан

$$c \equiv \Sigma^{i=e-1}_{i=0} F^{i} \ (mod\ n)$$

таққосламасдан $F$ ни ҳисоблаб топиш лозим; бу ерда $c \equiv a^{-1} * a^{\backslash e} (mod\ n)$ маълум натурал сон.

Келтирилган таққослама $e=3$ бўлганда $c \equiv \Sigma^{i=e-1}_{i=0} F^{i} \ (mod\ n)$ ифодаси $a^{-1} * a^{\backslash 3} \equiv 1+F+F^2 \ (mod\ n)$ шаклини олади. Бу таққослама туб модулли ҳолларда иккинчи даражали таққосламага осонгина келтирилади ва масала квадрат илдизни топишдан иборат бўлади. Мураккаб модулли ҳолларда, квадрат илдиз топиш муаммоси факторлаш муаммосига тенг кучлидир.

Туб модулли ҳолларда ҳам $e$ туб сон бўлиб, $e>2^{159}$ бўлганда юқори даражали таққосламаларни ечиш мураккаб муаммодир. Бу $e$ туб сон бўлганда $\Sigma^{i=e-1}_{i=0} F^{i}$ келтирилмайдиган кўпҳади [9, 47] билан ҳам боғлиқ. Шундай қилиб, даража параметри муаммосини қўпол куч усули билан ҳал этишдан бошқа усул ҳозирча маълум эмас.

Туб модулли криптотизимлар учун $R$ ни топиш эҳтимоллиги $2^{-q}$ га тенг бўлиб, $p>2^{160}$ бўлганда уни топиш имконияти амалда йўққа чиқади.

Даража параметри муаммосининг мураккаблигига асосланган криптотизимдан *қонуний фойдаланувчи томон*лардан бири дискрет логарифм муаммосини ечиш учун етарли ресурсларга эга бўлса, криптотизимнинг криптобардошлилиги асосан берилган модуль учун дискрет логарифм муаммосини ечиш сарф-ҳаражатларига боғлиқ бўлади. Бунга қарши туриш учун дискрет логарифм муаммосининг мураккаблигига асосланган криптотизимларга хос пухта модуллардан $(p>2^{1023})$ фойдаланиш лозим бўлади.

Юқорида билдирилган фикрлар параметрли функция асосида қурилган Полиг-Хеллман усулига асосланган шифрларга, Эль Гамал ва Диффи-Хеллман усулига мос махфий калит алмашиш криптотизимларига ҳамда ЭРИ умумий схемасига мос криптотизимларга тааллуқлидир.

Яна шуни таъкидлаш жоизки, даража параметри муаммосининг мураккаблигига асосланган криптотизимлар синфига оид барча ЭРИ умумий схемаларидан фойдаланилганда, махфий асосдан фойдаланилганлиги боис ҳам қонуний фойдаланувчи томонлар учун, ҳам ноқонуний фойдаланувчи томонлар учун криптотизимни обрўсизлантириш эҳтимоллиги икки марта пасаяди ва сеанс калитли маромда ЭРИ сохталигини пайқаш имконияти пайдо бўлади.

Факторлаш муаммосининг мураккаблигига асосланган RSA усулига мос шифр ва ЭРИ схемалари учун, *ноқонуний томонлар* учун махфий саналган параметр $R$ ни топиш эҳтимоллиги $2^{-n}$ га тенг. Ноқонуний томон криптотизимни обрўсизлантириши учун топилган параметр $R$ дан фойдаланган ҳолда, яна модуль $n$ учун факторлаш муаммосини ечиши ҳам лозим бўлади. Бинобарин, дискрет логарифм ёки факторлаш муаммосини ечиш имконияти бўлган ноқонуний томоннинг криптотизимни обрўсизлантириш эҳтимоллиги нолга яқин.

Даража параметри муаммосининг мураккаблигига асосланган барча ЭРИ умумий схемаларининг криптотаҳлил йўналишлари қуйидагиларга бўлинади. Булар [9]:

1. ЭРИнинг ошкора калитларини сохталаштиришга йўналтирилган криптотаҳлил.
2. Ўзаро махфий калит – параметр $R$, $R_{ij}$ ларни топишга йўналтирилган криптотаҳлил.
3. ЭРИнинг ҳақиқийлигини тасдиқлаш таққосламаси асосида криптотаҳлил.
4. Хэш-функциянинг коллизиялар мавжудлигига асосланган ЭРИни сохталаштиришга йўналтирилган криптотаҳлил.
5. Ишлатиладиган протокол камчиликларидан фойдаланиш асосида имзони сохталаштиришга йўналтирилган криптотаҳлил.

Криптотаҳлилдан мақсад, имзо калитини билмаган ҳолда, алоқа канали бўйлаб жўнатилган сигналлар ўрнига аслига мос деб қабул

қилинадиган бошқа мазмун бериб, ЭРИни ҳам сохталаштиришдир. Криптотаҳлилда одатда, биринчидан, имзоланган ҳужжат ва имзоловчининг идентификатори, иккинчидан, махфий имзо калитидан бошқа ЭРИ ва ошкора сеанс калитини шакллантириш ҳамда уни текширишга оид барча алгоритмлар ва протоколлар маълум деб ҳисобланади.

1-2-бандларда келтирилган криптотаҳлил турлари фақат даража параметри муаммосининг мураккаблигига асосланган ЭРИ схемалари учун хосдир, чунки ўзга ЭРИ схемаларида ошкора калитлар ифодасида даража асоси ошкора параметр бўлиб, криптотаҳлилни мураккаблаштирувчи махфий асос ва параметр $R$, $R_{ij}$ лар қатнашмайди. Бу ерда $R_{ij}$ – махфий назорат калити. 3-бандда келтирилган криптотаҳлил тури ҳам, тасдиқлаш тақкосламасида махфий параметр $R$, $R_{ij}$ лар қатнашиши туфайли, ўзининг мураккаблиги билан ажралиб туради. ЭРИ дастурий таъминотидан фойдаланишда, ундан барча фойдаланувчилар ягона хэш-функция дастурий воситасига эга бўлишлари шарт бўлгани туфайли ҳужум объектлари қаторига хэш-функция дастурий воситаси ҳам киритилган. Қуйида хэш-функция дастурий воситаси зарур сифатларга эга ва ишлатиладиган протокол камчиликлардан ҳоли деб қаралган.

1-3-бандларга оид криптотаҳлил усуллари криптотаҳлил объекти синфининг моҳиятига кўра, қўпол куч асосида ва даража параметри муаммосини ечишга қаратилган криптотаҳлил жараёнлари кетма-кетлигидан иборат. Даража параметри муаммосини ечиш, аввало, қўпол куч усули асосида махфий параметр $R$, $R_{ij}$ ларни топишга, сўнгра даража параметри муаммосини дискрет логарифм муаммосига айлантириб, уни ечишга келтирилади.

Шуни таъкидлаш керакки, рақиб томон крипотаҳлилчиси дискрет логарифм муаммосини еча олганда ҳам, сохталаштирилган ЭРИ икки қайта тасдиқлаш маромида барибир фош этилади. Бу ишлаб чиқилган ЭРИ алгоритмининг энг кучли томонидир.

Носимметрик криптоалгоритмлар учун криптотаҳлил жараёнида уриниш амаллари сонининг ва уриниш натижасини синаш учун зарур бўлган амаллар сони сохта ошкора калитни (ва сеанс калитини) генерация қилиш учун зарур амаллар сони билан аниқланади [9] ва модуль узунлиги ошиши билан чизиқсиз равишда ортиб боради.

O‘z DSt 1092:2005, O‘z DSt 1092:2009 электрон рақамли имзо криптотизимлари учун криптотаҳлил объектлари бўлиб қуйидаги параметрлар хизмат қилади.

- Биринчидан, имзоловчи шахсга тегишли калитлар. Булар юқорида қайд этилган криптотаҳлил йўналишлари рўйхатининг 1-3-бандларига оид қуйидаги параметрлардир:

1-объект: *(x, u, $x_1$, a)* – махфий калитлар тўртлиги – имзолаш калитлари; ошкора калитлар учлиги – *(y, z, $y_1$)* ни генерациялаш учун зарур бўлиб, буларнинг чин қийматлари топилса, имзони сохталаштиришга йўл очилиши мумкин, аммо $R > 1$ бўлганда бу етарли эмас, чунки $y \equiv a^{\backslash x} \ (mod\ p)$, $z \equiv a^{\backslash u} \ (mod\ p)$, $y_1 \equiv a^{\backslash x1} \ (mod\ p)$ ифодалари бўйича ҳисобланиб, ифодаларда даражага ошириш учун $R > 1$ параметри қўлланилади;

2-объект: $R$ – ноқонуний фойдаланувчилар учун махфий параметр; у ошкора калитлар жуфтлигини генерациялаш ва ЭРИ ҳақиқийлигини дастлабки тасдиқлаш учун зарур;

3-объект: $R_{ij}$ – ноқонуний фойдаланувчилар учун махфий бўлган назорат калити, унда $R_{ij}$ имзоловчи шахс ва текширувчи томон учунгина маълум.

- Иккинчидан, криптотаҳлил йўналишлари рўйхатининг 3-бандида келтирилган ЭРИ киради:

4-объект: *(r, s)* – жуфтлик – *M* хабарга қўйилган ЭРИ.

Криптотаҳлилчига 4-объектни сохталаштириш учун 1-, 2-, 3-объектлар маълум бўлиши лозим. Келтирилган криптотаҳлил объектлари орасида 1-, 2-, 3-объектлар энг юқори криптобардошлиликка эгадир, чунки уларни топиб олиш учун кўпол куч усулидан фойдаланишга тўғри келади.

Шундай қилиб, ҳар бир объектни сохталаштириш учун бир марта ёки ундан ортиқ қўпол куч усулидан фойдаланишга тўғри келади.

1-объектни ташкил этувчи компонентлар $x$, $u$, $x_1$, $a$ ни тўғридан-тўғри танлаш усулида топиш эҳтимоллиги $2^{-q}$ га тенг.

Криптотаҳлилчи $a$ ни излашда қуйидаги стратегиядан фойдаланиш қулай бўлиши мумкин:

1-қадам: агар параметр $R$ берилган бўлса, ошкора калитларнинг қийматини даража кўрсаткичли қийматлар $y'$, $z'$, $y_1'$ га алмаштиринг, акс ҳолда $R$ ни $2^q$ фазосидан топинг. Бунинг учун

2-қадам: ихтиёрий $x'$ ни танланг;

3-қадам: $x'' \equiv x^{r-1} \pmod q$ ни ҳисобланг;

4-қадам: $a' \equiv y'^{x''} \pmod p$ ни ҳисобланг;

5-қадам: $y'' \equiv a'^{x'} \pmod p$ ни ҳисобланг;

6-қадам: $y'' == y'$ текширилади, агар тенглик бажарилса, унда $a'$ параметр $R$ га мос бўлган $a$ билан алмаштирилади, акс ҳолда 2-қадамга қайтилади.

7-қадам: ихтиёрий $u'$ ни танланг;

8-қадам: $z'' \equiv a'^{u'} \pmod p$ ҳисобланг;

9-қадам: $z'' == z'$ текширинг, агар тенглик бажарилса, унда ҳисоблашларни тўхтатинг, акс ҳолда 7-қадамга қайтинг.

10-қадам: ихтиёрий $x_1'$ ни танланг;

11-қадам: $y_1'' \equiv a'^{x1'} \pmod p$ ҳисобланг;

12-қадам: $y_1'' == y_1'$ текширинг, агар тенглик бажарилса, унда ҳисоблашларни тўхтатинг, акс ҳолда 10-қадамга қайтинг.

1-объектни ташкил этувчи компонентлар $x$, $u$, $x_1$, $a$ ни тўғридан-тўғри танлаш усулида топиш эҳтимоллиги $2^{-q}$ га тенг.

Агар бадният бузғунчи ёки рақиб томон криптотаҳлилчиси қонуний фойдаланувчилар орасида бўлиб, дискрет логарифм муаммосини ечишга қодир бўлса, айниқса туб модуль сифатида $p \sim 2^{256}$ дан фойдаланилганда, $R$ ва $R_1$ лар маълум бўлганда ва дастурий, анъанавий аппарат ёки аппарат-

дастурий криптографик модулдан фойдаланилса, 1-объектни ташкил этувчи компонентлар *x, u, $x_1$, a* ни *аниқ ҳисоблаб топиш мумкин.* Бунда бошланғич маълумот сифатида ЭРИнинг барча ошкора параметрлари, имзоланган маълумот *M* нинг хэш-қиймати *m*, ЭРИ *(r, s, $y_i$)*, *R* ва $R_1$ лар бузғунчига маълум деб ҳисобланади.

1-объектни ташкил этувчи компонентлар *x, u, $x_1$, a* ни топиш учун қуйидаги қадамлар кетма-кетлигини амалга ошириш лозим.

1-қадамда қуйидаги

$y \equiv z^{\backslash i} \ (mod\ p),$

$y \equiv (m^{\backslash -1} \circledR\ r)^{\backslash j} (mod\ p)$

иккита таққосламалар тизими билан берилган тизимни дискрет логарифм масалалари тизимига келтириш [9].

2-қадамда логарифм масаласи тизимини ечиш, яъни *i* ва *j* ни топиш.

3-қадамда ***i, j*** ва *s* учун ночизиқли таққосламалар тизимини қуйидаги

$i \equiv x*u^{-1} (mod\ q),\ j \equiv x*(-k)^{-1} (mod\ q),\ s*u \equiv k-r*x\ (mod\ q)$

кўринишда тузиш.

4-қадамда *i, j* ва *s* учун ночизиқли таққосламалар тизимини ечиш ва *x, u, k* ларни топиш. Бу қадамни бажариш мураккаблиги дискрет логарифм масаласини ечишга қараганда бир неча маротаба осон.

5-қадамда $ut = u^{-1}$ қабул қилиб**,** $a \equiv z^{\backslash ut}\ (mod\ p)$ таққосламадан *a* топиш**.**

Натижада, сохта имзони шакллантириш имконияти туғилади. Бироқ, сохта ЭРИ давлат стандарти O‘z DSt 1092:2005, O‘z DSt 1092:2009га хос НСКУ [9]га асосланган протоколга мувофиқ фойдаланувчига, сеанс назорат калити $(y_1, a^{\backslash\backslash k})$ эса КРОМ орқали фойдаланувчиларга етказилиши туфайли, сохта ЭРИ бузғунчининг ўзигагина тегишли қилиб КРОМ ЭРИ билан тасдиқланади. Фойдаланувчи эса ЭРИ ҳақиқийлигини тасдиқлаш жараёнида бузғунчининг ошкора калитларидан фойдаланади ва ЭРИни ҳақиқий эмас деган хулосага келади. Чунки, бузғунчига ҳақиқий ЭРИ эгасининг КРОМ билан боғланишда фойдаланадиган махфий симметрик калит маълум эмас ва у $(y_1, a^{\backslash\backslash k})$ ни фақат ўзининг махфий симметрик калити билан шифрлаб

КРОМга жўнатиши мумкин. Натижада, протокол туфайли, криптотаҳлилчининг сохталаштирилган ЭРИси фош бўлиб, рақиб томон криптотаҳлилчисининг меҳнати зое кетиши туфайли бузғунчи бундай ҳужум стратегиясидан фойдаланмайди. Бузғунчи бундай стратегиядан, қонуний ЭРИ эгасининг КРОМ билан боғланадиган махфий симметрик калитини қўлга киритган бўлсагина, ундан фойдаланиб ўз мақсадига эришиши мумкин. Бундай имконият ҳар қандай ЭРИ схемасига тенг тааллуқлидир.

2-объект $R$ топиш эҳтимоллиги ва 3-объект $R_{ij}$ ни топиш эҳтимоллиги $2^{-q}$. Бинобарин, юқорида санаб ўтилган махфий параметрларни топиш учун ўлчамлари $q = 2^{255}$ бўлган улкан фазода кетма-кет танлаш усулини қўллаш лозим бўлади. Маълумки, яқин келажакда буни мавжуд ҳисоблаш техникаси воситалари ёрдамида амалга ошириш имконияти мавжуд эмас.

4-объектни сохталаштириш учун криптотаҳлилчи даставвал, текшириш ифодасидаги ҳақиқий ҳужжат хэш-функцияси қиймати $m$ ни сохта ҳужжатнинг хэш-функцияси $m'$ билан алмаштирилган ифодани шакллантиради, сўнгра дискрет логарифм муаммосини ечиш натижасида сохта имзонинг биринчи қисми $s'$ ни топади. Яъни, криптотаҳлил қуйидаги қадамлар кетма-кетлигини бажаришдан иборат:

1-қадам: $m' \equiv z^{\backslash s} \circledR y^{\backslash r1} \circledR r \pmod p$ шакллантиринг; бу ерда $r_1 = r \pmod q$.

2-қадам: $z^{\backslash s'} = m' \circledR y^{\backslash -r1} \circledR r^{\backslash -1} \pmod p$ ҳисобланг; бу ерда $y^{\backslash -r1} \pmod p - y^{\backslash r1}$ нинг $p$ модуль бўйича параметрли тескари қиймати, $r^{\backslash -1} \pmod p - r$ нинг $p$ модуль бўйича параметрли тескари қиймати.

3-қадам: $z^{\backslash s'}$ нинг қийматига мос $z^{s'}$ қиймат билан алмаштиринг.

4-қадам: дискрет логарифм муаммосининг ечими сифатида $s'$ ни топинг.

Оқибатда, сохта ҳужжат хэш-функцияси $m'$ учун мос сохта имзо $(r, s')$ ни шакллантиради. Бунда ҳар бир ҳақиқий имзони сохталаштириш учун ҳар сафар янгидан дискрет логарифм муаммосини тўла ечиш зарур бўлади.

Шундай қилиб, махфий калитлар $x$, $u$, $x_1$, махфий асос $a$ ни дискрет логарифм масаласи асосида ҳисоблаш учун, аввало махфий параметр $R$,

назорат калити $R_{ij}$ маълум бўлиши даркор; улардан ҳар бирини ҳисоблаб топиш учун $5,79*10^{76}$ амални бажариш зарур ва бу $1,93*10^{63}$ mips – йилни ташкил қилади.

### 3.5. Электрон рақамли имзо алгоритмларини криптотаҳлиллашнинг параметрлар группаси усули

Маълумки, агар дискрет логарифм муаммосини ҳал этиш мумкин бўлса, унда факторлаш муаммоси ҳам ечилади ва бу икки муаммони бир хил узунликдаги модуллар учун ечиш бир-бирига яқин миқдордаги амалларни талаб этади. Ошкора калитли криптоалгоритмларни замонавий криптотаҳлил усуллари орасида *365* битга тенг ёки ундан катта узунликдаги модуллар учун энг самарали усул умумий сонли майдон ғалвири усули NFC юқорида баён этилган эди.

Қуйида Х.П. Хасанов томонидан ишлаб чиқилган ошкора калитли криптотизимларни криптотаҳлиллашнинг параметрлар группаси усули келтирилган [48].

Параметрлар группаси асосида ҳозиргача маълум бўлган барча симметрик блокли шифрлар ва ошкора калитли ва криптотизимларга ўхшаш криптотизимларни амалга ошириш, уларни такомиллаштириш ҳамда уларга ўхшаши бўлмаган криптотизимларни яратиш мумкин. Шунингдек, янги криптотаҳлиллаш усулларини ҳам яратиш мумкин. Бунга далил бўлиб келтирилган RSA криптотизимини криптотаҳлиллаш усули хизмат қилади.

Юқорида айтиб ўтилганидек, параметрлар группасида RSA криптотизимига аналог бўлган алгоритмни амалга ошириш учун параметр $R\geq 1$ ни танлаш, сўнгра RSA криптотизимида даражага ошириш амали ўрнига коэффициент $R$ билан даражага ошириш амалини қўллаш кифоя қилади. Натижада [14, 49-50] да келтирилган RSA алгоритмига аналог бўлган ЭРИ алгоритми шаклланади. ЭРИни шакллантириш, узатиш ва ЭРИ ҳақиқийлигини тасдиқлаш жараёнлари қуйидаги қадамлар кетма-кетликларини ўз ичига олади:

1) *M* хабар учун хэш-функция $m = h(M)$ ҳисобланади:

$m = h(M);$

2) модуль *n* ва махфий калитдан фойдаланиб *m* учун рақамли имзо *S* шакллантирилади:

$S \equiv m^{\backslash d} \pmod{n},$

бу ерда $d*e \pmod{(p-1)*(q-1)} \equiv 1$, *p* ва *q* махфий туб сонлар, *d* -тоқ сонли даража кўрсаткичи, *e* - ошкора калит қисми (тоқ сонли даража кўрсаткичи)*;*

3) хабар *M* ва рақамли имзо *S* алоқа каналидан узатилади.

Қабул қилувчи томонда:

1) ошкора калит *(n; e)* дан фойдаланиб *S* учун хэш-функция қиймати m шакллантирилади:

$m \equiv S^{\backslash e} \pmod{n};$

2) *M* хабар учун хэш-функция $m' = h(M)$ ҳисобланади:

$m' = h(M);$

3) *m* билан *m'* таққосланади:

$m = = m'.$

Агар таққосланган қийматлар тенг чиқса, у ҳолда хабар олувчи *(M, S)* жуфтлигининг ҳақиқийлигини тан олади. *M* хабардаги рақамли имзо *S* ни фақат *d* махфий калит эгасигина шакллантириши мумкинлиги ўз тасдиғини топади, акс ҳолда ЭРИ ҳақиқий эмас деб топилади.

RSA криптотизимига аналог бўлган криптотизим криптобардошлилиги модули *n* ни факторлаш муаммосини ечиш учун зарур амаллар миқдори билан белгиланади. Агар параметр *R* имзо муаллифи ва уни қабул этувчи учун ўзаро махфий тасодифий сон бўлса, криптотизимнинг криптобардошлилиги бошқа криптотаҳлилчилар учун факторлаш муаммосининг мураккаблигига нисбатан ҳаддан зиёд ортиб кетади. Чунки, параметр *R* ни қўпол ҳужум (тўлиқ танлаш усули)дан ўзга усулдан фойдаланиб топиш усули ҳозирча маълум эмас. Шу боис, RSA криптотизимини Ўзбекистон Республикасида фойдаланиш мадомики лозим

бўлса, унда параметрлар группасида яратилган унинг аналогидан фойдаланиш мақсадга мувофиқ экани ҳеч қандай шубҳага ўрин қолдирмайди.

Факторлаш муаммосини ечиш учун RSA криптотизимини параметрлар группасидаги аналоги учун параметр $R$ ва ошкора калит $(n, e)$ берилган деб қаралади. Криптотаҳлиллаш усуллари Хасанов Х.П. томонидан аниқланган параметрлар группасида даражага ошириш функцияларининг хоссаларидан фойдаланишга асосланади.

Криптотаҳлиллаш усули қуйидаги қадамлар кетма-кетлигини ўз ичига олади:

1) $p+q$ қийматида битлар сонининг пастки чегараси

$i_{min} = \lfloor Lg_2 \sqrt{n} \rfloor$ ва $R_{i\,min} = 2^{i\,min}$ ҳисобланади ва $R = 2^{i\,min+\nabla}$ танланади, бу ерда $\nabla \geq 1$.

2) даража асоси $a$ танланади, буерда $a \in \{1,3,5. .., n-2\}$.

3) $a_4^{\backslash n+1} \pmod{n_4}$ ҳисобланади,

бу ерда $i=4$, $a_4^{\backslash n+1}$ - $a$ нинг $n_4 = n*2^4$ модуль бўйича параметр $R=2^4$ билан $(n+1)$ - даражаси қиймати.

4) $n_i = n*2^4$ ва $c_i = a_i^{\backslash n+1}$, бу ерда $i=4$;

5) $x_i \equiv c_i \pmod{R}$ ҳисобланади; агар $R_{i\,min} > x_i$ ёки $x \geq R$ бўлса, унда кейинги қадамга ўтилади ва $i = i+1$ қабул қилинади,

агар $R > x_i > R_{i\,min}$ бўлса, унда $p_i = x_i/2 + (x_i/2+n)^{1/2}$, $q_i = x_i - p_i$ ва $n_i = p_i * q_i$ ҳисобланади,

агар $n_i = n$ бўлса, ҳисоблашлар тўхтатилади, акс ҳолда кейинги қадамга ўтилади ва $i = i+1$ қабул қилинади;

6) $a_4^{\backslash n+1} = c_i$ қабул қилинади ва

$d_i \equiv c_i + R_i * n$ ҳисобланади, бу ерда $R_i = 2^i$; натижалардан $z_i \in \{c_i, d_i\}$ тўплами шакллантирилади;

7) $z_i$ тўпламининг алгоритм элементи учун $x_i \equiv z_i \pmod{R}$ ҳисобланади, бу ерда $z_i \in \{ c_i, d_i \}$; агар $R_{i\,min} > x_i$ ёки $x \geq R$ бўлса, унда кейинги қадамга ўтилади ва $i = i+1$ қабул қилинади,

агар $R > x_i > R_{i\ min}$ бўлса, унда $p_i = x_i/2 + (x_i/2+n)^{1/2}$, $q_i = x_i - p_i$ ва $n_i = p_i * q_i$ ҳисобланади,

агар $n_i = n$ бўлса, ҳисоблашлар тўхтатилади, акс ҳолда кейинги қадамга ўтилади ва $i = i+1$ қабул қилинади;

8) $c_i = c_i$ , $d_i = d_i$, қабул қилинади ва

$e_i \equiv c_i + R_i * n$, $f_i \equiv d_i + R_i * n$ ҳисобланади, бу ерда $R_i = 2^i$; натижалардан $z_i \in \{c_i, d_i, e_i, f_i\}$ тўплами шакллантирилади;

9) $z_i$ тўпламининг ҳар бир элементи учун $x_i \equiv z_i \ (mod\ R)$ ҳисобланади; агар $R_{i\ min} > x_i$ ёки $x \geq R$ бўлса, унда кейинги қадамга ўтилади ва $i = i+1$ қабул қилинади,

агар $R > x_i > R_{i\ min}$ бўлса, унда $p_i = x_i/2 + (x_i/2+n)^{1/2}$, $q_i = x_i - p_i$ ва $n_i = p_i * q_i$ ҳисобланади,

агар $n_i = n$ бўлса, ҳисоблашлар тўхтатилади, акс ҳолда кейинги қадамга ўтилади ва $i = i+1$ қабул қилинади;

10) $c_i = c_i$ , $d_i = d_i$, $e_i = e_i$, $f_i = f_i$ қабул қилинади ва

$g_i \equiv c_i + R_i * n$, $h_i \equiv d_i + R_i * n$, $i_i \equiv c_i + R_i * n$, $j_i \equiv d_i + R_i * n$ ҳисобланади, бу ерда $R_i = 2^i$; натижалардан $z_i \in \{c_i, d_i, e_i, f_i, g_i, h_i, i_i, j_i\}$ тўплами шакллантирилади;

9-10 қадамлар итератив тарзда ижобий натижа чиққунча давом этади.

Қуйида модуль $p-1$ ва $q-1$ нинг факторлари туб сон бўлиши шарти қаноатлантирадиган модуль $n=8881$ учун юқорида келтирилган усул бўйича ҳисоблашлар бажарилганда, 5-қадамдаёқ ижобий натижа олиниши акс этган (7-жадвал).

7-жадвал

**Параметрлар группаси усулида факторлаш**

| | 4 | 8 | |
|---|---|---|---|
| $a_1^{\backslash n+1}$ | 26362 | 26362 | |
| $c_i$ | 26362 | 61886 | |
| $x_i$ | | | 190 |
| $p_i$ | | | 107 |
| $q_i$ | | | 83 |
| $n_i$ | | | 8881 |

Қуйида модуль $n=8881$ учун ҳисоблашлар то $R=2^8$ бўлгунча бетўхтов давом этган ҳол учун ҳисоблашлар натижалари келтирилган. 8-жадвал ўз моҳияти бўйича тўлиқ танлаш усулини акс эттиради.

8-жадвал

**Тўлиқ танлаш усулида факторлаш**

| | 4 | 8 | 16 | 32 | 64 | 128 | 256 | |
|---|---|---|---|---|---|---|---|---|
| $a_1^{\backslash n+1}$ | 26362 | 26362 | 97410 | 239506 | 523698 | 523698 | 523698 | 178 |
| $c_i$ | 26362 | 61886 | 61886 | 61886 | 61886 | 61886 | 61886 | 190 |
| | | | 132934 | 203982 | 346078 | 630270 | 1198654 | 62 |
| | | | | 132934 | 203982 | 346078 | 630270 | 254 |
| | | | | 275030 | 488174 | 914462 | 1767038 | 126 |
| | | | | | 132934 | 203982 | 346078 | 222 |
| | | | | | 417126 | 772366 | 1482846 | 94 |
| | | | | | 275030 | 488174 | 914462 | 30 |
| | | | | | 559222 | 1056558 | 2051230 | 158 |
| | | | | | | 132934 | 203982 | 206 |
| | | | | | | 701318 | 1340750 | 78 |

8-жадвалнинг давоми

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | **417126** | **772366** | **14** |
| | | | | | | **985510** | **1909134** | **142** |
| | | | | | | **275030** | **488174** | **238** |
| | | | | | | **843414** | **1624942** | **110** |
| | | | | | | **559222** | **1056558** | **46** |
| | | | | | | **1127606** | **2193326** | **174** |
| | | | | | | | **132934** | **70** |
| | | | | | | | **1269702** | **198** |
| | | | | | | | **701318** | **134** |
| | | | | | | | **1838086** | **6** |
| | | | | | | | **417126** | **102** |
| | | | | | | | **1553894** | **230** |
| | | | | | | | **985510** | **166** |
| | | | | | | | **2122278** | **38** |
| | **4** | **8** | **16** | **32** | **64** | **128** | **256** | |
| | | | | | | | **275030** | **86** |
| | | | | | | | **1411798** | **214** |
| | | | | | | | **843414** | **150** |
| | | | | | | | **1980182** | **22** |
| | | | | | | | **559222** | **118** |
| | | | | | | | **967748** | **68** |
| | | | | | | | **1127606** | **182** |
| | | | | | | | **2264374** | **54** |

Келтирилган параметрлар группаси усули асосида криптотаҳлил самарали бўлиш эҳтимоли мавжудлиги RSA криптотизимини лойиҳалаш процедураси албатта танланган модуль *n* ни параметрлар группаси асосида криптотаҳлилга бардошлилигига синаш амалларини бажариш зарурлигига шубҳа қолдирмайди. *Бу, айниқса Ўзбекистон Республикасида қўлланилиши*

*мумкин бўлган RSA, PGP ва ESIGN криптотизимлари учун алоҳида аҳамият касб этади, чунки бу криптотизимлар криптобардошлилиги параметрлар группаси асосида ҳеч қачон синовдан ўтмаган.*

RSA, PGP ва ESIGN криптотизимларини лойиҳалаш жараёнида уларнинг параметрлар группаси усули асосида крптоҳужумларга етарли даражадаги криптобардошлилигини таъминлаш асос *a* нинг даража кўрсаткичи *p+q* га тенг бўлганда параметр *R* билан даража қийматлари қатори $a_i^{\backslash p+q}$ *(mod* $n_i$*)* қаторида ва кўплаб унга қўшни қаторларда қиймат фарқлари кетма-кетлиги камида *256* битли код билан ифодаланган бўлиши шарт. Бундай қаторда ёнма-ён қийматлар фарқи агар *0* бўлса, унда иккилик код рақами *0*, акс ҳолда, яъни $R_i$**n* бўлса, унда иккилик код рақами *1* га тенг олинади; бу ерда $R_i = 2^I$ учун i$\in${*1,2,3. .., R*}.

Дискрет логарифм муаммосининг мураккаблигига асосланган ЭРИ умумий схемалари алгоритмларининг криптобардошлилиги факторлаш муаммосининг мураккаблигига асосланган алгоритмларни параметрлар группаси усулида криптотаҳлилга бардошлилиги модуллар узунлиги бир хил бўлса, *R* $2^{\sqrt{n}}$ марта катта бўлади.

### 3.6. RSA криптотизими протоколининг заиф томонларидан фойдаланишга асосланган ҳужумлар ва уларни олдини олиш

#### 3.6.1. RSA алгоритмидан фойдаланиб шифрланган маълумотни калитсиз очиш усули

***Бошланғич шартлар***: Бузғунчи (хакер, криптотаҳлилчи)га очиқ калит *(e, n)* ва шифрматн *C* маълум [1].

***Қўйилган масала***: Очиқ матн *M* топилсин.

Криптотаҳлилчи $C^{e^j} (\mathrm{mod} n) = C$ тенгликни қаноатлантирувчи *j* сонини танлайди, яъни криптотаҳлилчи каналдан олинган шифрматнни *j* марта очиқ калит ёрдамида шифрлайди (бу қуйидаги кўринишга эга $((((C^e)^e)^e)...)^e (\mathrm{mod} n) = C^{e^j} (\mathrm{mod} n)$). Шу тенгликни қаноатлантирувчи *j* ни

топгандан кейин криптотаҳлилчи $C^{e^{j-1}} (\mathrm{mod} n)$ ни ҳисоблайди (яъни *j-1* марта шифрлаш амалини бажаради) – ушбу қиймат очиқ матн *M* га тенг бўлади. Бу $C^{e^j} (\mathrm{mod} n) = (C^{e^{j-1}} (\mathrm{mod} n))^e$ дан келиб чиқади, яъни маълум бир *e* даражага оширилган $C^{e^{j-1}} (\mathrm{mod} n)$ сони шифрматн *C* беради.

***Мисол***: *p=983, q=563, e=49, M=123456.*

$C=M^{49} (mod\ n)=1603,$

$C^{49^7} (mod\ n)=85978,$

$C^{49^8} (mod\ n)=123456,$

$\tilde{N}^{49^9} (mod\ n)=1603.$

### 3.6.2. Нотариусли схемада ишлатилган RSA алгоритми ёрдамида қўйилган имзога ҳужум

***Бошланғич шартлар***: Ундан ўтадиган ҳужжатларни имзоловчи электрон нотариус бор деб тасаввур қиламиз. *N* – бу нотариус имзолашни рад этаётган очиқ матн. Криптотаҳлилчига нотариусни очиқ калити *(e, n)* маълум.

***Қўйилган масала***: *N* матнини имзолаш.

Криптотаҳлилчи *N* билан ўзаро туб бўлган маълум бир тасодифий сон *x* ни танлайди ва $y=x^e\ (mod\ n)$ ҳисоблайди. Сўнгра $M=yN$ қийматни олади ва нотариусга имзолаш учун жўнатади. Нотариус эса уни имзолайди $M^d (mod\ n)=S$ (чунки, у энди *N* эмас), яъни $S=M^d (mod\ n)=y^d N^d=(x^e)^d N^d=xN^d$, демак $N^d=Sx^{-1} (mod\ n),$ яъни фақатгина *S* ни *x* га бўлиш кифоя.

***Ҳимоя қилиш***: Имзо қўйиш вақтида маълумотга бирон-бир тасодифий сон (масалан, вақт моменти) қўшиш лозим. Шу орқали *M* сонининг бузилиши рўй беради, яъни $M_{(қўшилгандан сўнг)} + yN.$

### 3.6.3. Танланган шифрматн бўйича RSA алгоритмидан фойдаланиб қўйилган имзога ҳужум

***Бошланғич шартлар***: *C* шифрматни мавжуд. Криптотаҳлилчига жўнатувчининг очиқ калити *(e, n)* маълум.

***Қўйилган масала***: Очиқ матн $M$ ни топиш.

Криптотаҳлилчи қандайдир $r$ ни танлайди: $r<n$, $(r,n)=1$ ва $x=r^e(mod\ n)$ ни ҳисоблайди. Сўнгра у $t=r^{-1}(mod\ n)$ ва $y=xC(mod\ n)$ ҳисоблайди ва $y$ ни жўнатувчи имзолаши учун жўнатади.

Жўнатувчи ҳеч нарсадан шубҳаланмай $y$ матнни имзолайди: $w=y^d(mod\ n)$ ва $w$ қайтариб жўнатиб юборади.

Криптотаҳлилчи $tw(mod\ n)=r^{-1}y^d(mod\ n)=(r=x^d mod\ n$ бўлгани учун$)=x^{-d}x^dC^d(mod\ n)=C^d=M$, $M$ ни топади.

Криптотаҳлилчи $C$ ни бирданига имзолаш учун юбора олмайди, чунки жўнатувчи имзолашдаги натижаларни текшираётган бўлиши мумкин ва провокацияни сезиб қолиши мумкин.

Ушбу ҳужум озмунча гипотетик хусусиятга эга эмас, лекин шунга қарамай, қуйидагича бир нечта хулосалар чиқариш имконини беради:

а) имзолаш ва шифрлашни турли хил калитларда амалга ошириш лозим;

б) имзолаш пайтида тасодифий вектор қўшиш лозим ёки хэшлаш функциясидан фойдаланиш лозим.

## 3.7. Носимметрик криптотизимларни криптотаҳлиллаш усулларининг таснифи

Носимметрик криптотизимларни криптотаҳлиллаш усуллари ва алгоритмларини таснифлаш мумкин бўлган асосий белгилар тўпламига қуйидагилар киради:

1 Ҳар қандай носимметрик криптотизимга қўлланиш даражаси.

2 Криптотизим бардошлилигини таъминловчи муаммо тури.

3 Криптотаҳлил амалга ошириладиган алгебраик структура тури.

4 Носимметрик криптотизимни таҳлиллашда силлиқлик хоссасидан фойдаланиш даражаси.

5 Криптотизим учун протокол камчиликларидан фойдаланиш даражаси.

6 Қўшимча каналлардан фойдаланиш даражаси.

Носимметрик криптотизимларни криптотаҳлиллаш усуллари ва алгоритмлари биринчи белги - ҳар қандай носимметрик криптотизимга қўлланиш даражаси бўйича универсал ва ноуниверсал синфларга бўлинади. Универсал синфга оид усуллар 2-бўлимда баён этилган, ноуниверсал синфга оид усул ва алгоритмлар 3-бўлимда келтирилган.

Носимметрик криптотизимларни криптотаҳлиллаш усуллари ва алгоритмлари иккинчи белги - криптотизим бардошлилигини таъминловчи муаммо тури бўйича факторлаш муаммоси, дискрет логарифмлаш муаммоси, ЭЭЧ группасида дискрет логарифмлаш муаммоси, даража параметри ва дискрет логарифмлаш муаммоси композицияси синфларига, шунингдек криптотизим бардошлилигини таъминловчи булардан бошқа муаммолар синфларига бўлинади. Энг кўп фойдаланиладиган факторлаш, дискрет логарифмлаш ва ЭЭЧ группасида дискрет логарифмлаш муаммолари синфларига оид усуллар ва алгоритмлар 3-бўлимда баён этилган. Даража параметри ва дискрет логарифмлаш муаммоси композицияси синфига оид криптотаҳлиллаш усуллари ҳам шу бўлимда келтирилган.

Носимметрик криптотизимларни криптотаҳлиллаш усуллари ва алгоритмлари учинчи белги - криптотаҳлил амалга ошириладиган алгебраик структура тури бўйича группа, ҳалқа ва майдон синфларига бўлинади. 3-бўлимда келтирилган криптотаҳлиллаш усуллари ва алгоритмлари учун тегишли алгебраик структуралар уқтириб ўтилган.

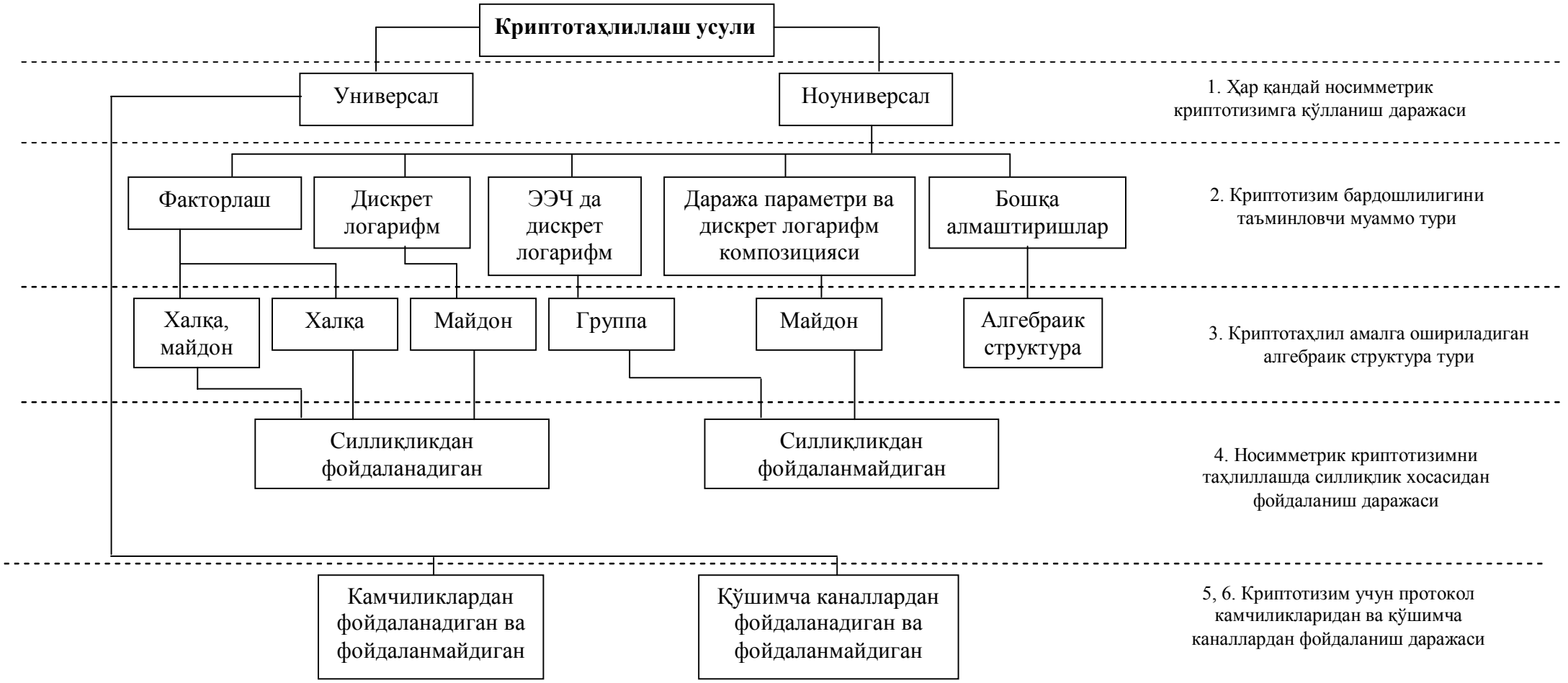
Носимметрик криптотизимларни криптотаҳлиллаш усуллари ва алгоритмлари тўртинчи белги - носимметрик криптотизимни таҳлиллашда силлиқлик хоссасидан фойдаланиш даражаси бўйича силлиқликдан фойдаланадиган ва силлиқликдан фойдаланмайдиган синфларга бўлинади. Иккала синфга оид усуллар ва алгоритмлар 3-бўлимда баён этилган.

Носимметрик криптотизимларни криптотаҳлиллаш усуллари ва алгоритмлари бешинчи белги - криптотизим учун протокол камчиликларидан фойдаланиш даражаси бўйича протокол камчиликларидан фойдаланадиган ва

протокол камчиликларидан фойдаланмайдиган синфларга бўлинади. Биринчи синфга оид усуллар 3.6. да баён этилган, 2-бўлимда келтирилган усуллар эса иккинчи синфга оиддир.

Носимметрик криптотизимларни криптотаҳлиллаш усуллари ва алгоритмлари олтинчи белги - қўшимча каналлардан фойдаланиш даражаси бўйича қўшимча каналлардан фойдаланадиган ва қўшимча каналлардан фойдаланмайдиган синфларга бўлинади. Биринчи синфга оид усуллар 2-3-бўлимларда баён этилган, 2-бўлимда келтирилган қолган усуллар ва 3-бўлимга тегишли усул ва алгоритмлар иккинчи синфга оиддир.

Қуйидаги 5-расмда носимметрик криптотизимларни криптотаҳлиллаш усуллари ва алгоритмларининг таснифи келтирилган [1].




5-расм. Криптотаҳлиллаш усулларининг таснифи

## Назорат саволлари

1. Носимметрик криптотизимларнинг кўпчилиги қандай муаммоларнинг мураккаблигига асосланади ва криптотаҳлил процедураси қандай мақсадларни кўзлайди?

2. Факторлаш муаммосининг криптотаҳлили билан қайси буюк математиклар шуғулланганлар?

3. Субэкспоненциал алгоритмлар синфига оид қайси усулларни биласиз? Уларнинг қайсиларида силлиқлик хоссасидан фойдаланилади?

4. Диксон усули нечта босқичда амалга оширилади? Унда қайси алгебраик амаллардан фойдаланилади?

5. Квадратик ғалвир усулининг Диксон усулига ўхшаш томонлари нимада?

6. Квадратик ғалвир тузиш нима ҳисобига фактор базасини шакллантириш ишини осонлаштиради?

**7.** Померанц квадратик ғалвир усули қандай асосда такомиллаштирилган?

8. Сонли майдон ғалвири усулига ким биринчи бўлиб асос солган ва у қандай сонларни факторлаш имконини беради?

9. Замонавий сонли майдон ғалвири усули сонларнинг қайси чегаралари (ўнли хоналарда) учун энг тезкор ҳисобланади?

10. Сонли майдон ғалвири усули билан факторланган сонларнинг рекорд қиймати қанча?

11. Сонли майдон ғалвири усули билан криптотаҳлиллаш учун зарур амаллар бажариш вақти қандай ифода бўйича аниқланади?

12. Замонавий дискрет логарифмлаш усуллари сонли майдон ғалвири усуллари билан ўхшаш ва фарқли томонларини ва босқичларини тушунтиринг?

13. Индексли ҳисоблаш усулининг асосий ғояси нимада?

14. Эллиптик эгри чизиқ группасида дискрет логарифмлаш муаммосининг мураккаблигига асосланган тизимларни энг тезкор криптотаҳлиллаш усуллари йўқлигининг асосий сабаби нимада?

15. ЭЭЧ группасида дискрет логарифмлаш муаммосини ечишнинг самарали ҳисобланган қайси криптотаҳлил усулларини биласиз? Уларни амалга ошириш учун зарурий амаллар сони қандай ифодаланади?

16. Даража параметри муаммосининг мураккаблигига асосланган криптотизимларни криптотаҳлиллашнинг қайси йўналишларини биласиз?

17. Агар криптографик модуллар махсус аппаратли модуль турига мансуб бўлса, даража параметри муаммосининг мураккаблигига асосланган криптотизимларнинг бардошлилиги нима сабабдан энг юқори бўлади?

18. Даража параметри муаммосининг мураккаблигига асосланган дастурий криптомодулда амалга оширилган криптотизимларнинг бардошлилиги нима сабабдан қонуний ва ноқонуний кимсалар учун ҳар хил бўлади?

19. O‘z DSt 1092:2005, O‘z DSt 1092:2009 электрон рақамли имзо криптотизимлари учун криптотаҳлил объектлари бўлиб қандай параметрлар хизмат қилади?

20. Махфий параметр $R$, назорат калити $R_{ij}$ дан ҳар бирини ҳисоблаб топиш учун зарур амаллар сони қандай ифодаланади?

21. Параметрлар группасида RSA криптотизимига аналог бўлган алгоритмни амалга ошириш қандай қадамларни ўз ичига олади?

22. Криптотаҳлиллашнинг параметрлар группаси усули қандай қадамлар кетма-кетлигини ўз ичига олади?

23. RSA алгоритмидан фойдаланиб шифрланган маълумотни калитсиз очиш усули қандай қадамлар кетма-кетлигини бажаришни кўзда тутади?

24. RSA алгоритмидан фойдаланиб шифрланган маълумотни калитсиз очиш усули қандай қадамлар кетма-кетлигини бажаришни кўзда тутади?

25. Нотариусли схемада ишлатилган RSA алгоритми ёрдамида қўйилган имзога ҳужум қандай уюштирилади ва ҳужумдан қандай химояланиш мумкин?

26. Танланган шифрматн бўйича RSA алгоритмидан фойдаланиб қўйилган имзога ҳужум қандай уюштирилади?

27. Носимметрик криптотизимларни криптотаҳлиллаш усуллари ва алгоритмларини таснифлаш мумкин бўлган асосий белгилар тўпламига қайси тасниф белгилари киради?

# 4. СИММЕТРИК КРИПТИЗИМЛАРНИ КРИПТОТАҲЛИЛЛАШ УСУЛЛАРИ

## 4.1. Симметрик криптотизимлар ва уларни криптотаҳлиллашнинг замонавий усуллари

### 4.1.1. Симметрик криптотизимлар

Ўзбекистон Республикаси коммуникацион тизимларида фойдаланишда бўлган симметрик шифрлар узлуксиз (оқимли) ва блокли шифрлар бўлиб, оқимли шифрлар асосан хориждан харид қилинган коммуникация воситаларида фойдаланилади. Оқимли шифрларнинг криптобардошлилиги хавфсизлик талабларига жавоб беради. Ўзбекистон Республикасида фойдаланишда бўлган блокли шифрларга асосан O‘z DSt 1105:2006, O‘z DSt 1105:2009 [51] ва ҳамдўстлик мамлакатлари учун собиқ Совет Иттифоқи давридан мерос бўлиб қолган ГОСТ 28147-89 [52] киради.

Криптографлар орасида машҳур бўлган маълумотларни шифрлаш алгоритмлари гуруҳига АҚШ давлат стандартлари – DES [9, 14], AES [53], ГОСТ 28147-89, IDEA [9, 14], FEAL [9, 14] киради.

**DES** IBM фирмасининг бутун бир криптографлари гуруҳи томонидан ишлаб чиқилган [9, 14]. Маълумотларни шифрлаш стандарти 1976 йил 23 ноябрда Миллий Стандартлар Бюроси томонидан АҚШнинг давлат стандарти сифатида қабул қилинган ва у 1977 йил июль ойидан 2000 йил октябрь ойигача рақамли маълумотларни шифрлаш учун стандарт бўлиб хизмат қилган. Ҳозирги вақтда у фақат назарий аҳамиятга эга. DES занжирсимон тузилмали мувозанатланган Фейстал тармоғи архитектурасига эга. Мутахассисларнинг фикрига кўра бу стандарт ёйиш ва аралаштириш тамойилларига асосланган энг яхши криптоалгоритмлардан биридир. Шифрлаш алгоритмида шифрматннинг ҳар бир бити дастлабки матн ва калит барча битларининг функцияси бўлади.

Стандартда ўрнига қўйиш, ўрин алмаштириш ва 2 модуль бўйича қўшиш амалларининг комбинациясидан фойдаланилади.

**ГОСТ 28147-89** - собиқ Совет Иттифоқида ишлаб чиқилган DES каби мувозанатланган Фейстал тармоғи архитектурали, *64*-бит блокли ва калит узунлиги *256* бит бўлган криптографик ўзгартириш алгоритмидир. Алгоритм босқичлари сони *32* га тенг бўлса-да, у DESга нисбатан тезкордир.

Шифрматнни дастлабки матнга ўгириш ҳам худди дастлабки матнни шифрматнга ўгириш каби бажарилади, фақат бунда калитлар кетма-кетлиги ўзгартирилади.

ГОСТ 28147-89да DES, AESга хос электрон код китоби маромига жуда ўхшаш оддий алмаштириш мароми, DES, AESга хос маромлардан бироз фарқли бўлган гаммалаштириш, тескари боғланишли гаммалаштириш маромлари ва улардан тамойилли фарқли имитоқистирма ишлаб бериш маромидан фойдаланади.

ГОСТ 28147-89 алгоритми DESга нисбатан анча юқори криптобардошлиликни таъминлайди. Бу кунгача у энг самарали ҳисобланган дифференциал ва чизиқли криптотаҳлил усулларига нисбатан етарли даражада криптобардошли саналадиган алгоритмлардан биридир. Бу асосан, DESга нисбатан узун, яъни *256* битли калитдан ва *S*-блокларга тегишли деярли *354* бит (*S*-блок генерацияловчилар ва фойдаланувчилар гуруҳидан ўзгалар учун) махфий маълумотдан фойдаланилиши билан изоҳланади.

**AES** алгоритмида кириш ва чиқиш блоклари узунлиги *128* бит шифрлаш калитининг узунлиги *128*, *192* ёки *256* бит этиб белгиланган.

Шифрлашда қўлланиладиган барча алмаштиришлар ёйилиш ва тарқалиш тамойилларини амалга оширишга қаратилган. Стандартда блок ва калитнинг узунлигига боғлиқ равишда босқич (раунд)лар сони *10* дан *14* гача белгилаб қўйилган.

Шифрлаш процедураси босқич калитларини генерациялаш процедурасини ҳам, босқичлар сонига мос узунликдаги шифрматнга ўгириш (дастлабки матнга ўгириш) учун босқич калитларини юклашни ҳам ўз ичига олади.

Шифрматнни дастлабки матнга ўгириш амалларни инверсия (тескари) тарзида бажариш орқали амалга оширилади.

Ҳозирги кунгача AES юқори криптобардошлиликка эга бўлган шифрлар қаторига киради.

**IDEA** – яна бир *64*-битли блокли шифрлаш алгоритми бўлиб, калитининг узунлиги *128* битга тенг. IDEA шифрининг биринчи варианти Ксуеджи Лай ва Джеймс Масси томонидан *1990* йилда таклиф этилган. У тезлиги бўйича DES алгоритмидан қолишмайди, криптотаҳлилга бардошлилиги жиҳатидан эса ундан ҳам устун.

IDEAда дастлабки матнни шифрматнга ўгириш ва шифрматнни дастлабки матнга ўгиришда ягона алгоритмдан фойдаланилади.

IDEA алгоритмида ҳам бошқа блокли шифрлаш алгоритмларидаги каби аралаштириш ва ёйиш тамойиллари етарли даражада амалга оширилган. Унинг асосида “турли алгебраик группаларнинг амалларини бирлаштириш” фалсафаси ётади. Унда уч алгебраик группа аралаштирилган ва уларнинг барчаси ҳам қурилма, ҳам дастур кўринишида осон амалга оширилади.

Шифрни очиш амали ҳам худди шифрлаш амали каби бажарилади, бунда фақат қисм калитлар бироз ўзгартирилади.

**FEAL** алгоритми япон мутахассислари Акихиро Шимузу ва Шоджи Миягучи томонидан таклиф этилган бўлиб, унда кириш ва чиқишда *64*-битли блоклардан ва *64*-битли калитдан фойдаланилади [9, 14]. Мақсад DESга нисбатан кучли алгоритм яратишдан иборат бўлган, лекин пировардида бу алгоритм бошланғич мақсаддан узоқлашиб кетган.

**FEAL** алгоритми дифференциал ва чизиқли криптотаҳлилга нисбатан етарли криптобардошлиликни таъминлай олмаганлиги маълум [9, 14]. Шу боис, у асосан криптотаҳлилчилар орасида машҳур, чунки кимда-ким янги криптотаҳлил усулини яратса, уни аввало **FEAL** алгоритми учун синаб кўриши одат тусига кирган.

**O‘z DSt 1105:2005** ва **O‘z DSt 1105:2009** «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Маълумотларни шифрлаш алгоритми» (МША) [51]да модуль арифметикасининг диаматрицалар алгебрасидан фойдаланилади, бунда ҳисоблашнинг қийинлик даражаси матрицалар алгебрасидаги сингари бажарилади [54-57].

Шифрматнга ўгириш ва дастлабки матнга ўгириш процедураларида фойдаланиладиган диаматрицалар алгебрасининг асосий амали диаматрицани *p* модуль бўйича тескарилаш амали ҳисобланади. Бу амалларда икки ўлчамли сеанс калити массивининг махсус тузилмали *4*х*4* тартибли квадрат диаматрица билан акс эттирилувчи қисмлари иштирок этади. Махсус тузилмали диаматрицанинг муҳим хоссаси диаматрицанинг диааниқловчисини ҳисоблаш формуласининг соддалигидир, бу эса диаматрицани тескарилаш шартларини текшириш ишларини соддалаштиради.

Махсус тузилмали диаматрицани тескарилаш шартларини текшириш МША параметрларига қўйиладиган асосий талаб ҳисобланади. МШАда, шунингдек бутун сонларни параметрли кўпайтириш, тескарилаш ва даражага ошириш деб аталган параметрли группа амалларидан ҳам фойдаланилади. МША белгилаб қўйилган икки хил - *256* ва *512* бит узунликдаги калитлар ёрдамида амалга оширилади.

Барча юқорида баён этилган ГОСТ 28147-89дан бошқа алгоритмлар бўйича маълумотларни шифрлашда 5 хил иш маромини қўллаш мумкин [52]: электрон код китоби (ECB); шифр блокларининг илашиши (CBC); чиқиш орқали тескари боғланиш (OFB); шифрматн орқали тескари боғланиш (тескари

боғланишли гаммалаштириш) (CFB); саноқчи (CTR). Табиийки, ҳар бир иш мароминиг ўзига хос афзаллиги ва камчилиги бўлади. Масалан, калитларни шифрлашда электрон код китоби иш маромини, алоҳида белгилар учун шифрматн орқали тескари боғланиш иш маромини, алоқа тизимида (одатда, бирор шифрматнни такрор узатиш имконияти бўлмаганда) чиқиш орқали тескари боғланиш иш маромини қўллаш қулай ҳисобланади.

### 4.1.2. Блокли симметрик шифрлаш алгоритмларини криптотаҳлиллашнинг замонавий усуллари

Қадимда мавжуд бўлган ва янгидан яратилган криптоалгоритмлар криптотаҳлили ҳар қачон долзарб бўлган, чунки алгоритмни бардошли ёки уни янгиси билан алмаштириш лозимлиги ҳақида ўз вақтида қарор қабул қилиш мумкин. Криптобардошлилиги паст бўлган криптоалгоритмларни аниқлаш учун эса, ҳар доим мавжуд криптотаҳлил усулларини такомиллаштириб, янгиларини яратиб бориш зарур. Ҳар бир янги яратилган криптотаҳлил усули у қўлланилиши мумкин бўлган шифрларни қайта кўриб чиқишни тақозо этади.

Симметрик шифр криптобардошлилигини баҳолаш унинг ҳозирги кунда энг самарали деб тан олинган криптотаҳлил усулига нисбатан унинг криптобардошлилигини аниқлаш демакдир. Бунда криптотаҳлилчи ихтиёрида шифрлаш калитидан бошқа барча зарур бўлган ахборот бор деб қаралади, яъни етарли ҳажмда дастлабки матнга оид шифрматнлар берилган бўлади.

Симметрик шифрлаш криптомодулларига нисбатан энг самарали деб тан олинган криптотаҳлил усуллари сирасига ҳозирги кунда статистик криптотаҳлил, чизиқли криптотаҳлил, дифференциал криптотаҳлил [1, 6] ва уларнинг композициялари киради. Бу усуллар шифрга кўпол куч усулида ҳужум уюштиришга нисбатан анча кам амаллар билан калит топишга имкон беради.

### 4.2. Статистик усул

Дастлабки ва шифрланган хабарларнинг статистик қонуниятларини ўрганиш асосида криптотизимларни бузиш имкониятини тадқиқ қиладиган криптотаҳлил тури статистик усул деб аталади [11].

Статистик криптотаҳлилнинг вазифаси махфий калит (ёки калит қисми) $k \in Z_2^n$ ни аниқлаш алгоритмини яратишдан иборат. Блокли шифрлар учун статистик усулнинг таянч принциплари ва тушунчаларини кўриб чиқамиз.

Бир қатор блокли шифрлар учун криптотаҳлил статистик усулининг амалга оширилиши тўлиқ танлаш усулида баҳолашидан яхши бўлган махфий калитни топиш алгоритмлари самарадорлигини баҳолаш имконини беради. Алгоритм кириши бўлиб $k$ калит билан $F$ акслантиришини қўллаш натижасида олинган, очиқ ва шифрланган матнлар – $(X_i, Y_i), i=1,\ldots, N$ сонлар жуфтлиги ҳисобланади. Бундай жуфтликларни *материаллар* деб атаймиз ва $M$ ҳарфи билан белгилаймиз. Материал миқдори (ҳажми ) жуфтликлар сонига мос бўлиб $(X_i, Y_i)$: $|M| = N$ га тенг. $X_i, i=1,\ldots, N$ очиқ матн $Z_2^m$ майдондан эҳтимолий ва мустақил ҳолда тасодифий танланган деб қаралади.

Мумкин бўлган тасодифий кузатишлар бўйича махфий параметрни топишга мўлжалланган *статистик таснифлаш процедураси* (СТП) статистик усул таҳлилининг муҳим қисми бўлиб ҳисобланади. Кузатиш учун эҳтимоллик тақсимоти функцияси ушбу параметрга боғлиқ. СТП вазифаси шундан иборатки, агарда ушбу эҳтимоллик тақсимотлари ҳар хил бўлса, у ҳолда етарли даражадаги кузатишларда маълум миқдордаги ишонч билан кузатишлар тақсимоти қонунини аниқлаш мумкин, у эса топилиши керак бўлган номаълум параметрдир.

Мумкин бўлган тасодифий кузатишлар $M$ материал, калитнинг бир қисми ёки калит битларининг баъзи чизиқли комбинацияси номаълум параметр бўлсин. Номаълум параметр бевосита қиймат қабул қилувчи тўпламни $\Gamma$, $|\Gamma| = s \leq 2^n$ деб белгилаймиз.

Ҳар бир СТП бутун майдонининг $T>1$ кесишмайдиган соҳаларини аниқлайди:

$M = M_1 U M_2 U \dots M_T$; $M_i \cap M_j \neq \emptyset$, *бу ерда* $i \neq j$, $i,j \in \{1, \dots, T\}$.

$i \in \{1, \dots, T\}$ $M_i$ соҳа *қарор қабул қилиш соҳаси* дейилади. Бунда берилган кузатиш $m \in M$ учун тартиб рақами $i(m)$ ни аниқлаш алгоритми мураккаблиги паст ҳисобланади. Барча соҳа $M_i$ учун СТП $\Gamma$: $\gamma_{i,1}, \gamma_{i,1}, \dots \gamma_{i,s}$ тўплам элементлари миқдори (ҳажмини) $s`$ $(1 \leq s` \leq s)$нинг тартибланган рўйхатини ҳам аниқлайди, бу ерда $j_1 \neq j_2$ бўлганда $\gamma_{i,j1} \neq \gamma_{i,j2}$.

$\Gamma$ тўпламдан номаълум параметрни аниқлаш учун қуйидаги амаллар бажарилади. Дастлаб олинган кузатиш $m \in M$ бўйича қарор қабул қилиш соҳаси тартиб рақами $i(m)$ аниқланади. Кейинчалик навбатма-навбат $\Gamma$: $\gamma_{i(m),1}$, $\gamma_{i(m),1}$, … $\gamma_{i(m),s`}$ тўпламдан параметрлар саралаб олинади ва $j$-параметр $(j = 1 \div s`)$ қиймати изланган нарсами йўқми текшириб кўрилади. Текшириш алгоритми икки босқичдан иборат:

1. Калитнинг қолган қисмларини аниқлаб олиш;

2. Калит тўғри топилдими йўқми текшириб кўриш.

Агар номаълум параметр сифатида бутун калит қаралса, биринчи қадам бажарилмайди. Бу ҳолда $\Gamma = Z_2^n$. Калитнинг қолган қисмини аниқлаш учун калитнинг қолган барча номаълум битларини тўлиқ танлашдан фойдаланилади. Агар параметр сифатида калит қисми ёки калит битлари бузилган чизиқли комбинацияси қаралса ва $\Gamma = Z_2^{n^*}$, $1 \leq n^* \leq n$ бўлса, $2^{n-n^*}$ вариантни танлаб текширишга тўғри келади.

Калит тўғри аниқланганми йўқми қуйидаги тарзда текширилади: $M$ материалдан очиқ ва шифрланган матн $(X_i, Y_i) \in M$, $X_i, Y_i \in Z_2^m$, $i \in \{1, \dots, N\}$ жуфтлик учун қуйидаги муносабат текширилади: $F(X_i, k^*) = Y_i$, бу ерда $K^* \in Z$ – бутун калитнинг синаб кўрилган варианти. Сохта калит дастлабки қадамларданоқ маълум бўлади. Бунда $d$ та дастлабки очиқ ва шифрланган матнлар жуфтлиги учун текширишни амалга ошириш етарли, бу ерда $d$ шундай

сонки $d$ та турли очиқ матнлар $X_i$, $i = 1, ..., d$ дан исталган тўплами ва ҳамда исталган иккита турли калит $k_1 \neq k_2$ учун шундай тартиб рақами $j \in \{1, ..., d\}$ топиладики бунда $F(X_j, k_1) \neq F(X_j, k_2)$ (ушбу шартни қаноатлантирувчи минимал $d_0$ *F шифрнинг ягоналик (ёлғизлик) масофаси* дейилади) бўлади.

Калитни топиш алгоритмлари учта параметр бўйича таққосланади: $N$ – фойдаланиладиган материал миқдори (ҳажми), $Q_0$ – алгоритм бажарган ишининг ўртача қийинлиги ва $\pi_0$ – алгоритм ишончлилиги. $Q_0$ ва $\pi_0$ қандай очиқ матн ва зарур калит тасодифий танланганлигига боғлиқ. Алгоритм бажарган ишининг қийинлиги очиқ матнни тасодифий танлашдаги ва тасодифий, эҳтимолий ҳамда очиқ матндан мустақил равишда калитни танлашдаги математик кутиладиган қадамлар сонига мос келади. Алгоритм ишончлилиги калит $Z_2^n$ майдондан тасодифий, эҳтимолий ва очиқ матндан мустақил равишда танлангандаги процедуранинг кутилгандагидек тўғри натижа бериши эҳтимоллигининг математик кутилишига тенг. $Q_0$ ва $\pi_0$ параметрлар ўртасида қуйидаги тўғри боғланиш мавжуд: ишончлилик қанча юқори бўлса, шунчалик кўп қийинчилик пайдо бўлади ва аксинча.

### 4.3. Дифференциал криптотаҳлил усули

Дифференциал криптотаҳлил усули 1990 йили Исроиллик математиклар Эли Бихам ва Ади Шамир [1, 6, 14] томонидан таклиф этилган. *Дифференциал криптотаҳлил усули* битта калит билан шифрланган, танланган икки очиқ матн ўртасидаги фарқларни криптотаҳлил қилишга асосланган криптотаҳлил усули бўлиб, шифрланган матн ўзгаришининг дастлабки матн ўзгаришига боғлиқлигини таҳлил қилишга асосланган. Бу усулдан фойдаланилса, маълум дастлабки матнга оид шифрматнлар берилганда ҳам, танланган дастлабки матнга оид шифрматнлар берилганда ҳам блокли шифрлаш калитини топиш мумкин. Таҳлилда ҳар бир раундда ўз шифрлаш калитидан фойдаланилади деб қаралади. $r$-раундли шифрларни муваффақиятли очиш $(r-1)$–раунд

дифференциалларининг мавжудлигига боғлиқ бўлиб, уларнинг мавжудлик эҳтимоллиги юқори бўлганда криптотаҳлил муваффақиятли кечади.

Дифференциал криптотаҳлил усули икки шифрматн фарқининг икки дастлабки фарқидан боғлиқ эканлигига асосланади.

Фараз қилайлик, шифрлаш алгоритмида иккита дастлабки матн $n$ ўлчамли вектор $X'$ ва $X''$ бўлиб, уларнинг чиқишида $n$ ўлчамли векторлар $Y'$ ва $Y''$ бўлсин. Кириш қийматлари фарқи $\nabla X = X' \oplus X''$, чиқиш қийматлари фарқи $\nabla Y = Y' \oplus Y''$ бўлади, бунда $\oplus$ - векторлар устида **XOR** амалидир. Идеал шифр учун бирор чиқиш фарқи $\nabla Y$ алгоритм чиқишида киришдаги $\nabla X$ учун ҳосил бўлиш эҳтимоллиги $2^{-n}$ га тенгдир. Дифференциал криптотаҳлил $\nabla X$ учун чиқишда $\nabla Y$ ҳосил бўлиш эҳтимоллиги $2^{-n}$ га тенг эҳтимолликдан оғишдан фойдаланилади. Бирор бир киришдаги $(\nabla X, \nabla Y)$ жуфтлик дифференциал деб аталади. Назарий эҳтимоллик $2^{-n}$ дан етарлича катта эҳтимоллик оғиши юз берганда, шифрлаш алгоритмининг $r$-$1$ раунди учун етарли юқори эҳтимоллик билан дифференциал модель тузиш имконияти туғилади. Бу шифрлаш алгоритмининг охирги раундига оид калит қисмини топишга йўналтирилган ҳужумни амалга ошириш имконини беради. Бундай ҳужум механизми чизиқли ҳужумга ўхшаб кетади.

$r$-раундли шифрни дифференциал криптотаҳлиллаш процедураси қуйидаги қадамларни ўз ичига олади [14-16]:

1. Олдиндан бажариб қўйиладиган ҳисоблашлар босқичида $r$-раундли дифференциаллар тўплами $\{(\nabla X_1, \nabla Y_1)_{r-1}, (\nabla X_2, \nabla Y_2)_{r-1}, \ldots, (\nabla X_s, \nabla Y_s)_{r-1}\}$ тузилади ва улар эҳтимоллик қийматлари бўйича тартибга солинади.

2. Ихтиёрий дастлабки матн $X$ олиниб, шундай $X^*$ ҳисобландики, $X$ ва $X^*$ фарқи $\nabla X_1$ бўлсин. $X$ ва $X^*$ ҳақиқий калит билан шифрланиб, $r$-рауннддан сўнг $y(r)$, $y^*(r)$ ҳосил қилинади. $r$-$1$ – раунд чиқишида шифрматнлар фарқи энг юқори эҳтимоллик билан $\nabla y(r-1) = \nabla_1$ га тенг деб тахмин қилинади. $(\nabla y(r-1),$

*y(r), y*(r))* учлиги учун ҳар бир мумкин бўлган охирги раунд учун калит қисми $k_r$ топилади ва $k_r$ ни юзага чиқишлар сони орттириб қўйилади.

3. 2 қадам токи битта ёки бир неча калит қисми $k_r$ ечим сифатида қабул этилади.

4. 1-3–қадамлар *r-1*-раунд учун такрорланади. *y(r-1)* шифрматнларни дастлабки матнга ўгириш охирги раунд калит қисми $k_r$ асосида амалга оширилади. Бундан сўнг ҳар бир раунд учун калитлар очиб ташланмагунча юқоридагиларга ўхшаш амаллар бажарилади.

Дастлаб муайян шифр криптотаҳлили учун таклиф этилган дифференциал криптотаҳлил усули ҳозирги кунда Марков шифрлари оиласи учун фойдаланиши мумкин эканлиги маълум бўлди. Марков шифри, шундай шифрки, унда ҳар бир раунд шифрлаш тенгламаси учун дифференциал эҳтимоллиги дастлабки матнларни танлашга боғлиқ эмас. Унда, агар раундлар қисм калитлари ўзаро мустақил бўлса, ҳар бир раунддан сўнг ҳосил бўладиган фарқлар кетма-кетлигида кейинги фарқ фақат олдинги фарқ билан аниқланадиган Марков занжирини ҳосил этади. Дифференциал криптотаҳлилнинг ўзига хос томони шундаки, у фақатгина дифференциаллар эҳтимолликлари тақсимотига асосланган бўлиб, унда шифрнинг алгебраик хоссаларидан фойдаланилмайди.

Дифференциал модель тузиш шифрнинг чизиқсиз компоненти учун юқори эҳтимолликка эга бўлган дифференциаллардан фойдаланишга асосланган. Процедуранинг 1-қадамига тегишли барча мумкин бўлган дифференциаллар эҳтимоллиги ҳақида ахборот фарқлаш тақсимоти жадвали орқали берилади. Жадвал ҳам аввалги жадвалга ўхшаш бўлиб, унинг биринчи устунида барча мумкин бўлган $\nabla x$ лар, биринчи сатрда мумкин бўлган $\nabla y$ лар келтирилган. Мос келувчи дифференциал эҳтимоллиги катак элементини $2^n$ га бўлиб топилади, бу ерда *n*-*S*-блок ўлчамлари. Жадвал таҳлили юқори эҳтимолликка эга бўлган дифференциалларнинг йўқлигини, бу эса

алгоритмнинг яхши дифференциал моделини тузишга имкон бермаслигини кўрсатади.

Дифференциалларнинг энг юқори эҳтимоллиги 24 катакда қатнашган *4/16* га тенг ва *72* катакда қатнашган *2/16* га тенг. Бинобарин, бу алгоритм *S*-блоки энг юқори даражага яқин қилиб оптималлаштирилганлигини кўрсатади. Бизга маълумки, бундай *S*-блокли алгоритмга чизиқли ёки дифференциал ҳужум муваффақиятсиз чиқади. [48, 58]да чизиқли ва дифференциал криптотаҳлил асосида янада муваффақиятли ҳужумларни амалга ошириш учун ўзаро боғланган *S*-блоклар тўпламидан фойдаланиш усули келтирилган.

### 4.4. Чизиқли криптотаҳлил усули

Чизиқли криптотаҳлил усули Мицуру Мацуи [1, 14] томонидан таклиф этилган бўлиб, унда блокли шифр алгоритмининг криптотаҳлиллаш моделини тузишда чизиқли яқинлашишдан фойдаланилади. Дастлабки ва шифрланган матн ўртасидаги чизиқли аппроксимацияни излашга асосланган бундай криптотаҳлил усули *чизиқли криптотаҳлил усули* деб аталади.

Чизиқли криптотаҳлил аслида дастлабки матн битлари $X_i$ ва шифрматн битлари $Y_j$ дан таркиб топган

$$X_{i1} \oplus X_{i2} \oplus \ldots X_{ir} \oplus Y_{j1} \oplus Y_{j2} \oplus \ldots Y_{js} = 0, \qquad (1)$$

шаклдаги чизиқли ифодаларни топишга асосланган. Бу ифодалар блокли шифрлаш алгоритмининг чизиқсиз шифр компонентасига барча мумкин бўлган киришлар учун *1/2* дан энг юқори эҳтимоллик билан фарқ қилиши мумкин бўлган эҳтимоллик билан кучга эгадир. Ушбу ифоданинг бажарилиш эҳтимоллиги *1* дан фарқ қилувчи абсолют қиймати $|1/2-p|$ «чизиқли ифода кучга эга бўлиш эҳтимоллигининг *1/2* дан оғиши» деб ёки қисқача «эҳтимолликнинг оғиши» деб аталади. Бу ерда $p$ – эҳтимоллик.

Бунинг маъноси шуки, агар очиқ матннинг баъзи битлари, сўнгра шифр матннинг баъзи битлари устида, сўнгра уларнинг натижавий битлари устида *2*

модули бўйича қўшиш **(XOR)** амали бажарилса, шундай бит ҳосил қилинадики, у калитнинг баъзи битлари устида **XOR** амали натижасини беради. Бу бирор бир *p* эҳтимоллик билан тўғри бўлган чизиқли яқинлашиш деб аталади. Агар $p \neq 1/2$ бўлса, у ҳолда бундай эҳтимоллик оғишидан криптотаҳлилда фойдаланиш мумкин. Дастлабки матнлар ва уларга тегишли шифрматнларнинг жамламасидан калит бити қиймати тўғрисида башорат қилиш учун фойдаланилади. Маълумотлар қанчалик кўп бўлса, башорат ҳам шунчалик тўғри бўлади. Эҳтимоллик оғиши қанча юқори бўлса, шифрни очишда шунчалик тез муваффақиятга эришилади.

Бунда аҳамиятли маълумотлар симметрик шифрларда қўлланиладиган *4, 8* ёки ундан кўп битли алмаштириш блоклари тузиш рол ўйнайди. Чизиқли яқинлашишни аниқлаш эҳтимоллик оғиши жадвалларидан фойдаланилади.

Катта ҳажмдаги дастлабки матн/шифрматн жуфтликлари билан калит битлари орасидаги муносабатни тушунтиришда (1) ўрнига қуйидаги кўринишдаги чизиқли яқинлашиш ифодаси қўл келади.

$$X_{i1} \oplus X_{i2} \oplus \ldots X_{ir} \oplus Y_{j1} \oplus Y_{j2} \oplus \ldots Y_{js} = Z_{k1} \oplus Z_{k2} \oplus \ldots Z_{kt}, \qquad (2)$$

Агар $|1/2 - p|$ етарлича катта ва криптотаҳлилчига етарли миқдорда дастлабки ва унга тегишли шифрматн жуфтликлари сони маълум бўлса, унда ифоданинг ўнг томонида тегишли позициядаги калит битларини *2* модули бўйича йиғиндиси (қисқача, йиғиндиси) дастлабки ва шифрматнлар битларининг тегишли позицияларга муносиб позициялардаги битларининг йиғиндисига тенг [58].

Агар $p > 1/2$ бўлса, унда (2) ифода ўнг тарафидаги калит битларининг йиғиндиси *0* га тенг, агарда ифоданинг чап қисмига тегишли битлар йиғиндиси *0* га тенг бўлган ҳоллари дастлабки матн шифрматнлар шифрлар сонининг ярмидан кўп бўлса, шунингдек, ифоданинг ўнг тарафидаги калит битлари йиғиндиси *1* га тенг, агар ифоданинг ўнг тарафидаги калит битлари йиғиндиси *1* га тенг бўлган ҳоллари матнлар сони ярмидан кўп бўлса.

Агар $p<1/2$ бўлса, бунинг тескариси бўлади. Ифоданинг ўнг тарафидаги калит битларининг йиғиндиси *0* га тенг, агарда ифоданинг чап қисмига тегишли битлар йиғиндиси *1* га тенглик ҳоллари дастлабки матн/шифрматн жуфтликлари сонининг ярмидан кўп бўлса, шунингдек, ифоданинг ўнг тарафидаги калит битлари йиғиндиси *1* га тенг, агар ифоданинг чап тарафидаги битлар йиғиндиси *0* га тенг бўлган ҳоллари матнлар сони ярмидан кўп бўлса.

Калитнинг ҳар бир битини топиш учун бундан сўнг мазкур битларни маълум комбинациялари учун чизиқли тенгламалар системасини ечиш кифоя. Бу системани ечиш мураккаблиги 3-даражадан юқори бўлмаган калит узунлигидан тузилган полином билан ифодаланади.

Чизиқли ифодаларни топиш ва *S*-блокларнинг чизиқли хоссаларини таҳлил этиш учун чизиқли эҳтимолликлар оғиши бўйича олинган маълумотлар асосида чизиқли яқинлашиш (аппроксимация) жадвали тузилади. Қуйида бундай жадвал АҚШ давлат стандарти AESни қабул қилиш жараёнида ўтказилган конкурсда иккинчи ўринни эгаллаган Буюк Британия, Исроил, Норвегия криптологлари томонидан таклиф этилган Serpent [58] учун келтирилган. Бу мисолни [58] да келтиришга сабаб муаллифлар таркибида дифференциал криптотаҳлил усулини яратган Эли Бихам ва бошқа машҳур криптотаҳлилчилар Даниялик олим Ларс Кнудсен, инглиз олими Росс Андерсон қатнашганидир. Чунки, яхши шифрни кучли криптотаҳлилчилар яратиши эҳтимоллиги юқори бўлади. Қуйидаги 9-жадвалда чизиқли ифода (1) учун барча мумкин бўлган эҳтимоллик оғиши келтирилган. Унда биринчи устун чизиқли ифодада қатнашадиган кириш битларини, биринчи сатр – унда қатнашадиган чиқиш битларини ифодалайди.

9-жадвал катакларида чизиқли ифода кучга эга бўлган ҳоллар сони келтирилган. Шунинг учун, эҳтимоллик оғиши қиймати, катак қийматини $2^n$ га бўлиб топилади, бунда $n$ - *S*-блокнинг ўлчами $(n=4)$. Раундлар ва ҳар бир *S*-блокка тузилган бундай жадвални тузиш ва сақлаш учун $2^{2n}$ хотира ячейкаси

талаб этилади. Келтирилган жадвалда эҳтимоллик оғишининг *16/2* га тенг қиймати олинган катаклар сони *96* та, *16/4* эҳтимоллик оғган катаклар сони *36* та. Бу аслида берилган *S*-узел учун энг яхши характеристикадир. Жадвалдан энг кўп эҳтимоллик оғишига тааллуқли чизиқли ифодалар асосида *r* раундли алгоритмнинг *r-1* раунди учун чизиқли модель тузилади. Бундай модель дастлабки матн битлари ва охиридан аввалги раундда чиқиш битлари қатнашган чизиқли ифодалар эҳтимоллиги оғишини башорат қилишга имкон беради. Бу эса тўла танлаш усули бўйича *r-1* раунд учун калит қисмини топишга олиб келади. Чизиқли модель эҳтимоллиги *1/2* дан қанчалик оз оғса, шифрга ҳужум қилиш учун шунчалик кўп дастлабки матн ва шифрматн жуфтлари зарур бўлади.

Бошланғич ва якуний ўрин алмаштириш қаралмайди, чунки улар шифрни очишга таъсир этмайди.

Тажрибалар шуни кўрсатдики [58] 16 босқичли DESнинг калитини топиш учун ўртача $2^{43}$ очиқ матн/шифрматн жуфтидан фойдаланилган. Бундай шифр очиш дастурий таъминоти билан 12 та HP 9735 иш станциясидан фойдаланиб, DES калити 50 кунда очилган.

Чизиқли криптотаҳлил *S*-блокларнинг структурасига жуда ҳам боғлиқ, аммо DES *S*-блоклари чизиқли криптотаҳлилга қарши оптималлаштирилмаган. DES муаллифларидан бири Дон Копперсмитнинг сўзига қараганда чизиқли криптотаҳлилга бардошлилик «DESни лойиҳалашда зарур бўлган тамойиллар қаторига киритилмаган».

Шуни эътиборга олган ҳолда, DESни Ўзбекистон Республикасида соф ҳолда бундан буён фойдаланиш мақсадга мувофиқ эмас. ГОСТ 28147-89 чизиқли криптотаҳлилга бардошли ҳисобланади.

9-жадвал

**Serpent алгоритмининг 4 битли 1-5 – блокининг чизиқли яқинлашуви**

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | a | b | c | d | e | f |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | -2 | -2 | 0 | -2 | 0 | 0 | -2 | 0 | -2 | 2 | 4 | -2 | 0 | -4 | 2 |
| 2 | 0 | 2 | -2 | 0 | 0 | 2 | 2 | 4 | 0 | -2 | -2 | 4 | 0 | -2 | 2 | 0 |
| 3 | 0 | 0 | -4 | 0 | 2 | -2 | -2 | -2 | 0 | -4 | 0 | 0 | 2 | 2 | 2 | -2 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | -4 | -4 | -4 |
| 5 | 0 | 2 | -2 | 4 | -2 | -4 | 0 | 2 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 2 |
| 6 | 0 | -2 | 2 | 0 | 0 | -2 | -2 | 4 | -4 | -2 | -2 | 0 | 0 | 2 | -2 | 0 |
| 7 | 0 | 0 | 0 | -4 | 2 | -2 | 2 | 2 | 4 | 0 | 0 | 0 | 2 | 2 | -2 | 2 |
| 8 | 0 | -2 | -2 | 0 | 2 | 0 | 0 | 2 | 0 | -2 | 2 | -4 | -2 | -4 | 0 | 2 |
| 9 | 0 | 0 | 0 | 0 | 0 | 4 | -4 | 0 | 0 | 0 | 0 | -0 | 4 | 0 | 0 | 4 |
| a | 0 | 4 | 0 | 0 | 2 | -2 | -2 | -2 | 0 | 0 | -4 | 0 | -2 | -2 | -2 | 2 |
| b | 0 | -2 | 2 | 0 | 4 | -2 | -2 | 0 | 0 | 2 | 2 | 4 | 0 | -2 | 2 | 0 |
| c | 0 | -2 | 2 | 4 | 2 | 0 | 4 | -2 | 0 | -2 | -2 | 0 | 2 | 0 | 0 | 2 |
| d | 0 | -4 | -4 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | -4 | 0 | 0 | 0 | 0 | 0 |
| e | 0 | 0 | 0 | 4 | 2 | 2 | -2 | 2 | 4 | 0 | 0 | 0 | -2 | 2 | -2 | -2 |
| f | 0 | -2 | 2 | 0 | -4 | -2 | -2 | 0 | 4 | -2 | -2 | 0 | 0 | -2 | 2 | 0 |

### 4.5. Симметрик шифрлаш алгоритмларининг криптографик хоссалари таҳлилида Буль функцияларидан фойдаланиш

Криптограф криптотизим яратишда зарурий бардошлиликни таъмин этувчи тамойиллар, криптографик хоссалар, шартлар ва мезонларни имкон

борича эътиборга олиши зарур. Шу асосда криптограф криптотизимнинг зарурий бардошлиги таъминланганлигига ишонч ҳосил этади.

Криптотаҳлилчи берилган криптотизим алгоритмини таҳлиллашга киришишдан олдин унда ишлатилган акслантиришлар мажмуида бардошлилиликни таъмин этишга йўналтирилган қандай тамойиллар, криптографик хоссалар, шартлар ва мезонлар қай даражада эътиборга олинганини таҳлилдан ўтказиши лозим**.** Шунга боғлиқ тарзда криптотаҳлилчи шифрлаш тизимининг заиф жойларини башорат қилиб, уларга ҳужум уюштиришни мўлжалга олади. Шу боис шифрлаш алгоритмлари акслантиришларининг криптографик хусусиятларини билиш криптограф учун ҳам криптотаҳлилчилар учун ҳам муҳимдир. Қуйида шу ҳақида сўз боради [23, 59].

### 4.5.1. Симметрик шифрлаш алгоритмлари акслантиришлари

Блокли ва оқимли шифрлаш алгоритмларининг барчасига хос бўлган акслантириш – бу Буль функция (БФ)ларидир [23, 59]. Шифрлаш алгоритмлари акслантиришларини умумий ҳолда $GF(2)^n = \{x = (x_1, x_2, ..., x_n) \in X : x_i \in \{0;1\}\}$ – фазо элементларини бирор амал ёки амалларнинг чекли сондаги кетма-кетлиги орқали бошқа $GF(2)^m = \{y = (y_1, y_2, ..., y_m) \in Y : y_i \in \{0;1\}\}$ – фазо элеменларига алмаштириш деб қараш мумкин ва у БФлари кўринишида қуйидагича ифодаланади:

$$Y = F(X) \ : \ GF(2)^n \to GF(2)^m .$$

Бу акслантириш ифодасидаги вектор-функция ушбу $F(X) = \{y_1, y_2, ..., y_m\} = \{f_1(X), f_2(X), ..., f_m(X)\}$ кўринишида тасвирланади, бу ерда барча $i \in \{1, ..., m\}$ учун $y_i = f_i(X)$, $X \in GF(2)^n$ $y_i \in GF(2)$ ва $f_i(X)$ функциялар $Y = F(X)$ ни *шакллантирувчи БФ*лар деб аталади.

Акслантиришларнинг криптографик хусусиятлари очиқ маълумот блоки элементлари, калит (махфий параметр) ва оралиқ алмаштиришлар натижалари блоки элементлари устида бажарилиши керак бўлган амаллар, жадваллар, тенглик, тенгсизлик ҳамда тегишлилик муносабатлари билан ифодаловчи математик моделнинг чинлик жадвали асосида қурилган унга мос келувчи БФ хоссалари орқали ўрганилади.

БФлар ифодалари учун Жегалкин полиномидаги қўшилувчилар ёки алгебраик нормал форма (АНФ) деб аталувчи қуйидаги

$$f_{АНФ}(X) = a_0 \oplus \left( \bigoplus_{1 \le i \le n} a_i x_i \right) \oplus \left( \bigoplus_{1 \le i < j \le n} a_{ij} x_i x_j \right) \oplus \ldots \oplus a_{12\ldots n} x_1 x_2 \ldots x_n ,$$

кўринишдан фойдаланилади, бу ерда $X \in GF(2)^n$ ва коэффициент $a \in GF(2)$. Шундай қилиб, БФ нинг $GF(2)^n$ - майдондаги АНФ ифодалари деганда $x_1, x_2, \ldots, x_n$-ўзгарувчиларнинг барча мумкин бўлган кўпайтмаларини мос коэффициентлари $a \in GF(2)$ билан биргаликдаги ҳадларининг $\oplus$-амали орқали йиғиндиси тушунилади. .

Берилган $f(x)$ БФнинг АНФ ифодасида қўшилувчиларнинг энг кўп ўзгарувчилар қатнашган кўпайтмасидаги ўзгарувчилар сони бу функциянинг алгебраик *даражаси* дейилади ва $\deg(f)$ деб белгиланади.

$GF(2)^n$-фазода аниқланган бирор $f(X) \in GF(2)$ функциянинг $\alpha$-векторга (бу ерда $X, \alpha \in GF(2)^n$) нисбатан Уолш-Адамар акслантириши (УАА) деб $GF(2)^n$- фазо элементларини $Z$-ҳақиқий сонлар тўпламида акслантирувчи ушбу чизиқли акслантиришга айтилади:

$$U_\alpha(f) = \sum_{X \in GF(2)^n} f(X)(-1)^{<\alpha, X>} ,$$

бу ерда “< >” – скаляр кўпайтма белгиси, яъни $<\alpha, X> = \alpha_1 x_1 \oplus \alpha_2 x_2 \oplus \ldots \oplus \alpha_n x_n$.

Тушунарлики, $U_\alpha(f): GF(2)^n \to Z$ - акслантириш унинг ифодасидаги $f$-функцияга нисбатан чизиқлидир, яъни

$$U_\alpha(af_1 + bf_2) = a \sum_{X \in GF(2)^n} f_1(X)(-1)^{<\alpha, X>} + b \sum_{X \in GF(2)^n} f_2(X)(-1)^{<\alpha, X>} \quad .$$

$GF(2)^n$-фазо элементларини *{-1; 1}* тўплам элементларига акслантирувчи ушбу функция $\hat{f}(X)=(-1)^{f(X)}$ берилган $f$- функцияга қўшма функция дейилади ва унинг УАА деб қуйидагига айтилади:

$$\hat{U}_\alpha(f) = \sum_{X \in GF(2)^n} (-1)^{f(X)}(-1)^{<\alpha, X>} = \sum_{X \in GF(2)^n} (-1)^{f(X) \oplus <\alpha, X>} .$$

Берилган $f: GF(2)^n \to GF(2)$- БФнинг чинлик жадвалини $S(f)$, скаляр кўпайтма билан аниқланган $<\alpha, X>$- функциянинг чинлик жадвали $\hat{S}(\langle \alpha, X \rangle)$ деб белгиланади. У ҳолда қуйидаги тенгликлар ўринли:

$$U_\alpha(f) = \left\langle S(f), \hat{S}(\langle \alpha, X \rangle) \right\rangle \text{ ва } \hat{U}_\alpha(f) = \left\langle \hat{S}(f), \hat{S}(\langle \alpha, X \rangle) \right\rangle,$$

ҳамда

$$\hat{U}_\alpha(f) = -2U_\alpha(f) + 2^n \delta(\alpha) \text{ ва } U_\alpha(f) = -\frac{1}{2}\hat{U}_\alpha(f) + 2^{n-1}\delta(\alpha),$$

бу ерда $\delta(\alpha) = \begin{cases} 1, \text{агарда } \alpha = (0,0,...,0) \\ 0, \text{агарда } \alpha \neq (0,0,...,0). \end{cases}$

УААга тескари акслантириш

$$f(X) = \frac{1}{2^n} \sum_{X \in GF(2)^n} U_\alpha(f)(-1)^{\langle \alpha, X \rangle} \quad \text{ва} \quad \hat{f}(X) = \frac{1}{2^n} \sum_{X \in GF(2)^n} \hat{U}_\alpha(f)(-1)^{\langle \alpha, X \rangle},$$

тенгликлар билан аниқланади.

### 4.5.2. Мувозанатлашганлик ва мунтазамлик хоссалари

Криптографик акслантиришларга мос келувчи БФларининг *мувозанатлашганлик* (*баланслашганлик*) ва *мунтазамлик (регулярлик)* шартларини қаноатлантиришини таъминлаш масаласини ечиш уларнинг

криптобардошлилиги билан боғлиқ бўлган муҳим талаблардан ҳисобланади. Блокли шифрлаш алгоритмлари акслантиришлари криптографик хоссаларини таҳлил қилишда, уларга мос келувчи БФларини қуриб, уларнинг *мувозанатлашганлик* ва *мунтазамлик* хоссаларига эгалигини таъминлаш блокли шифрлар криптобардошли акслантиришларини яратиш имконини беради [23, 59].

**1-таъриф.** Берилган $f(X)$ БФ *мувозанатлашган* дейилади, агар унинг чинлик жадвалида *"0"* ва *"1"* лар сони тенг бўлса, яъни ушбу муносабат

$$\#\{X \mid f(X)=0\} = \#\{X \mid f(X)=1\} = 2^{n-1}$$

ўринли бўлса.

**2-таъриф.** $Y = f(X): GF(2)^n \to GF(2)^m$ , $n \geq m$, акслантириш *мунтазам* дейилади, агар $X \in GF(2)^n$-элементларнинг барча $2^n$ та ҳар хил қийматларида $Y$ – функция ўзининг $GF(2)^m$-майдондаги $2^m$ та ҳар хил қийматларини роппа-роса $2^{n-m}$ мартадан қабул қилса.

Бу таърифдан қуйидаги тасдиқ келиб чиқади.

**1-тасдиқ.** Агарда $Y = f(X): GF(2)^n \to GF(2)^m$ - акслантиришда $n = m$ бўлиб, у *мунтазамлик* шартини қаноатлантирса, у биектив акслантириш бўлади, яъни бу функция ва унга тескари бўлган функция ўзаро бир қийматлилик хоссасига эга бўлади.

БФнинг мунтазам бўлишининг зарурий шарти қуйидаги тасдиқда ифодаланган.

**2-тасдиқ.** $F(X)=\{f_1(X), f_2(X),..., f_m(X)\}$ - векторнинг барча чизиқли комбинациялари мувозанатлашган бўлса, $Y = F(X): GF(2)^n \to GF(2)^m$-акслантириш $n \geq m$ бўлганда мунтазамлик шартини бажаради, яъни барча $\alpha = (\alpha_1, \alpha_2, ..., \alpha_m) \in GF(2^m)$ учун йиғинди $\sum_{i=1}^{m} \alpha_i f_i(x)$ - мувозанатлашган БФ.

1-таърифдан келиб чиқадики, УАА $\alpha=(0,0,...,0)$ нуқтада $f(X)$ БФнинг мувозанатлашганликдан четлашганлик даражасини кўрсатади, бунда мувозанатлашганлик шарти қуйидагича ифодаланади:

$$U_0(f)=2^{n-1} \quad \text{ва} \quad \hat{U}_0(f)=0.$$

***Мисол.*** БФ $f(X)=x_1x_2\oplus x_3x_4\oplus x_5x_6$ (бу ерда $X=(x_1,x_2,...,x_6)\in GF(2)^6$) мувозанатлашмаган, ҳақиқатан ҳам бевосита ҳисоблаш билан ишонч ҳосил қилиш мумкинки, $\alpha=(0,0,...,0)=0$ нуқтада $\hat{U}_0(f)=8$. Бу БФнинг чинлик жадвали қуйидагидан иборат:

$S(f)=[0001000100011110000100010001111000010001000111101110111011100001]$.

Мувозанатлашган БФ қуриш учун ушбу хоссадан фойдаланилади: агар $f_1(X)$ ёки $f_2(W)$ ($X\in GF(2)^{n_1}$, $W\in GF(2)^{n_2}$) БФлардан бири мувозанатлашган бўлса, у ҳолда

$$f(X,\ W)=f_1(X)\oplus f_2(W)$$

функция ҳам мувозанатлашган бўлади.

Криптографик алмаштиришларда шакллантирувчи БФларниг мувозанатлашганлиги ва барча алмаштиришларнинг мунтазамлиги муҳим талаб бўлиб ҳисобланади. Ушбу талаб блокли шифрларнинг элементларига тўғридан-тўғри статистик криптоҳужумнинг олдини олади ва кўпгина ҳолларда блокли шифрларнинг криптографик хусусиятларини шакллантиришда зарурий шарт деб қаралиши лозим.

### 4.5.3. Буль функцияларнинг корреляция хоссалари

Берилган $Y=f(X):GF(2)^n\to GF(2)^m$ - БФнинг *мувозанатлашган*лигига қўшимча равишда унинг ихтиёрий $k$ та $(1\le k<n)$ўзгарувчиларини қайд этиш натижасида хосил бўлган барча хусусий БФларнинг ҳам мувозанатлашганлигини талаб этиш билан, дастлабки берилган функцияни

мувозанатлашганлик хоссаси кучайтирилади. Бу эса унинг криптобардошлилик даражасини яна ҳам оширади. Ушбу хусусият ва БФларнинг бошқа криптографик муҳим сифатлари КИ кўрсаткичи билан боғлиқ [23, 59].

**3-таъриф.** Берилган $f(X)$ ва $g(X)$ БФ функциялари ўртасидаги Хэмминг масофаси деб, уларнинг ортогонал (қийматлари фарқли) компоненталари сонига айтилади ва қуйидагича белгиланади:

$$d_H(f,g) = w_H(S(f) \oplus S(g)),$$

бу ерда $w_H$ функция - Хэмминг оғирлиги (0 га тенг бўлмаган компоненталари сони)ни аниқлайди, $S(f)$ ва $S(g)$ мос равишда $f(x)$ ҳамда $g(x)$ функцияларининг чинлик жадваллари.

**Мисол.** $f(X) = \{1001010110101101\}$, $g(X) = \{1101000110101010\}$ БФлари ўртасидаги Хэмминг масофаси 5 га тенг.

БФ $f(X)$, $X \in GF(2)^n$ $k$-тартибли корреляцион иммунликка (КИ) (CI(k)), $(1 \le k < n)$, эга дейилади, агарда Хэмминг оғирлиги ушбу $1 \le w_H(\alpha) \le k < n$ шартни қаноатлантирувчи барча $\alpha \in GF(2)^n$ учун УАА компоненталари спектри $\hat{U}_\alpha(f) = 0$ бўлса.

**4-таъриф.** Шундай қилиб, БФ $f(X)$, $X \in GF(2)^n \to GF(2)^m$ $k$-тартибли КИга эга бўлади, агарда бу функциянинг $X_j = (x_1^j, x_2^j, ..., x_n^j)$ - аргументларининг ихтиёрий $k$ та $x_{i_1}^j, x_{i_2}^j, ..., x_{i_k}^j$, $1 \le i_l \le n$, компонентасини қийматларининг ўзгариши унинг $Y_j = (y_1^j, y_2^j, ..., y_m^j) \in GF(2)^m$ - қийматлари тўплами ўзгаришига статистик боғлиқ бўлмаса. Бирор функция $k$-тартибли корреляцион иммунликка эга бўлса, у ҳолда бу функция $k$ тадан кўп бўлган $x_{i_1}^j, x_{i_2}^j, ..., x_{i_{k+d}}^j$, $1 \le i_l \le n$, $1 \le d < n-k$, компонентасини қийматларининг ўзгаришига $Y_j = (y_1^j, y_2^j, ..., y_m^j) \in GF(2)^m$ - қийматларнинг ўзгариши статистик боғлиқ бўлади, яъни $w_H(\alpha) > k$ бўлганда

$U_\alpha(f) \neq 0$ бажарилади. Бундан, БФнинг корреляцион иммунлик тартибининг юқори чегараси $(n-1)$ дан ошмаслиги келиб чиқади.

Умуман $f(x)$, $x \in GF(2)^n$ БФ КИ даражаси "*k* "=*n*-1 бўлиши мумкин, яъни шундан ошмайди.

**3-тасдиқ.** Энг катта КИ даражасига эга бўлган, яъни "*k* "=*n*-1 функция бу аффин функцияси:

$f(x_1, x_2, ..., x_n) = x_1 \oplus x_2 \oplus ..... \oplus x_n$ ва $f(x_1, x_2, ..., x_n) = x_1 \oplus x_2 \oplus ..... \oplus x_n \oplus 1$.

Бу турдаги функцияларнинг *n*=6 бўлгандаги чинлик жадвали қуйидаги қийматларга эга:

$S(f) = [01101001100101101001011001101001100101100110100101101001100101 10],$

*32* та *0* (ноль) ва *32* та *1* (бир)дан иборат, яъни чинлик жадвали қийматлар тўплами мувозанатлашган.

Юқорида келтирилган тасдиқдан шуни хулоса қилиб айтиш мумкинки, чизиқли акслантириш ҳисобланган "**XOR**" амали энг юқори КИ даражасини таъминлайди. Бундан ташқари дастурлаш таъминотларида самарали қўлланиладиган стандарт кўринишдаги арифметик ва алгебраик амаллар ёки чизиқсизлик даражаси кам бўлган *($2^n$ модуль бўйича қўшиш)* ёки бўлмаса аппаратли қўлланилиши мураккаб бўлган *«даражага ошириш», «$2^n$ модуль бўйича кўпайтириш», «туб модул бўйича кўпайтириш»* амаллари ҳам мисол бўлиши мумкин.

Аслида чизиқсизлик ва КИ тушунчалари криптографик моҳиятлари жиҳатидан ўзаро зид тушунчалар эканлигидан, махсус жадвал кўринишида бериладиган чизиқсиз «ўрнига қўйиш» акслантиришлари КИ кўрсаткичларига мос келмайди деган хулоса ўринли.

*Криптографик акслантиришнинг БФ ифодасини КИ тартибини юқори бўлишини таъминлаш билан унинг статистик криптоҳужум турларига бардошлилигини юқори бўлишига эришилади.*

Бир пайтнинг ўзида бир-нечта самарали криптографик ҳоссаларни (масалан: чизиқсизлик, мувозанатлашганлик, мунтазамлилик, энг катта КИ тартибга эгалик) қаноатлантирувчи битта криптографик акслантиришни қуриш мураккаб масала ҳисобланади. Шунинг учун ҳам энг катта КИ тартибга эгалик хоссасидан кучсизроқ бўлган – БФнинг *корреляция-самарадорлиги* тушунчаси киритилади. Бунда, функциянинг чинлик жадвали қийматлар тўплами мувозанатлашган бўлмайди, яъни *0* (ноль) ва *1* (бир)лар сони ҳар-хил бўлиб, мувозанатлашганлик кўрсаткичи атрофида бўлади.

**5-таъриф**. КИ тартиби *k* бўлган $f(X)$-БФ *k*-тартибли *мукаммал* КИ ёки *резидентлик* хоссасига эга дейилади, агарда у мувозанатлашган бўлса.

**6-таъриф.** Берилган $f(X)$ ва $g(X)$ БФлар корреляцияси деб, қуйидаги қийматга айтилади:

$$C(f,g)=\frac{1}{2^n}\sum_{X\in GF(2)^n}\hat{f}(X)\hat{g}(X)=\frac{1}{2^n}<\hat{S}(f),\hat{S}(g)>=$$

$$=\frac{1}{2^n}\sum_{\substack{X\in GF(2)^n\\ f(X)=g(X)}}\hat{f}(X)\,\hat{g}(X)+\frac{1}{2^n}\sum_{\substack{X\in GF(2)^n\\ f(X)\neq g(X)}}\hat{f}(X)\,\hat{g}(X).$$

Келтирилган таърифлардан Хэмминг масофаси ва корреляция тушунчалари орасида қуйидагича муносабат мавжуд эканлиги келиб чиқади:

$$C(f,g)=1-\left(1/2^{n-1}\right)d_H(f,g).$$

***Мисол***. $f(X)$ ва $g(X)$ БФлар дизъюнктив нормал форма (ДНФ)да қуйидагича берилган:

$$f(X)=f(x_1,x_2,x_3)=x_1x_3\vee x_2\bar{x}_3 \text{ - ДНФ;}$$

$$g(X)=g(x_1,x_2,x_3)=x_1\bar{x}_3\vee x_2x_3 \text{ - ДНФ;}$$

ифодаларига эга бўлиб, мос чинлик жадваллари эса: $S(f)=\{00100111\}$ ва $S(g)=\{00011011\}$ бўлса, у ҳолда ушбу функциялар ўртасидаги корреляция ($C(f,g)$) қандай ҳисобланиши кўриб чиқилади.

***Ечиш.*** ДНФ ифодадан АНФ ифодасига ўтиб олинади, яъни:

$$f(X) = x_1x_3 \vee x_2\bar{x}_3 = x_1x_3 \oplus x_2(x_3 \oplus 1) = x_1x_3 \oplus x_2x_3 \oplus x_2;$$

худди шунингдек, $g(X) = x_1\bar{x}_3 \vee x_2x_3 = x_1(x_3 \oplus 1) \oplus x_2x_3 = x_1x_3 \oplus x_1 \oplus x_2x_3$.

Хэмминг масофаси: $d_H(f,g) = w_H(S(f) \oplus S(g)) = 4$, ҳақиқатдан ҳам $f(X)$ ва $g(X)$ БФлари чинлик жадваллари қийматлари 4 та мос битларда фарқ қиляпти.

Қуйидаги формула ёрдамида ҳам Хэмминг масофасини ҳисоблаш мумкин:

$$d_H(f,g) = 2^{n-1} - \frac{1}{2}(< \hat{S}(f), \hat{S}(g) >);$$

$\hat{S}(f)$ ва $\hat{S}(g)$ қўшма функцияларининг мос чинлик жадвалларини ёзиб олинади:

$\hat{S}(f)$={1, 1, -1, 1, 1, -1, -1, -1} , $\hat{S}(g)$ ={1, 1, 1, -1, -1, 1, -1, -1}.

Буларга кўра скаляр кўпайтма қуйидагича ҳисобланади:

$$< \hat{S}(f), \hat{S}(g) >= 1\cdot 1 + 1\cdot 1 + (-1)\cdot 1 + 1\cdot(-1) + 1\cdot(-1) + (-1)\cdot 1 + (-1)\cdot(-1) + (-1)\cdot(-1) = 0,$$

у ҳолда, келтирилган формулага асосан ушбу қийматга эга бўлинади

$$d_H(f,g) = 2^{n-1} - \frac{1}{2}(< \hat{S}(f), \hat{S}(g) >) = 2^{3-1} - \frac{1}{2}\cdot < \hat{S}(f), \hat{S}(g) >= 2^2 - \frac{1}{2}\cdot 0 = 4.$$

Бу қийматдан фойдаланиб функциялар ўртасидаги корреляция ҳисобланади:

$$C(f,g) = 1 - \frac{1}{2^{3-1}}\cdot d_H(f,g) = 1 - \frac{1}{4}\cdot 4 = 0.$$

Дифференциал, чизиқли ва корреляция таҳлил усулларига бардошли БФ қуришда бу функциянинг *автокорреляция* хоссасини ўрганиш муҳим ҳисобланади. $f(X)$ - БФнинг $\beta \in GF(2)^n$ - векторга нисбатан *автокорреляция* деганда ушбу

$$r_\beta(f) = \frac{1}{2^n}\sum_{X \in GF(2)^n} \hat{f}(X)\,\hat{f}(X \oplus \beta) =< \hat{S}(f), \hat{S}(f(X \oplus \beta)) >$$

тенглик билан ифодаланувчи функция тушунилади. Бу функция қийматининг *0* га яқин бўлиши, яъни $r_\beta(f) \to 0$ бўлиши унга мос БФнинг юқорида келтирилган криптотаҳлил усулларига бардошли эканлигини билдиради.

**4-тасдиқ.** Берилган $f(X)$ ва $g(X)$ БФлар учун Хэмминг масофаси ушбу:

$$d_H(f,g) = w_H(S(f) \oplus S(g)) = 2^{n-1} - \frac{1}{2}\sum_{X \in GF(2)^n} \hat{f}(X)\,\hat{g}(X) = 2^{n-1} - \frac{1}{2}(< \hat{S}(f), \hat{S}(g) >);$$

ифода билан ҳисобланади.

### 4.5.4. Буль функцияларининг қатъий кескин ўзгариш самарадорлик ва тарқалиш тамойиллари

Криптографик акслантиришларнинг муҳим криптобардошлилик характеристикаларидан бири *қатъий кескин ўзгариш самарадорлик тамойили* (ҚКЎСТ) (Strict Avalanche Criterion, **SAC**) ва *тарқалиш тамойили* (ТТ) (Propagation Criterion, **PC**) ҳисобланади. Бу тамойилларнинг асосий моҳиятлари БФ аргументи битларининг бирор қисмини ўзгаришига кўра унинг қийматларини ўзгариши эҳтимоллигини баҳолашдан иборат. Ушбу тушунчалар бевосита криптографик алмаштиришни баҳолаш масалалари билан боғлиқ. Шунинг учун қуйида ушбу тушунчалар билан танишиб чиқамиз [23, 59].

**7-таъриф.** Берилган $f(X)$, $X \in GF(2)^n$ Буль функция ҚКЎСТ эга бўлади, агар Хэмминг оғирлиги $w_H(\beta)=1$ га тенг бўлган барча $\beta$ - векторлар учун $\Delta f(X,\beta)$ - функция баланслашган БФ бўлса.

Ўзгарувчилар $X, \beta \in GF(2)^n$ бўлиб, $f(X) \in GF(2)$ - функция аргументининг $\beta$-қийматга ўзгаришига функциянинг $\Delta f(X,\beta) = f(X) \oplus f(X \oplus \beta)$ - фарқи (айирмаси) мос келсин, у ҳолда $f(X)$– БФ:

- ҚКЎСТ хоссасини қаноатлантиради, агарда $\forall \beta \in GF(2)^n$, $w_H(\beta) = 1$, векторлар учун $\Delta f(X,\beta)$ - БФ мувозанатлашган бўлса;

- $k$-тартибли ҚКЎСТ хоссасини қаноатлантиради, агарда $f(X)$– БФнинг ихтиёрий $k$ та ўзгарувчисини қайд этиш натижасида олинган барча хусусий функциялар ҚКЎСТ хоссасини қаноатлантирса.

**5-тасдиқ.** Агар $\forall \beta \in GF(2)^n$, $w_H(\beta)=1$, векторлар учун $r_\beta(f)=0$ бўлса, $f(X)$– БФ ҚКЎСТ хоссасини қаноатлантиради.

**8-таъриф.** Берилган $f(X)$, $X \in GF(2^n)$ БФ "$e$" – даражали тарқалиш тамойилига эга дейилади, агар $f(X)$ БФ ва Хэмминг оғирлиги ушбу $1 \le w_H(\beta) \le e$ қаноатлантирувчи барча $\beta \in GF(2)^n$ - векторлар учун $r_\beta(f)=0$ бўлса.

Ўзгарувчиси $X \in GF(2)^n$ бўлган $f(X)$– БФ:

- $l$ – даражали, бу ерда $l \le n$, тарқалиш тамойилини (PC($l$)) қаноатлантиради, агар унинг ихтиёрий $i$ та $(1 \le i \le l)$ кириш битларини уларнинг тўлдирувчиларига (тескари қийматли ифодаларига) алмаштирилганда $f(X)$– функция $\Pr\{f(X) \ne f(X \oplus \beta)\} = 0{,}5$ - эҳтимоллик билан ўзгарса, бу эса $\forall \beta \in GF(2)^n$, $1 \le w_H(\beta) \le l$, функция $\Delta f(X, \beta)$ - мувозанатлашганлигини билдиради;

- $l$ – даражали ва $k \le n-1$-тартибли, бу ерда $l \le n$, тарқалиш тамойилини (PC($l$)/$k$) қаноатлантиради, агар унинг ихтиёрий $k$ та кириш битларини қайд этишдан олинган барча хусусий функциялар $l$ – даражали тарқалиш тамойилини қаноатлантирса.

**6-тасдиқ.** Агар $\forall \beta \in GF(2)^n$, $1 \le w_H(\beta) \le l$, векторлар учун $r_\beta(f)=0$ бўлса, $f(X)$– БФ $l$ – даражали ТТни қаноатлантиради.

Келтирилган таъриф ва тасдиқлардан ТТнинг ҚКЎСТни умумлашган эканлиги, ёки аниқроғи, ҚКЎСТ $l$ тартибли ТТга эквивалент (тенг кучли) эканлиги келиб чиқади.

**Мисол.** Қуйидаги 6 та аргументли АНФ кўринишдаги БФ берилган

$$f(X) = x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_1x_5 \oplus x_1x_6 \oplus x_2x_3 \oplus x_2x_4 \oplus x_2x_5 \oplus x_2x_6 \oplus$$
$$\oplus x_3x_4 \oplus x_3x_5 \oplus x_3x_6 \oplus x_4x_5 \oplus x_3x_6 \oplus x_5x_6$$

БФга мос келувчи чинлик жадвали:

$$S(f)=\{0001011101111110011111101110100001111110111010001110100010000001\}$$

бўлиб, мос равишда қуйидагича Уолш-Адамар ва автокорреляция векторларига эга бўлади

$$U_{\alpha}^{*}(f)=\{-8,-8,-8,8,-8,8,8,8,-8,8,8,8,8,8,8,-8,-8,8,8,8,8,8,8,-8,8,8,8,-8,8,-8,-8,-8,-8,8,8,8,8,8,-8,8,8,8,8,8,8,8,-8,8,8,8,-8,8,-8,-8,-8,8,8,8,-8,8,-8,-8,-8,8,-8,-8,-8,-8,-8,8\}$$

$$r_{\beta}(f)=\{000000000000000000000000000000000000000000000000000000000000\}$$

Юқорида келтирилган таърифлардан қатъий кескин ўзгариш самарадорлик ва тарқалиш тамойиллари даражаларини ҳисоблаб қуйидагилар олинади:

$SAC(4)$ - даражали қатъий кескин ўзгариш самарадорликка эга;

$PC(6)$ - даражали тарқалиш тамойилига эга.

Юқоридаги мисолда берилган функция юқори қатъий кескин ўзгариш самарадорлик ва тарқалиш тамойиллари даражаларига эга бўлган 6 та аргументли БФ қаторига кирар экан. Лекин бундай кўринишдаги функциялар (бент функциялар) қанчалик юқори чизиқсизлик, қатъий кескин ўзгариш самарадорлик ва тарқалиш тамойиллари даражаларига эга бўлмасин, умумий талабларда келтирилган биринчи мунтазамлилик ва мувозанатлашганлик шартларини қаноатлантирмайди.

### 4.5.5. Буль функцияларнинг чизиқсизлик характеристикалари

БФни уларнинг хоссаларидан фойдаланиб таҳлил қилиш нисбатан енгил кечади. Криптографик акслантиришлар БФ чизиқсизлиги уларнинг криптобардошлилик кўрсаткичлари самарадорлигини таъминлайди, хусусан, чизиқли криптотаҳлил усулига бардошлилигини. Бирор БФнинг чизиқсизлиги унинг аффин ёки чизиқли БФлар тўпламидан қанчалик даражада четлашганлигини билдиради [23, 59].

**9-таъриф.** Аффин функциялар деб $\{f_{aff}(X)\}$, $X=(x_1,x_2,...,x_n)\in GF(2)^n$

$f_{aff}(X) =< \alpha, X \oplus c >$ шаклдаги функцияга айтилади, бу ерда $\alpha_i, x_i \in GF(2)$.

**10-таъриф.** Берилган $f(X)$ ( $GF(2)^n \to GF(2)$ ) БФнинг чизиқсизлиги

$$N(f) = \min_{\forall f_{aff}} d_H(f, f_{aff})$$

ифода бўйича ҳисобланади.

БФлар атамаларида чизиқсизлик тушунчаси қуйидагича аниқланади:

$$N(f) = 2^{n-1} - 2^{n-1} \cdot \max_{\forall f_{lin}} \left| C(f, f_{lin}) \right|,$$

бу ерда,

$$C(f, f_{lin}) = \frac{1}{2^n} \left\langle S^{\wedge}(f), S(< \alpha, X >) \right\rangle = \frac{1}{2^n} \cdot U^{\wedge}_{\alpha}(f),$$

$f_{lin} =< \alpha, x > = \alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 + ... + \alpha_n \cdot x_n$ га тенг.

**7-тасдиқ.** Берилган $f(x)$ БФ учун чизиқсизлик қиймати қуйидаги ифода билан аниқланади [21, 58]:

$$N(f) = 2^{n-1} - \frac{1}{2} \cdot \max_{\forall f_{lin}} \left| \left\langle S^{\wedge}(f), S^{\wedge}(f_{lin}) \right\rangle \right| = 2^{n-1} - \frac{1}{2} \cdot \max_{\forall \alpha \in GF(2)^n} \left| U^{\wedge}_{\alpha}(f) \right|$$

Демак, охирги формуладан фойдаланиб, $n$ – лар учун $N(f)$ - нинг қийматини топиш мумкин.

**8-тасдиқ.** Агар $f(X)$ БФ мувозанатлашган бўлса, у ҳолда

$$N(f) \le \begin{cases} 2^{n-1} - 2^{(1/2)n-1} - 2 & \text{, агар n – жуфт бўлса;} \\ \left[\!\left[ 2^{n-1} - 2^{(1/2)n-1} \right]\!\right] & \text{, агар n – тоқ бўлса;} \end{cases}$$

бу ерда $[\![x]\!]$ - $x$ дан катта бўлмаган энг катта жуфт сонни билдиради.

**Мисол.** Берилган ($n$=3) $f(X) = x_1 \cdot x_3 \oplus x_2 \cdot x_3 \oplus x_1$ мувозанатлашган Буль функция учун $N(f(X)) = 2$ бўлишлигини кўрсатамиз.

$f(X)$ функциянинг чинлик жадвали: $S(f) = \{0\ 0\ 0\ 1\ 1\ 0\ 1\ 1\}$.

Умуман *n*=3 аргументли мувозанатлашган БФлар сони *24* та бўлади. Чунки берилган БФ чинлик жадвалида *4* та “0” ва 4 та “1” бўлиши мумкин. У ҳолда 4 та элементдан ўрин алмаштиришлар сони *4!=24.*

Бевосита ҳисоблаш мумкинки:

$$U_{\alpha_1}^{\wedge}(f)=\sum_{x\in GF(2)^3}(-1)^{f(x)\oplus<\alpha_1,x_1>}=(-1)^{f(x_0)\oplus<\alpha_1,x_0>}+(-1)^{f(x_1)\oplus<\alpha_1,x_1>}+$$
$$+(-1)^{f(x_2)\oplus<\alpha_1,x_2>}+(-1)^{f(x_3)\oplus<\alpha_1,x_3>}+(-1)^{f(x_4)\oplus<\alpha_1,x_4>}+(-1)^{f(x_5)\oplus<\alpha_1,x_5>}+$$
$$+(-1)^{f(x_6)\oplus<\alpha_1,x_6>}+(-1)^{f(x_7)\oplus<\alpha_1,x_7>}=1+1+1-1-1+1-1-1=0.$$

Худди шу каби қолганлари ҳам ҳисобланганда қуйидаги натижалар олинади:

$$U_{\alpha_2}^{\wedge}(f)=2,\ U_{\alpha_3}^{\wedge}(f)=2,\ U_{\alpha_4}^{\wedge}(f)=-1,\ U_{\alpha_5}^{\wedge}(f)=4,\ U_{\alpha_6}^{\wedge}(f)=4,$$
$$U_{\alpha_7}^{\wedge}(f)=0,\ U_{\alpha_8}^{\wedge}(f)=0$$

бу ерда, $\alpha_1=(0,0,0)$, $\alpha_2=(0,0,1)$, $\alpha_3=(0,1,0)$, $\alpha_4=(0,1,1)$, $\alpha_5=(1,0,0)$, $\alpha_6=(1,0,1)$, $\alpha_7=(1,1,0)$, $\alpha_8=(1,1,1)$

Демак,

$$N(f)=2^{3-1}-\frac{1}{2}\cdot\max_{\alpha_i\in GF(2)^3}\left|U_{\alpha_i}^{\wedge}(f)\right|=2^2-\frac{1}{2}\cdot 4=2,$$

яъни $N(f)$=2 энг катта чизиқсизлик даражасига эга экан.

Берилган $f(X)$ ( $GF(2)^n\rightarrow GF(2)$ ) БФнинг чизиқсизлик даражасига тескари бўлган чизиқлилик тушунчаси мавжуд бўлиб, у қуйидагича ифодаланади:

$$N(f)=2^{n-1}(1-L(f)),\quad L(f)=1-2^{1-n}N(f).$$

бу ерда: $L(f)$ - берилган $f(X)$ - БФнинг чизиқлилик даражаси.

$N(f)$ - берилган $f(X)$ - БФнинг чизиқсизлик даражаси.

Умумий ҳолда қуйидаги тасдиқ ўринли:

$2^{-\frac{n}{2}} \le L(f) \le 1$ ва $0 \le N(f) \le 2^{n-1} - 2^{(n/2)-1}$.

Юқорида $f(X)$ ( $GF(2)^n \to GF(2)$ ) БФга нисбатан чизиқлилик ва чизиқсизлик тушунчалари ҳамда уларнинг баҳолари ҳақида фикр юритилди. Умумий ҳолда $Y=\varphi(X)$ : $GF(2)^n \to GF(2)^m$ – акслантиришига нисбатан чизиқлилик ва чизиқсизлик тушунчаси қизиқтиради. Қуйида эса ушбу фикрлар (тушунчалар) ҳақида тўхталиб ўтамиз.

**11-таъриф.** $Y=\varphi(X)$ : $GF(2)^n \to GF(2)^m$ БФ учун мос равишда чизиқсизлик ва чизиқлилик даражалари қуйидагича аниқланади [23, 59]:

$$N(\varphi(X)) = \min_{\substack{\forall c \in GF(2)^m \\ c \neq 0}} N < c, \varphi >,$$

$$L(\varphi(X)) = \max_{\substack{\forall c \in GF(2)^m \\ c \neq 0}} L < c, \varphi >$$

бу ерда $\varphi = \{f_1, f_2, ..., f_m\}$, $c = (c_1, c_2, ..., c_m)$, $< c, \varphi >= c_1 f_1(X) + c_2 f_2(X) + ... + c_m f_m(X)$ яъни $< c, \varphi >$- скаляр кўпайтма натижаси БФ деб қаралади.

Бироқ амалиётда чизиқлилик ва чизиқсизлик даражалари юқори бўлган $\varphi(x)$ БФ эришиш қийин бўлгани учун ўртача чизиқлилик ва ўртача чизиқсизлик тушунчалари киритилиб, улар қуйидагича аниқланади:

$$\overline{N}(\varphi(X)) = \frac{1}{2^m - 1} \sum_{\substack{\forall c \in GF(2)^m \\ c \neq 0}} N < c, \varphi >,$$

$$\overline{L}(\varphi(X)) = \frac{1}{2^m} \sum_{\substack{\forall c \in GF(2)^m \\ c \neq 0}} L < c, \varphi >$$

Ушбу тушунчаларни киритиб бўлгач, “аслида энг катта чизиқсизлик даражасига эга бўлган БФлар мавжудми? ” деган савол туғилади. Бу саволга жавоб бериш учун қуйида айрим янги тушунчалар билан танишиб чиқамиз.

**12-таъриф.** Берилган $f(X)$ БФ ва $\beta \in GF(2)^n$ векторларга нисбатан автокорреляция деб, қуйидаги тенглик билан аталувчи:

$$r_\beta(f) = \frac{1}{2^n} \sum_{\forall X \in GF(2)^n} f^{\wedge}(X) \cdot f^{\wedge}(X \oplus \beta)$$

бу ерда $f^{\wedge}(X)$ БФ чизиқли, дифференциал ва корреляцион криптотаҳлил турларига юқори даражадаги бардошликларини таъминлашда муҳим инструмент ҳисобланади [14,9].

**13-таъриф.** Берилган $f(X)$ $(X \in GF(2)^n)$ БФ мутлақо чизиқсиз ёки бент функция (Bent function) деб аталади, агар $\forall \beta \in GF(2)^n$ учун

$$\#\{X \in GF(2)^n : f(X) = f(X \oplus \beta)\} = \frac{2^n}{2} = 2^{n-1}$$

ёки

$$r_\beta(f) = 0$$

тенглик ўринли бўлса.

**9-тасдиқ.** Берилган $f_{бент}(X)$, $X \in GF(2)^n$ функция энг катта чизиқсизлик қийматига ва минимал чизиқлилик қийматига эга бўлади, агарда:

$$N(f_{бент}(X)) = 2^{n-1} - 2^{\frac{n}{2}-1}, \qquad L(f_{бент}(X)) = 2^{-\frac{n}{2}}$$

бўлса.

Қуйида, бирор симметрик шифрлаш алгоритми ўрнига қўйиш алмаштиришига нисбатан қўйиладиган умумий талаблар келтирилади:

1. $Y = \varphi(X) : GF(2)^n \to GF(2)^m$, $n \geq m$ алмаштириш мунтазам бўлишлиги, яъни $\varphi(X) = \{f_1(X), f_2(X), ..., f_m(X)\}$ ташкил этувчи $f_i(X)$, $i = \overline{1,m}$ БФлар компоненталарининг мувозанатлашганлиги;

2. Шакллантирувчи БФларнинг юқори алгебраик даража $\deg(f)$ ва юқори чизиқсизлик $N(f)$ $(\overline{N}(f))$га эга бўлишлиги;

**Изоҳ.** Берилган $f_i(X)$, $i=\overline{1,m}$ БФнинг алгебраик чизиқсизлик даражаси деб, $f_i(X)$ нинг АНФ формасидаги ҳар хил $x_i$ - аргументлар қатнашган кўпайтмасининг ҳадларидаги энг катта иштирокига айтилади.

3. Шакллантирувчи БФларнинг юқори КИ кўрсаткичларига эга бўлиши;

4. БФларининг ҚКЎСТ кўрсаткичларига мос келиши, яъни автокорреляция ($r_\beta(f)$) қийматининг етарли даражада кичик бўлиши;

5. $\varphi(X)$ - алмаштириш учун $N(\varphi(X))$ - юқори ва $L(\varphi(X))$ - кичик қийматга эга бўлиши.

**Мисол.** Қуйидаги олтита (6 та) аргументли АНФ кўринишидаги БФ берилган бўлсин:

$$f(x)=x_1\oplus x_2\oplus x_3\oplus x_2x_5\oplus x_3x_6\oplus x_4x_5\oplus x_4x_6\oplus x_3x_5x_6\oplus x_4x_5x_6\oplus x_2x_5x_6.$$

Шу БФ учун чизиқсизлик характеристикаларини кўриб чиқамиз.

Берилган БФ чинлик жадвали қуйидагича:

*S(f)={00000111101111001101101001100001111110000100001100100101100111 10}*

бўлиб, чинлик жадвалида *0* лар сони *1* лар сонига тенг бўлганлиги учун ушбу БФ мунтазам ҳисобланади.

Бу БФ қўшма функциясига нисбатан барча $a\in 2^6$ ларда УАА ҳисобланади:

$$U_\alpha^*(f)=\{0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,$$
$$0,0,0,0,0,0,0,0,16,16,-16,-16,0,0,0,0,16,-16,16,-16,16,16,16,16,16,-16,-16,16\}$$

ва натижада БФ учун чизиқсизлик қийматини ҳисоблашнинг УАА орқали берилган таърифидан фойдаланиб, $N(f)=24$ эга бўлинади. Умуман олганда *6* та аргументли БФлари учун энг катта чизиқсизлик даражаси *26* га тенг. Демак, берилган функция чизиқсизлик даражаси юқори бўлган функциялар қаторига киради.

Симметрик блокли шифрлаш алгоритмининг криптографик алмаштиришини БФ кўринишида ифодаланса, шу БФга нисбатан чизиқсизлик даражаларини

юқорида келтирилганидек ҳисоблаш мумкин.

Маълумки DES стандарт алгоритми *S*–блокларида кириш *6* бит, чиқиш эса *4* бит. Қуйидаги 10-жадвалда *S2*- блок акслантириши берилган бўлиб, уни БФ кўринишида ифодалаш учун 10-жадвалнинг чинлик жадвали деб аталувчи қуйидаги 11-жадвал қуриб олинади.

10-жадвал

**DES стандарт алгоритми S2-блок акслантириши**

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 15 | 1 | 8 | 14 | 6 | 11 | 3 | 4 | 9 | 7 | 2 | 13 | 12 | 0 | 5 | 10 |
| 3 | 13 | 4 | 7 | 15 | 2 | 8 | 14 | 12 | 0 | 1 | 10 | 6 | 9 | 11 | 5 |
| 0 | 14 | 7 | 11 | 10 | 4 | 13 | 1 | 5 | 8 | 12 | 6 | 9 | 3 | 2 | 15 |
| 13 | 8 | 10 | 1 | 3 | 15 | 4 | 2 | 11 | 6 | 7 | 12 | 0 | 5 | 14 | 9 |

11-жадвал

**Чинлик жадвали**

| | $x_1$ | $x_2$ | $x_3$ | $x_4$ | $x_5$ | $x_6$ | $y_1$ | $y_2$ | $y_3$ | $y_4$ |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 |
| 2 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |
| 3 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 |
| 4 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 |
| . | . | . | . | . | . | . | . | . | . | . |
| 60 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |
| 60 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 |
| 61 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 |
| 62 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 |
| 63 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 |

Бу 11-жадвалга мос келувчи БФ ифодаси қуйидагича бўлади:

$$y_1 = (\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge \bar{x}_4 \wedge \bar{x}_5 \wedge \bar{x}_6) \oplus (\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge \bar{x}_4 \wedge x_5 \wedge x_6) \oplus (\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge x_4 \wedge \bar{x}_5 \wedge \bar{x}_6) \oplus$$
$$\oplus (\bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge x_4 \wedge x_5 \wedge \bar{x}_6) \oplus (\bar{x}_1 \wedge \bar{x}_2 \wedge x_3 \wedge \bar{x}_4 \wedge \bar{x}_5 \wedge x_6) \oplus (\bar{x}_1 \wedge \bar{x}_2 \wedge x_3 \wedge \bar{x}_4 \wedge x_5 \wedge \bar{x}_6) \oplus$$
$$\oplus (\bar{x}_1 \wedge \bar{x}_2 \wedge x_3 \wedge x_4 \wedge \bar{x}_5 \wedge x_6) \oplus (\bar{x}_1 \wedge \bar{x}_2 \wedge x_3 \wedge x_4 \wedge x_5 \wedge x_6) \oplus (\bar{x}_1 \wedge x_2 \wedge \bar{x}_3 \wedge \bar{x}_4 \wedge \bar{x}_5 \wedge \bar{x}_6) \oplus$$
$$\oplus (\bar{x}_1 \wedge x_2 \wedge \bar{x}_3 \wedge \bar{x}_4 \wedge \bar{x}_5 \wedge x_6) \oplus (\bar{x}_1 \wedge x_2 \wedge \bar{x}_3 \wedge x_4 \wedge x_5 \wedge \bar{x}_6) \oplus (\bar{x}_1 \wedge x_2 \wedge \bar{x}_3 \wedge x_4 \wedge x_5 \wedge x_6) \oplus$$
$$\oplus (\bar{x}_1 \wedge x_2 \wedge x_3 \wedge \bar{x}_4 \wedge \bar{x}_5 \wedge \bar{x}_6) \oplus (\bar{x}_1 \wedge x_2 \wedge x_3 \wedge \bar{x}_4 \wedge x_5 \wedge x_6) \oplus (\bar{x}_1 \wedge x_2 \wedge x_3 \wedge x_4 \wedge \bar{x}_5 \wedge x_6) \oplus$$
$$\oplus (\bar{x}_1 \wedge x_2 \wedge x_3 \wedge x_4 \wedge x_5 \wedge \bar{x}_6) \oplus (x_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge \bar{x}_4 \wedge \bar{x}_5 \wedge x_6) \oplus (x_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge \bar{x}_4 \wedge x_5 \wedge \bar{x}_6) \oplus$$
$$\oplus (x_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge \bar{x}_4 \wedge x_5 \wedge x_6) \oplus (x_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge x_4 \wedge \bar{x}_5 \wedge x_6) \oplus (x_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge x_4 \wedge x_5 \wedge \bar{x}_6) \oplus$$
$$\oplus (x_1 \wedge \bar{x}_2 \wedge x_3 \wedge \bar{x}_4 \wedge \bar{x}_5 \wedge \bar{x}_6) \oplus (x_1 \wedge \bar{x}_2 \wedge x_3 \wedge \bar{x}_4 \wedge x_5 \wedge x_6) \oplus (x_1 \wedge \bar{x}_2 \wedge x_3 \wedge x_4 \wedge \bar{x}_5 \wedge \bar{x}_6) \oplus$$
$$\oplus (x_1 \wedge x_2 \wedge \bar{x}_3 \wedge \bar{x}_4 \wedge \bar{x}_5 \wedge x_6) \oplus (x_1 \wedge x_2 \wedge \bar{x}_3 \wedge \bar{x}_4 \wedge x_5 \wedge \bar{x}_6) \oplus (x_1 \wedge x_2 \wedge \bar{x}_3 \wedge x_4 \wedge \bar{x}_5 \wedge \bar{x}_6) \oplus$$
$$\oplus (x_1 \wedge x_2 \wedge \bar{x}_3 \wedge x_4 \wedge x_5 \wedge x_6) \oplus (x_1 \wedge x_2 \wedge x_3 \wedge \bar{x}_4 \wedge \bar{x}_5 \wedge \bar{x}_6) \oplus (x_1 \wedge x_2 \wedge x_3 \wedge x_4 \wedge \bar{x}_5 \wedge x_6) \oplus$$
$$\oplus (x_1 \wedge x_2 \wedge x_3 \wedge x_4 \wedge x_5 \wedge \bar{x}_6) \oplus (x_1 \wedge x_2 \wedge x_3 \wedge x_4 \wedge x_5 \wedge x_6)$$

Бу ердаги ҳар бир қўшилувчи чинлик жадвалида $y_1$га *“1”* (чин) қиймат берувчи ўзгарувчилар конъюнкциясидан иборат бўлган *32* та ҳаддан ташкил топган бўлиб, ўзгарувчи инкорига $\bar{x}_i$ нол *“0”* қиймат, ўзгарувчининг ўзига бир *“1”* қиймат мос келади ва барча мумкин бўлган $2^6 = 64$ та қийматларда чинлик жадвалининг $y_1$ га мос келувчи устунини ифодалайди.

БФ ифодасида $\bar{x}_i = x_i \oplus 1$ алмаштиришни бажариб ва соддалаштириб, унинг қуйидаги АНФ кўриниши олинади:

$$y_1 = x_1 \oplus x_3 \oplus x_5 \oplus x_6 \oplus x_4x_5 \oplus x_2x_6 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1x_2x_3 \oplus x_1x_2x_6 \oplus x_2x_4x_5 \oplus x_2x_3x_6 \oplus x_1x_5x_6 \oplus x_1x_4x_5 \oplus$$
$$\oplus x_1x_4x_5x_6 \oplus x_1x_3x_5x_6 \oplus x_1x_2x_5x_6 \oplus x_1x_2x_4x_5 \oplus x_1x_2x_3x_6 \oplus x_1x_2x_4x_5x_6 \oplus 1.$$

## Назорат саволлари

1. Ўзбекистон Республикасида фойдаланишда бўлган блокли шифрлаш алгоритмлари қайси стандартлар билан белгиланган?

2. Криптотаҳлилчилар томонидан қайси блокли шифрлаш алгоритмлари учун криптотаҳлил усуллари ишлаб чиқилган?

3. Чизиқли криптотаҳлил усулининг моҳиятини тушунтиринг. Топилиши лозим бўлган чизиқли ифодаларнинг кўринишини келтиринг?

4. «Эҳтимолликнинг оғиши» деганда нимани тушунасиз ?

5. Чизиқли криптотаҳлил усули асосида DESнинг калитини топиш учун қандай миқдордаги очиқ матн ва шифрматн жуфтидан фойдаланиш зарур?

6. Дифференциал криптотаҳлил усули нимага асосланади, унинг моҳияти нимада?

7. Дифференциал криптотаҳлил усулини амалга ошириш процедураси қандай қадамларни ўз ичига олади?

8. Симметрик шифрлаш алгоритмларида БФнинг ифодалари учун алгебраик нормал форма қандай кўринишда ифодаланади?

9. Берилган $f(X)$ функциянинг алгебраик чизиқсизлик даражаси деганда нимани тушунасиз, у қадай белгиланади?

10. Уолш-Адамар акслантириши деганда нимани тушунасиз? УААга тескари акслантириш ифодаси қандай?

11. Мувозанатлашган БФга таъриф беринг?

12. Мунтазам акслантиришга таъриф беринг?

13. БФнинг мунтазам бўлишининг зарурий шарти нима?

14. БФ мувозанатлашганлиги УАА орқали қандай ифодаланади?

15. БФ $f(X)$ қандай ҳолда $k$-тартибли корреляция - иммунлик(КИ)ка эга бўлади?

16. КИ тартиби $k$ бўлган БФ қандай ҳолда $k$-тартибли мукаммал КИ хоссасига эга бўлади?

17. БФ функциясининг автокорреляция хоссасини ўрганиш қандай мақсадларда муҳим ҳисобланади?

18. Берилган $f(X)$ ва $g(X)$ БФ функциялари ўртасидаги Хэмминг масофаси қандай ифодаланади?

18. Берилган $f(X)$ ва $g(X)$ БФлар корреляцияси деганда қандай ифода бўйича ҳисобланган қийматни тушунасиз?

19. Қатъий кескин ўзгариш самарадорлик тамойили ва тарқалиш тамойили асосий моҳияти нимада?

20. БФ ҚКЎСТ хоссасини қаноатлантириши учун қандай шартлар қаноатлантирилиши лозим? ҚКЎСТ ва ТТ тенг кучлими?

21. Берилган $f(X)$ $(GF(2)^n \rightarrow GF(2))$ БФнинг чизиқсизлик ва чизиқлилик даражалари қандай таърифланади ва ифодаланади?

22. Берилган $f_{бент}(X)$, $x \in GF(2)^n$ функция қандай ҳолларда энг катта чизиқсизлик қийматига ва энг кичик чизиқлилик қийматига эга бўлади?

23. Қандай шартлар қаноатлантирилганда берилган БФ "$k$"- даражали корреляцион иммунликка эга бўлади?

24. Қандай функция энг катта КИ даражасига эга бўлган функциялар қаторига киради?

25. Берилган, БФ f(X) қандай ҳолда "$e$" – даражали тарқалиш тамойилига эга бўлади?

# 5. КРИПТОГРАФИК АЛГОРИТМЛАРНИНГ БАРДОШЛИЛИГИНИ БАҲОЛАШ

## 5.1. Ҳисоблаш мураккаблиги назарияси

Мураккаблик назарияси криптографик таҳлиллаш алгоритмларининг ҳисоблаш мураккабликлари билан шуғулланади. Ҳар хил криптографик таҳлиллаш алгоритмларининг ҳисоблаш мураккабликларини солиштириб, криптографик алгоритмларнинг ишончлилик - бардошлилик даражаси аниқланади [23].

**Алгоритмнинг мураккаблиги**, шу алгоритмни тўла амалга ошириш учун бажарилиши назарда тутилган барча амаллар сони билан аниқланади. Алгоритмнинг ҳисоблаш мураккаблиги одатда иккита параметр - алгоритмда кўрсатилган амалларни бажаришга сарфланадиган *вақт билан аниқланадиган мураккаблик* $T$ ва ҳисоблаш қурилмасида алгоритм параметрлари устида амаллар бажаришда керак бўладиган регистрлар сони билан аниқланадиган – *ҳисоблаш қурилмаси хотирасининг ҳажми билан боғлиқ бўлган мураккаблик* $S$ билан аниқланади.

Бу $T$ ва $S$ параметрлар алгоритм хусусиятларидан келиб чиқиб бошланғич қийматларнинг $n$ ўлчамига боғлиқ ҳолда, яъни $T=f(n)$ ва $S=s(n)$ функциялар билан аниқланади.

Алгоритмнинг ҳисоблаш мураккаблиги одатда ҳисоблаш мураккаблиги қийматининг тартибини кўрсатувчи “$O$” белгиси билан ифодаланади ҳамда бу белги $n$ параметр қийматининг ортиши билан мураккаблик функцияси ифодаси ичида қиймати энг тез ўсадиган ҳадни ифодалаб, бошқа ҳадларни ҳисобга олмайди. Масалан, алгоритмнинг вақт билан аниқланадиган мураккаблиги $T=f(n)=5n^2+6n+11$ бўлса, у ҳолда унинг $n^2$ тартибли ҳисоблаш мураккаблиги $O(n^2)$ кўринишда ифодаланади [23].

Ҳисоблаш мураккаблиги баҳолари бошланғич қийматларни, алгоритмнинг хусусиятларидан келиб чиққан ҳолда, алгоритмни амалга ошириш учун сарфланадиган вақт ва ҳисоблаш қурилмаси хотирасига қўйиладиган талабларни яққол намоён этади. Масалан, $T=O(n)$ бўлса, бошланғич қиймат ўлчамининг икки марта ўсиши вақтнинг ҳам икки марта ўсишига олиб келади; агарда $T=O(2^n)$ бўлса, бошланғич қиймат ўлчамига битта битнинг қўшилиши алгоритмни амалга ошириш учун сарфланадиган вақтни икки баравар ортишини билдиради.

**Алгоритмлар** вақт ва ҳисоблаш мураккабликларига кўра қуйидаги **синфларга ажратилади** [15, 23]:

1. Алгоритм *доимий* дейилади, агарда унинг мураккаблик қиймати бошланғич қиймат ўлчамига боғлиқ бўлмаса, яъни $O(1)$.

2. Алгоритм *чизиқли* дейилади, агарда унинг мураккаблиги қийматининг тартиби $O(n)$ бўлса.

3. Алгоритм *полиномиал* дейилади, агарда унинг мураккаблиги қийматининг тартиби $O(n^m)$ (бу ерда $m>1$) бўлса.

4. Алгоритм *экспоненциал* дейилади, агарда унинг мураккаблиги қийматининг тартиби $O(t^{f(n)})$ (бу ерда $const=t>1$ ва $f(n)$ – бошланғич қиймат ўлчами $n$ га нисбатан полиномиал функция) бўлса.

5. Мураккаблиги қийматининг тартиби $O(t^{f(n)})$ бўлган *экспоненциал* алгоритмлар тўпламига қисм тўплам бўладиган алгоритмлар *суперполиномиал* дейилади, агарда $f(n)$ – полиномиал функция $t$ ўзгармасга нисбатан тезроқ, лекин чизиқли функцияга нисбатан секинроқ ўсса, мисол учун: $O\left(t^{\sqrt{n}}\right)$, $1<t<\sqrt{n}$ бўлса.

Шу ерда таъкидлаш жоизки, криптоалгоритмлар натижасига кўра унинг номаълум параметрларини топишнинг мавжуд алгоритмлари суперполиномиал мураккабликка эга бўлиб, уларнинг полиномиал мураккабликка эга бўлган алгоритмларини топиш мумкин эмаслиги исбот қилинмаган. Яъни бирор

алгоритмнинг номаълум параметрини полиномиал мураккабликка эга бўлган алгоритмларини топиш мумкинлиги унинг криптобардошсиз бўлиб қолганлигини билдиради.

**Масаланинг (муаммонинг) мураккаблиги.** Бирор масалани ечиш алгоритмининг мураккаблигидан ташқари, масалани ўзининг мураккаблиги тушунчаси ҳам мавжуд. Масаланинг мураккаблиги назарияси ечилиши энг мураккаб бўлган масалани **Тьюринг машинаси** деб аталувчи – **назарий компьютерда** ечиш учун сарфланадиган минимал вақт ва хотира ҳажмини баҳолаш масалалари билан шуғулланади. Тьюринг машинаси – ўқиш ва ёзиш учун чексиз хотирага эга бўлган чекли сондаги амалларни бажарувчи ҳисоблаш қурилмасидан иборат.

Полиномиал мураккабликка эга бўлган алгоритмлар билан ечиладиган масалаларни *ечиш мумкин бўлган* масалалар дейилади, яъни булар бошланғич киритиладиган қийматларнинг бирор чекли *n*-ўлчамида қониқарли вақт бирлиги ичида ечилиши мумкин полиномиал мураккабликка эга бўлган масалалардир. Полиномиал вақт бирлиги ичида ечилмайдиган масалаларни *қийин ечиладиган* ёки *қийин* масалалар дейилади, яъни бу ҳолда бошланғич киритиладиган қийматларнинг бирор етарли кичик чекли *n*-ўлчамидан бошлаб ечиш учун бажарилиши керак бўлган амаллар сонининг етарли даражада тез ўсиб кетишига олиб келиб, бу амалларнинг барчасини амалга ошириш имкони бўлмайди. Бошланғич киритиладиган қийматларнинг нисбатан етарли кичик чекли *n* ўлчамида супер полиномиал мураккабликка эга бўлган алгоритмлар билан ечиладиган масалаларни *ҳисобланиши қийин* бўлган масалалар дейилади.

Ечиш алгоритмлари яратилмаган (ёки қандай яратилиш асослари замонавий илм-фан ютуқларига мантиқан маълум бўлмаган) масалалар – *ечилмайдиган* масалалар дейилади.

Иккилик саноқ тизимининг сўзлари деб аталувчи, иккилик саноқ тизимининг алифбо белгиларидан *{0; 1}* иборат барча:

*0; 1; 00; 01; 10; 11; 000; 001; … ; 111; …; 00…0; 00…1; …; 11…1; …*

чекли сондаги *0* ва *1* белгиларнинг кетма-кетликлари блокларидан (векторларидан) тузилган тўпламни $\Sigma$ деб белгилаймиз. Барча ўлчами $n$ га тенг бўлган иккилик саноқ тизимининг сўзлари тўпламини $\Sigma^n$ деб белгилаймиз. Мураккаблик назариясида $\Sigma$ тўпламга қисм бўлган тўпламлар $L \in \Sigma$ - тиллар дейилади деб қабул қилинган.

Агар Тьюринг машинаси $M$ да у ихтиёрий чекли $n$ ўлчамли бошланғич кириш қийматига (сўзига) боғлиқ бўлган $p(n)$ – кўпҳаднинг (энг катта) қийматидан кўп бўлмаган амалларни бажаргандан сўнг тўхтаса, у полиномиал вақт бирлиги ичида ишлайди (ёки полиномиал) дейилади.

$M$ Тьюринг машинаси $L$ тилни тушунади (қабул қилади) дейилади, агарда у $L$ тилга тегишли бўлган ихтиёрий кириш сўзида, яъни $\forall x \in L$ бўлганда, амалларни бажариб, яна қабул қилиш ҳолатида ҳамда, $\forall x \notin L$ бўлганда, амалларни бажариб рад этиш ҳолатида тўхтаса.

Полиномиал вақт бирлиги ичида ишлайдиган Тьюринг машинаси $M$ қабул қиладиган барча тиллар синфи $P$ – синф деб белгиланади.

Агарда функция $f$ учун полиномиал Тьюринг машинаси мавжуд бўлиб, бошланғич қиймат - кириш $x \in \Sigma$ сўзида амалларни бажариб, тўхтаганда $f(x)$ қийматни берса, у $f: \Sigma \to \Sigma$ полиномиал вақт бирлиги ичида ҳисобланади дейилади.

Агарда полиномиал вақт бирлиги ичида ҳисобланадиган $P(x,y)$: $\Sigma \times \Sigma \to \{0, 1\}$ – функция (предикат) мавжуд бўлиб, бошланғич кириш қийматлари ўлчамига нисбатан аниқланувчи мураккаблик полиноми $p \in L = \{x \mid \exists\, y\ P(x,y) \,\&\, |y| \le p(|x|)\}$ бўлса, $L$ тил $NP$ тўлиқ синфга тегишли бўлади. Яъни $L$ тил $NP$ тўлиқ синфга тегишли бўлади, агарда ихтиёрий $n$-ўлчами $x \in L$ сўз учун унга мос $p(|x|) = p(n)$ полиномиал узунликка эга бўлган $y$ сатрни кўрсатиш мумкин бўлиб, кўрсатилган сатрни тўғри ёки нотўғрилиги $P(x, y)$ предикат орқали аниқланган.

Юқоридаги фикр ва мулоҳазалардан $P \subseteq NP$ эканлиги келиб чиқади. Бу тегишлилик муносабати қатъий, яъни: $P \subset NP$ ва $P \neq NP$ эканлиги тўғрисида ҳозирги кунда бирор исбот қилинган далил мавжуд эмас.

*NP* тўлиқ синфдан энг катта полиномиал мураккабликка эга бўлган тилларнинг қисм синфи ажратилган, яъни ихтиёрий $L \in NP$ тўлиқ тил полиномиал вақт бирлиги ичида тушунилиши (қабул қилиниши) учун $P = NP$ бўлиши зарур ва етарли.

Юқорида киритилган *Тьюринг машинаси* тушунчасидан ташқари *Тьюрингнинг эҳтимоллик машинаси* тушунчаси ҳам мавжуд. Бу тушунчаларнинг фарқи қуйидагича. Тьюринг машинасининг кейинги (янги) ҳолати унинг бундан олдинги ҳолати билан тўлиқ аниқланади. Тьюринг эҳтимоллик машинасининг кейинги (янги) ҳолати унинг бундан олдинги ҳолати ва яна *0* ҳамда *1* қийматларни ½ эҳтимоллик билан қабул қилувчи тасодифий миқдорнинг қиймати билан биргаликда аниқланади. Яъни Тьюрингнинг эҳтимоллик машинаси унинг ҳолатини ифодаловчи қўшимча тасодифий миқдорнинг *0* ва *1* қийматлари чексиз кетма-кетлиги сатрининг ҳолатига ҳам боғлиқ.

Табиий равишда савол туғилади: ушбу $P \neq NP$ тенгсизлик бардошли криптографик тизимлар мавжудлигининг зарурий ва етарлилик шартини ифодалайдими?

Ҳақиқатан ҳам бу шартнинг зарурийлиги – бардошли криптотизимлар учун $P \neq NP$ шартининг бажарилишига бевосита ишонч ҳосил қилиш мумкинлигидадир. Юқорида кўрилган мисолга қайтган ҳолда, ушбу

$L = \{(k1,d,i) | \exists$ маълумот $m$: $d = E_{k_1}(m)$ ва $m_i = 1\}$

тилни аниқлаймиз. Яъни тўплам $L \subset \Sigma^n$ бирор *n*-ўлчамли барча $m = (m_1, m_2, ..., m_i, ..m_n) \in \Sigma^n$ сўзлардан, *i*–бити *1* га тенг $m_i = 1$ бўлганлари бўлиб (уларнинг сони $2^{n-1}$ та), уларни $k_1$ -калит билан $E$ - бир томонламалик хусусиятига эга бўлган алгоритмдан фойдаланган ҳолда шифрланганда

$d = E_{k_1}(m)$ тенгликни қаноатлантиради. Ушбу $k_1$ ва $d$ параметрларни ҳамда $E$-алгоритмни билган ҳолда $d = E_{k_1}(m)$ ва $m_i=1$ тенгликларни қаноатлантирувчи барча $m = (m_1, m_2, ..., m_i, ..m_n) \in L \subset \Sigma^n$ топиш экспоненциал мураккабликка эга. Бундай аниқланган тил $L \in NP$ бўлиб, экспоненциал вақт бирлиги ичида бу тилда шундай $m$ матнларни кўрсатиш мумкинки, бу матнлар учун $d = E_{k_1}(m)$ ва унинг ($m$ нинг) $i$–бити *1* га тенг, яъни $m_i = 1$. Агар шундай бўлса, кириш сўзи ($k_1$, $d$, $i$) қабул қилинади, акс ҳолда рад этилади.

Агарда $P = NP$ деб фараз қилинса, $L$ тилни тушунувчи (қабул қилувчи) полиномиал мураккабликка эга бўлган $E$ алгоритм мавжуд бўлиб, $k_1$ ва $d$ параметрларни билган ҳолда, бу алгоритмдан фойдаланган ҳолда $d = E_{k_1}(m)$ ва $m_i = 1$ шартларни қаноатлантирувчи $m = (m_1, m_2, ..., m_i, ..m_n) \in L \subset \Sigma^n$ очиқ матнларни ҳисоблаш мумкин. Бундай хусусиятга эга бўлган алгоритмлар криптобардошсиз бўлади.

Ушбу $P \neq NP$ тенгсизлик ўринли бўлганда, $NP$ тўлиқ масала асосида яратилган ҳар қандай алгоритм махфий параметрларини аниқлаш ҳар доим ҳам $NP$ тўлиқ масала бўладими, яъни экспоненциал мураккабликка эга бўладими? Бундай саволга жавоблар носимметрик криптографик алгоритмларни таҳлил қилиш орқали қидирилган ҳамда $NP$ тўлиқ масала асосида яратилган ҳар қандай криптоалгоритм махфий параметрларини аниқлаш ҳар доим ҳам $NP$ тўлиқ масала бўлавермаслигига ишонч ҳосил қилинган. $NP$ тўлиқ масала унга фақатгина бошланғич киритиладиган қийматларнинг бирор чекли $n$ ўлчами бирор қийматдан кичик бўлмагандагина қийин ечиладиган масала бўлиши аниқланган. Бундан келиб чиқадики, $P \neq NP$ шартнинг бажарилиши криптобардошлилик учун етарли эмас. Шунинг учун ҳам криптобардошли алгоритмлар асосида бир томонламалик хусусиятига эга бўлган акслантиришлар ётади.

## 5.2. Хорижий шифрлаш алгоритмларининг бардошлилиги

4-бўлимда криптографлар орасида машҳур бўлган хорижий шифрлаш алгоритмларидан АҚШ давлат стандартлари – DES, Triple DES, AES, Россия Федерацияси давлат стандарти ГОСТ 28147-89 ва бошқалар кўриб чиқилган эди.

Ўзбекистон Республикасида фойдаланишда бўлган симметрик шифрлаш криптомодуллари асосан ГОСТ 28147-89 ва DES бўлиб улар соф дастурий кўринишда фойдаланиб келинган.

16-босқичли DES ни тўла очиш учун $2^{47}$ та танланган очиқ матн зарур бўлади. Уни очиқ матн билан очишга алмаштириш мумкин, лекин бунда $2^{55}$ та очиқ матн керак бўлади. Бунда $2^{37}$ та DES амалидан фойдаланилади.

Ўзбекистон Республикасида ГОСТ 28147-89 кўпдан бери қўлланилиб келинганлигини ҳисобга олиб, ГОСТ 28147-89 билан DES орасидаги асосий фарқларни келтириш ўринлидир:

– DES калитидан қисм калитларни вужудга келтиришда мураккаб жараёндан фойдаланилса, ГОСТ 28147-89да бу жараён жуда соддадир; лекин, DESда калитларни вужудга келтириш жараёнининг мураккаблиги шифрлаш тезлигига сезиларли таъсир этмайди.

– DESда *56* битли калит, ГОСТ 28147-89 да эса *256* битли калит ишлатилади. Агар *S*–блоклардаги махфий ўрин алмаштиришлар ҳисобга олинса, у ҳолда ГОСТ 28147-89 даги махфий ахборот ҳажми тахминан *610* битга тенг бўлади ва бу асосан ГОСТ 28147-89нинг юқори криптобардошлилигини таъминлайди;

– DESдаги *S*–блоклар кириши 6 бит, чиқиши 4 бит бўлса, ГОСТ 28147-89 даги *S*–блокларнинг кириши ҳам, чиқиши ҳам 4 бит, лекин DESда *S*–блоклар чизиқли криптотаҳлилга нисбатан оптималлаштирилган эмас. Иккала алгоритмда ҳам 8 тадан *S*–блок ишлатилади, лекин ГОСТдаги

*S*–блокнинг ўлчами DES даги *S*–блок ўлчамининг тўртдан бирига тенг ва улар махфий бўлиб, белгиланган ташкилотлар томонидан етказиб берилади. ГОСТ 28147-89 *S*–блоклари *0÷15* гача бўлган сонларнинг ўрин алмашувлари сифатида берилади:

– DESда регуляр бўлмаган P-блок деб аталувчи ўрин алмаштиришлардан, ГОСТ 28147-89да эса *11* битли чапга циклик силжитишдан фойдаланилади.

– DES 16 раундли, ГОСТ 28147-89 эса ундан *2* марта кўп шифрлаш раундларидан фойдаланилади;

Уч марта ҳар хил калит билан шифрланадиган Triple DESда намоён бўлган калит узунлиги ва унумдорлик муаммосига жавоб тариқасида кўпчилик криптографлар ва компаниялар янги блокли шифрларни таклиф этишди. Таклифлар орасида RSA Data Security компаниясининг RC2 ва RC5, Ascom компаниясининг IDEA, Entrust компаниясининг Cast, Cylink компаниясининг Safer, Counterpane Systems компаниясининг Blowfish алгоритмлари кўпроқ машҳур бўлиб қолди. Аммо улардан бирортаси ҳам стандарт даражасига ета олмади.

2001 йил DES ва Triple DES ўрнига белгиялик Д. Деймен ҳамда В. Райменлар томонидан яратилган ҳозирга кунда амалда бўлган AES стандарти – Rijandael алгоритми ишлаб чиқилди. У тезкор, содда, ҳимояланган, универсал ва смарт-картларда амалга ошириш учун қулайдир. Rijandael шифри яратувчиларининг баҳолашича ушбу алгоритм тўртинчи раунддаёқ криптотаҳлилнинг кўрсатилган усуллари учун етарли даражадаги бардошлиликка эга бўлади. Назарий жиҳатдан блок ўлчамига боғлиқ ҳолда 6-8 раунддаёқ чизиқли ва дифференциал криптотаҳлил усуллари маъносини йўқотади. Шифрда эса 10-14 раунд амалга оширилиши кўрсатилган. Бу эса Rijandael шифри кўрсатилган криптотаҳлил турларига етарли даражадаги заҳира билан бардошли деганидир.

ГОСТ 28147-89ни чизиқли ва дифференциал таҳлиллашнинг муваффақиятли бўлгани ҳақида ҳозиргача ҳеч қандай маълумотлар йўқ бўлгани боис уни жуда ҳам хавфсиз алгоритмларга қўйиладиган талабларга жавоб беради деб ҳисоблаш ўринли. ГОСТ 28147-89нинг баъзи *S*–блоклари DES нинг белгиланган *S*–блокларига нисбатан бўшроқ бўлса ҳам, уларнинг махфийлиги ҳамда ГОСТ 28147-89да босқичлар сони 2 марта кўплиги ГОСТ 28147-89нинг дифференциал ва чизиқли криптотаҳлилга бардошлилигини оширади.

ГОСТ 28147-89 алгоритмининг DES алгоритмидан асосий фарқи – $Z_2^{32}\ x\ Z_2^{48} \rightarrow Z_2^{32}$ акслантиришни ифодаловчи функцияларнинг тузилишида ва цикл калитларни ҳосил қилиш алгоритмидадир. Шунингдек ГОСТ 28147-89 алмаштиришларининг дастурий амалга ошириш учун соддалигидир.

Тузилиши бўйича ГОСТ 28147-89га яқин бўлган шифр DESни ўрганиш шуни кўрсатдики 16 раундли шифрни криптотаҳлил қилиш мумкин, лекин жуда катта миқдордаги маълумотларни талаб қилади. 20-24 раундли шифрларда эса бунинг назарий жиҳатдан имкони йўқ. ГОСТ 28147-89 32 раундли шифрлашни назарда тутади, бу эса кўрсатилган криптотаҳлил усулларига етарли даражадаги заҳира билан қаршилик қила олишини билдиради.

- Изланишлар шуни кўрсатадики, Россия стандарти бардошлилиги бўйича америка AES стандартидан қолишмайди. Хулоса қилиб шуни айтиш мумкинки, иккала алгоритм ҳам криптотаҳлилнинг мавжуд усуллари учун етарли бардошлиликка эга.

## 5.3. Хорижий носимметрик криптографик алгоритмларнинг бардошлилиги

### 5.3.1. Носимметрик криптографик алгоритмларнинг бардошлилиги

Носимметрик криптотизимлар симметрик криптотизимларга нисбатан ўнлаб марта катта узунликдаги (*512*, *1024*, *2048*, *4096* битли) калитлардан фойдаланади ва шу сабаб юзлаб марта секинроқ ишлайди. Бу ўз навбатида катта ҳажмли ахборотларни шифрлашда носимметрик криптотизимлардан фойдаланиш соҳасини чеклашга олиб келади. Аммо махфий калитларни тарқатиш, ЭРИ шакллантириш ва уни текшириш, аутентификация масалаларига тадбиқан носимметрик криптотизимларнинг аҳамияти беқиёсдир.

Хорижий носимметрик криптографик алгоритмлардан RSA, Эл Гамал, Шнорр, DSA ва ГОСТ Р 34.10–94 [1-4, 9, 14] криптографлар орасида машҳур. Ҳозирги кунда ЭЭЧларга асосланган алгоритмлар кўплаб халқаро, миллий ва соҳага оид стандартлар қаторидан ўрин олган бўлиб, улар жумласига Россия Федерациясининг ГОСТ Р 34.10-2001 [60], АҚШнинг EC-DSA-2000 [42], Кореянинг EC-KCDSA [34, 43], Германиянинг EC-GDSA [34, 43] ва Украинанинг ДСТУ 4145-2002 [61] стандартлари киради.

Ўзбекистон Республикасида фойдаланишда бўлган носимметрик криптографик модулларга ҳамдўстлик мамлакатларининг ўзаро алоқаларида фойдаланиш учун келишувга биноан ЭРИ стандартлари ГОСТ Р 34.10–94 [14]**,** ГОСТ Р 34.10–2001 асосида яратилган криптопровайдерлар киради. Яқин йилларгача кўпчилик банклар ва компаниялар ўзаро алоқаларда деярли халқаро стандарт мақомига кўтарилган RSA тизимидан, АҚШ стандарти DSA ва бошқа ЭРИ схемаларидан фойдаланиб келишган ва улардан фойдаланиш Ўзбекистон Республикасида ишлаб чиқилган норматив ҳужжатлар билан тартибга солинмаган эди. Бу схемалар тан олинган машҳур криптотаҳлил усулларига ва криптоҳужум турларига нисбатан криптотаҳлил амалларини бажариш вақти

*T>>300 mips-йил* бўлиши зарурлиги талабига жавоб бериши адабиётларда келтирилган.

Носимметрик криптотизимларнинг математик асоси бўлиб чекли майдон, группа, қисмгруппа кўринишидаги алгебраик структуралар ва уларда криптографик алгоритмга асос қилиб олинган модуль арифметикасининг махфийлик (секрет, лазейка)ка эга бир томонлама функция хизмат қилади. Махфийлик фойдаланувчи, масалан, ЭРИ соҳибининг шахсий махфийлиги бўлиб, унинг ошкора калитини ЭРИ шаклантиришда бевосита фойдаланилади. Шахсий махфийликнинг шахсга боғлиқлиги ахборот хавфсизлигини таъминлашнинг зарурий шартидир. Ошкора калит ЭРИ ҳақиқийлигини тасдиқлаш (верификациялаш), маълумот манбаини аутентификациялаш ва маълумот бутунлигига ишонч ҳосил этишда фойдаланиладиган асосий процедуралардир.

Аввал таъкидланганидек, махфийликни топиш криптотизимни барбод этишга олиб келиши боис уни топиш криптотаҳлил вазифалари орасида энг асосийси ҳисобланади ва бу масала 1-бўлимда келтирилган муаммоларни ҳал этишга келтирилади.

Носимметрик криптографик алгоритмларнинг бардошлилиги фойдаланилган хэш-функциянинг бардошлилиги ва чекли ҳалқаларда факторлаш, майдонда ва ЭЭЧ группасида дискрет логарифмлаш муаммоларининг ҳисоблаш мураккаблиги билан белгиланади. Ҳозирча энг тезкор криптотаҳлил усули сифатида чекли ҳалқаларда факторлаш ва майдонда дискрет логарифмлаш муаммоларини ҳал этишда сонли ғалвир усули NFS ҳисобланса, ЭЭЧ группасида дискрет логарифмлаш муамосини ҳисоблашнинг энг самарали алгоритми Поллардннг $\rho$-алгоритмидир.

Сонли майдон ғалвири усулининг мураккаблиги

$C_2=O(\exp(c(\ln p)^{1/3}(\ln\ln p)^{2/3}))$ амал билан баҳоланади, бу ерда $c\approx 1,9223$.

[62] да немис олимлари *530*-битли (*160* ўнли хонали) туб модуль $p$ учун дискрет логарифмлаш муаммосини ҳал этишгани ҳақида маълум этилган. Бу эса дискрет логарифм муаммосига асосланган алгоритмларнинг криптографик бардошлилиги ва хавфсизлик параметрларига бўлган талабларни кучайтиришга олиб келади.

Шундай қилиб, факторлаш ва дискрет логарифмлаш муаммоларининг мураккаблиги билан белгиланадиган барча бир хил узунликдаги шахсий калитлардан ва бир хил ЭЭЧдан фойдаланган ҳолда хорижий криптографик алгоритмларнинг бардошлилигининг юқори чегараси

$C_2=O(\exp(c(\ln p)^{1/3} (\ln \ln p)^{2/3}))$, $C'_2=O(\exp(c(\ln n)^{1/3} (\ln \ln n)^{2/3}))$

ифодалар бўйича ҳисобланадиган амаллар сони билан белгиланади, бу ерда $c\approx 1,9223$, $n=p_1 * p_2$, $p_1 * p_2$, $p$-туб сонлар.

ЭЭЧ нуқталари группасида дискрет логарифмлаш муаммосини Поллардниг $\rho$-алгоритмига биноан ҳал этиш учун зарур амалларнинг юқори чегараси қуйидаги ифода бўйича топилади:

$$I_\rho = \sqrt{\frac{\pi q}{2}},$$

бу ерда туб модуль $p$ ва ЭЭЧ нуқталарининг тартиби $q$ учун $2^{p-2} < q < 2^p$, $p > 2^{256}$ ифода ўринлидир.

Масалан $q = 2^{256}$ учун:

$$I_\rho = \sqrt{\frac{\pi q}{2}} \approx 2^{127}.$$

Факторлаш ва ЭЭЧ группасида дискрет логарифмлаш мураккабликларини таққослама таҳлили ЭЭЧларнинг баҳслашувдан ҳоли афзалликларини намоён этди [1]. 12-жадвалда таққослама маълумотлар

келтирилган (маълумотлар туб майдонда дискрет логарифмлаш муаммоси учун ҳам осон ҳисобланади).

12-жадвал

**Криптотаҳлил мураккабликлари бўйича маълумотлар**

| Алмаштириш модули узунлиги | ЭЭЧ группасида криптотаҳлил мураккаблиги | RSA модулини факторлаш мураккаблиги |
|---|---|---|
| 192 бит | $2^{95,82} \approx 10^{29,21}$ | $2^{40,41} \approx 10^{12,32}$ |
| 256 бит | $2^{127,82} \approx 10^{39}$ | $2^{40,56} \approx 10^{14,5}$ |
| 512 бит | $2^{255,82} \approx 10^{78}$ | $2^{65,15} \approx 10^{19,86}$ |
| 1024 бит | $2^{511,82} \approx 10^{156}$ | $2^{88,47} \approx 10^{27}$ |

XXI асрнинг бошидан бошлаб носимметрик криптографиянинг анъанага айланиб қолган криптотизимлардан бардошлилиги ЭЭЧ группасида дискрет логарифмлаш муаммосининг мураккаблигига асосланган тизимларга ўтиш бошлангани кўзга ташланди [1].

### 5.3.2. Ўзбекистон Республикасида ишлаб чиқилган электрон рақамли имзо алгоритмининг хорижий алгоритмлар билан қиёсий характеристикалари

Ўзбекистон алоқа ва ахборотлаштириш агентлиги Фан-техника ва маркетинг тадқиқотлари марказида 2003-2009 йиллар давомида олиб борилган илмий-тадқиқот ишлари натижасида Ўзбекистон Республикасининг давлат стандарти O'z DSt 1092:2005, O'z DSt 1092:2009 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Электрон рақамли имзони шакллантириш ва текшириш жараёнлари» [63] ишлаб чиқилди.

O’z DSt 1092:2009 стандарти O’z DSt 1092:2005нинг такомиллаштирилган русуми бўлиб, уларни қисқача O’z DSt 1092 деб белгилаймиз. Ишлаб чиқишда O’z DSt 1092 O’z DSt 1092 учун ***прототип сифатида АҚШ стандарти DSA танланган*** бўлиб, унда барча ўзгартиришлар прототип даражасида аниқ ва равшан берилган.

Стандартда имзоланган хабарни p-**NEW** схемаси бўйича тиклаш ғояси ва К. Шнорrнинг имзо узунлигини қисқартиришга йўналтирилган ғоясидан ҳам фойдаланилган.

Мазкур стандартни ишлаб чиқиш жарёнида унинг муаллифлари ўз олдиларига стандартнинг етарли бардошлилиги ва тезкорлигини таъминлаш ҳамда унда хорижий давлат стандартларида мавжуд бўлган камчиликларни қайтармаслик каби мақсадларни қўйган эдилар.

Маълумки, кўпчилик хорижий давлат стандартларининг асосий камчилиги ЭРИ сохталаштирилган бўлса, буни пайқаб олишишга оид механизм ва маълумотларнинг йўқлигидир. ЭРИни сохталаштириш эса бадният кимса томонидан факторлаш, дискрет логарифмлаш ёки эгри чизиқли дискрет логарифмлаш масалаларидан бирини ҳал этиш учун унинг вақт ва ҳисоблаш ресурслари етарли бўлганда амалга оширилиши мумкин. Зеро, компьютер технологияларининг унумдорлиги ва мураккаб ҳисоблаш усуллари ривожи темплари йилдан-йилга ўсиши бундай мураккаб ҳисоблаш масалаларини самарали ечиш усуллари яқин келажакда топилмаслигига ҳеч ким кафолат бера олмайди.

Шуни эътиборга олиб ЭРИни шакллантириш жараёнига сеанс калити процедурасини киритиш билан ЭРИ сохталигини аниқлашнинг захиравий йўли белгиланди.

O’z DSt 1092 стандарти бардошлилигини баҳолаш усулларидан фойдаланишда унинг DSA ва ГОСТ Р 34.10–2001 стандартларига ўхшаш ва ўзига хос фарқли томонларни эътиборга олиш лозим. O’z DSt 1092

стандартининг ***ўзига хос томонлари унинг бардошлилигини оширишга ва бошқа стандартларга хос камчиликларни йўқотишга йўналтирилган.***

Шу кунда машҳур бўлган ЭРИ алгоритмларини қуйидаги белгилар асосида тасниф этиш мумкин: алгебраик структура, процедураларда фойдаланиладиган асосий амаллар, модул типи ва ўлчамлари, даража асоси типи, ЭРИ узунлигини қисқартиришга ёндашув, ёпиқ калит шакли, ЭРИ шакли, бардошлилик, текшириш калити шакли, имзо текшириш натижаси шакли, фойдаланиладиган протокол.

O’z DSt 1092 стандарти учун бу белгиларга яна тўртта белги қўшилади: фойдаланиладиган маром, биргаликдаги калитлар типи, сохта имзони аниқлаш калити типи, имзони тан олмаслик имконияти (агар имзо сохта, лекин уни текшириш натижаси ижобий бўлса).

Қуйидаги 13-жадвалда шу белгилар бўйича O’z DSt 1092 нинг DSA ва ГОСТ Р 34.10-2001 билан қиёсий характеристикалари келтирилган [2].

13-жадвал

**O’z DSt 1092:2005, O’z DSt 1092:2009 нинг DSA ва ГОСТ Р 34.10-2001 билан қиёсий характеристикалари**

| **Белгилар** | **O’z DSt 1092:2005 O’z DSt 1092:2009** | **DSA** | **ГОСТ Р 34.10-2001** |
|---|---|---|---|
| *Алгебраик структура* | Параметрли алгебра (параметрли чекли мультипликатив группа) | Чекли оддий майдон | Чекли оддий майдонда аниқ-ланган ЭЭЧ |
| *Модул типи ва ўлчамлари* | Туб сон $p > 2^{255}$ (Афзаллиги *юқори тезкорликда*) | Туб сон $2^{511} < p < 2^{1024}$ | Туб сон $p > 2^{255}$ |

13-жадвалнинг давоми

| **Белгилар** | **O'z DSt 1092:2005**<br>**O'z DSt 1092:2009** | **DSA** | **ГОСТ Р**<br>**34.10-2001** |
|---|---|---|---|
| *Процедуралар да фойдаланилган асосий амаллар* | 1. Параметрли кўпайтириш<br>2. Параметр билан даражага ошириш<br>3. Параметр билан тескарилаш<br>4. Тескарилаш | 1 Кўпайтириш<br>2. Қўшиш<br>3. Даражага ошириш<br>4. Тескарилаш | 1. Қўшиш<br>2. Инкор<br>3.Кўп марталик қўшиш<br>4. Конкатенация **(***Камчилиги* амалларнинг мураккаблигида) |
| *Даража асоси типи* | Махфий – *g*<br>(Афзаллиги *дискрет логарифмлаш масаласини қўйиш мураккаблигида*) | Ошкора - *g*<br>(Камчилиги *дискрет логарифмлаш масаласини қўйиш осонлигида)* | Ошкора нуқта *P*<br>(Камчилиги *эллиптик эгри чизиқларда дискрет логарифмлаш масаласини қўйиш осонлигида)* |
| *ЭРИ узунлигини қисқартиришга ёндашув* | *Фактор((p-1) нинг туб кўпайтувчиси)дан фойдаланиш*<br>$2^{254} < q < 2^{256}$ | *Фактордан фойдаланиш*<br>$2^{159} < q < 2^{160}$ | *Циклик группанинг тартибидан фойдаланиш*<br>$2^{254} < q < 2^{256}$ ,<br>*q - группа тартиби* |
| *Ёпиқ калит шакли* | Учлик *(x, u, g)*<br>(Афзаллиги *махфийлик даражаси ошишида)* | Параметр *x* | Параметр *d* |
| *ЭРИ шакли* | Жуфтлик *(r, s)* $\mu=0$ да**,** учлик *(r, s, $y_1$)* $\mu=1$ да<br>(Камчилиги $\mu=1$ да) | Жуфтлик *(r, s)* | Жуфтлик *(r, s)* |
| *Бардошлилик* | $\mu=1$ *да даража параметри муаммосининг мураккаблигига* асосланган<br>**(**Афзаллиги *DSA га нисбатан юқори бардошлилигида)* | Модул *512-1024* бит бўлганда *дискрет логарифмлашнинг мураккаблигига асосланган* | Модул *255* битдан катта бўлганда *ЭЭЧда дискрет логарифмлашнинг мураккаблигига асосланган* |
| *Текшириш калити шакли* | Жуфтлик *(y, z)* $\mu=0$ да учлик *(y, z, $y_1$)* $\mu=1$ да<br>**(**Афзаллиги *сохта имзони аниқлашда)* | Жуфтлик<br>*(g, y)* | Параметр – *Q* |

13-жадвалнинг давоми

| **Белгилар** | **O'z DSt 1092:2005<br>O'z DSt 1092:2009** | **DSA** | **ГОСТ Р<br>34.10-2001** |
|---|---|---|---|
| *Имзо текшириш натижаси шакли* | Хэш-функция қиймати ёки хэшлашдан фойдаланилмаганда хабар блоки<br>**(**Афзаллиги хэшланиши шарт бўлмаган қисқа хабарларни узатмаслик мумкинлиги*)* | Ижобий ёки салбий | Ижобий ёки салбий |
| *Фойдаланиладиган протокол* | Стандартга хос *(μ=1 маромда* камчилиги *калитларни рўйхатга олиш марказига қўшимча юклама тушишида)* | Анъанавий | Анъанавий |
| *Фойдаланиладиган маром* | 1. Сеанс калитисиз *(μ=0***)**<br>2. Сеанс калитили *(μ=1)*<br>**(**Афзаллиги *янги имкониятлар туғилишида***)** | Сеанс калитисиз | Сеанс калитисиз |
| *Биргаликдаги калитлар типи* | *R, $R_1$* параметрлар<br>**(**Афзаллиги *махфийлик даражасининг ортишида*) | Йўқ | Йўқ |
| *Сохта имзони аниқлаш калити типи* | Жуфтлик *($R_1$, $y_1$)*<br>$R_1$ – назорат калити<br>$y_1$ – сеанс ошкора калити<br>**(**Афзаллиги**)** | Йўқ | Йўқ |
| *Имзони тан олмаслик имконияти* | Мавжуд<br>**(**Афзаллиги**)** | Йўқ | Йўқ |

O'z DSt 1092да алгебраик структура сифатида П.Ф. и Х.П. Хасановлар томонидан таклиф этилган *параметрли алгебра* қабул қилинган [9]. *Унда* модул арифметикасининг яширин(махфий) йўлли *янги бир томонлама функцияси*

(махфий параметрли бир томонлама функция) *аниқланган бўлиб*, бу функция қонуний фойдаланувчилар учун анъанавий даражага ошириш функцияси каби осон ҳисобланади, аммо яширин йўлга тегишли параметр маълум бўлмаган фойдаланувчилар уни ҳисоблашлари учун даража параметри муаммосини ечишга мажбурдирлар. Криптографик процедураларда фойдаланиладиган асосий амаллар параметрли кўпайтириш, параметр билан даражага ошириш ва параметр билан тескарилаш амалларидир. Анъанавий бир томонлама даражага ошириш функцияси мазкур функциянинг хусусий холи эканлиги бу функция асосида яратиладиган криптотизимларнинг *бардошлилиги* анъанавий криптотизимларнинг бардошлилигидан ҳеч қачон кам бўлмаслигини *кафолатлайди*.

Махфий параметрли бир томонлама функцияга *осонгина* иккитадан ортиқ махфийликни ўрнатиш мумкин. Булар даража кўрсаткичи, даража асоси ва биргаликдаги махфий параметрлардир.

O’z Dst 1092 стандарти маълум хорижий давлат стандартларига нисбатан ўзига хос фарқли хусусиятларга эга бўлиб, уларнинг ҳар бири бардошлиликни оширишга хизмат қилади. Булар қаторига қуйидагилар киради:

- *параметрли алгебрадан фойдаланиш*;
- бир томонлама функцияда *иккита шахсий ва битта ёки иккита биргаликдаги махфийлик* қатнашиши*;*
- сохта имзонинг *аниқланувчанлиги*;
- имзо сохталигини *аниқлаш* калитидан фойдаланиш;
- ЭРИ *сохталигини исбот этиш имконияти*;
- *стандартнинг ўзига хос протоколларидан* фойдаланиш**.**

*μ=0* маромида бошқа давлат стандартларида қўлланиладиган протоколларга ўхшаш протоколлардан ва узунлиги *1024* бит ва ундан ортиқ туб модуллардан фойдаланилади.

*μ=1* маромида O’z Dst 1092 *стандартининг ўзига хос протоколларидан* ва узунлиги *256* бит ва ундан ортиқ туб модуллардан фойдаланилади. Бундай протоколларга биноан, ошкора калитлар инфратузилмасида фақатгина Калитларни Рўйхатга Олиш Маркази (КРОМ) инфратузилмасидан фойдаланувчилар билан ўзи орасида ҳимояланган алоқа каналини ташкил этиш учун ишончли криптотизимга эга бўлиши етарлидир. Бундай криптотизимни *параметрли алгебрада* “RSA тизимининг аналоги” кўринишида амалга ошириш мақсадга мувофиқ. “RSA тизимининг аналоги”да инфратузилма фойдаланувчилари учун ошкора калит бўлиб *(n, e, R)* учлиги, махфий калит бўлиб *(d, $R_i$)* жуфтлиги қабул қилинади. Бу ерда *n* - икки ҳар хил туб сонлар кўпайтмаси, *e* - туб сон бўлган даража кўрсаткичи, *R* – параметр, $d \equiv e^{-1} (mod\ \varphi(n))$, $\varphi(n)$ - Эйлер пи-функцияси, $R_i$ - КРОМ ва *i*-имзо муаллифининг *биргаликдаги махфий назорат калити*.

Бунда сеанс калити ва уни КРОМга жўнатувчи муаллиф орасида бир-бирига бир қийматли мос келиши кафолатланади. КРОМ сеанс калитини ўз имзоси билан тасдиқлаши, келишмовчиликлар содир бўлганда сеанс калитининг кимга тегишли эканига гувоҳлик бериши мумкин.

O’z DSt 1092 *стандартининг ўзига хос протоколлари ошкора* назорат калитли ва *ёпиқ* назорат калитли *синфларга бўлинади*.

*Ошкора* назорат калитли протокол қуйидаги қадамларни ўз таркибига олади:

- муаллиф томонидан *(r, s, $y_1$)* шаклида ЭРИ шакллантириш; бу ерда $y_1$ фойдаланувчилар гуруҳи учун умумий бўлган ошкора назорат калити $R_1$ асосида генерацияланган;
- *(n, e, $R_i$)* дан фойдаланиб “RSA тизимининг аналоги” да $y_1$ шифрлаш ва шифрматнни КРОМга жўнатиш, хабар *M* билан *(r, s)* ни эса қабул қилувчи фойдаланувчига жўнатиш;

- КРОМда *(n, d, $R_i$)* дан фойдаланиб “RSA тизимининг аналоги” да $y_1$ ни тиклаш;
- *(n, d, R)* дан фойдаланиб “RSA тизимининг аналоги” да $y_1$ остига КРОМ имзосини шакллантириш ва имзоланган $y_1$ ни КРОМ маълумотлар базасига жойлаштириш.

ЭРИни текшириш босқичида хабар *M* билан *(r, s)* ни қабул қилган фойдаланувчи **(**фойдаланувчилар гуруҳи) КРОМ маълумотлар базасидан имзоланган $y_1$ ни қабул қилиб ундаги КРОМ имзосининг ҳақиқийлигини, сўнгра *(r, s)* ҳақиқийлигини текширади.

*Ошкора* назорат калитили протоколнинг зарурий бардошлилиги КРОМ *ва i*-имзо муаллифининг *биргаликдаги махфий назорат калити* $R_i$ нинг бардошлилиги туфайли таъминланади; $R_i$ нинг бардошлилиги факторлаштириш муаммосининг ва биринчи мураккаблик сатҳига оид даража параметри муаммосининг мураккаблигига асосланади.

*Ёпиқ* назорат калитили протокол қуйидаги қадамларни ўз таркибига олади:

- муаллиф томонидан *(r, s, $y_i$)* шаклида ЭРИ шакллантириш; бу ерда $y_i$ фойдаланувчилар жуфти *(i, j)* учун биргаликда махфий назорат калити $R_{ij}$ асосида генерацияланган;
- *(n, e, $R_i$)* дан фойдаланиб “RSA тизимининг аналоги” да $y_i$ шифрлаш ва шифрматнни КРОМга жўнатиш, хабар *M* билан *(r, s, $y_i$)* ни эса қабул қилувчи фойдаланувчига жўнатиш;
- КРОМда *(n, d, $R_i$)* дан фойдаланиб “RSA тизимининг аналоги” да $y_i$ ни тиклаш ва $y_i$ ни КРОМ маълумотлар базасига жойлаштириш.

ЭРИни текшириш босқичида *M* билан *(r, s, $y_i$)* ни қабул қилган фойдаланувчи *(r, s)* ҳақиқийлигини текширади.

Имзолаган хабарни ҳар бир *i*-қабул қилувчи фойдаланувчи ёки учинчи томон мавжуд протоколлардан фарқли ўлароқ хабар *M* остидаги *(r, s)*

ҳақиқийлигини тасдиқлаш учун биргаликда махфий назорат калити $R_{ij}$ га мос алоҳида ошкора сеанс калити $y_i$ га эга бўлиши зарур. Мазкур протоколдан хабар $M$ остидаги $(r, s)$ ҳақиқийлигини тасдиқлаш учун фойдаланувчилар давраси қатъий чекланган ҳолларда, яъни жуда муҳим ҳужжатлар айланишида фойдаланиш мақсадга мувофиқдир.

*Ёпиқ* назорат калитили протоколнинг зарурий бардошлилиги КРОМ ва *i*-имзо муаллифининг *биргаликдаги махфий назорат калити* $R_i$ нинг ва фойдаланувчилар жуфти $(i, j)$ учун биргаликда махфий назорат калити $R_{ij}$ бардошлилиги туфайли таъминланади; $R_i$ ва $R_{ij}$ нинг умумий бардошлилиги факторлаштириш муаммосининг ва биринчи ҳамда иккинчи мураккаблик сатҳларига оид даража параметри муаммосининг мураккаблигига асосланади.

Иккала протокол ҳаттоки ЭРИ *ёпиқ калити барчага маълум* бўлган холда ҳам туб модулнинг *қуйи чегарасида* $(p \approx 2^{256})$ етарли бардошлиликни таъминлай олади.

O'z DSt 1092 стандартидан фойдаланувчилар қуйидагиларни эътиборга олишлари мақсадга мувофиқ:

- ошкора калитлар инфратузилмаси ривожининг бошланғич босқичида $\mu=0$ маромидан, анъанавий протоколлардан ва узунлиги *1024* бит ва ундан ортиқ модуллардан фойдаланиш;
- агар КРОМ $\mu=1$ маромда стандартнинг ўзига хос протоколлар асосида хизмат кўрсатишга тайёр бўлса, унда узунлиги *1024* бит ва ундан ортиқ модуллардан фойдаланиш;
- агар криптомодул махсус аппаратли кўринишда тайёрланган бўлса, унда узунлиги *256* битдан *1024* битгача модуллардан фойдаланиш.

Параметрли алгебрада яратилган криптоалгоритмлар бадошлилигининг ошиши $g$ - махфий элемент, $R$, $R_i$ ёки $R_{ij}$ – фойдаланувчилар гуруҳи (ёки жуфти) учун биргаликдаги махфий калит бўлганда даража параметри муаммоси (3-бўлим) туғилиши билан боғлиқдир.

## 5.4. Криптотаҳлилда янги технологиялардан фойдаланиш

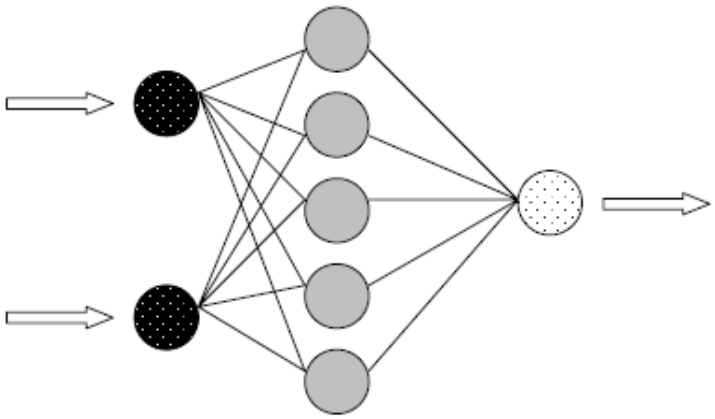
Бу параграф криптографик тизимларнинг тадқиқотларига бўлган энг ноодатий ва етарлича мунозарали ёндашувларига бағишланган. Шу билан бирга бу усуллар шифрларни бузишда катта бурилиш ясамаган ва уларга амалиётга нисбатан илмий қизиқиш кўпроқ. Шундай бўлсада, бу усуллар ўзига хослиги билан диққатга сазовордир; ундан ташқари, криптологияда уларнинг аҳамияти ўсиб бориши эҳтимолдан ҳоли эмас.

### *Нейрон тўрлари*

Криптотизимни «қора қути» деб қараш мумкин, яъни ички структураси номаълум, лекин киришга буйруқ ёки маълумот сигналларини юбориб, чиқишдан натижа олиш мумкин. Криптотаҳлилнинг вазифаси – бу тизимни идентификация қилиш, яъни киришига келадиган ва чиқишидан олинадиган сигналларга асосланиб, унинг структурасини аниқлаш. Бу масалани ечиш усулларидан бири нейрон тўрлари ҳисобланади. Сунъий нейрон тўри – математик модель ҳамда содда процессорларнинг ўзаро таъсирланувчи ва бирлашган тизимини ўзида намоён қилувчи параллел ҳисоблаш қурилмаларидир. Бу процессорлар, айниқса шахсий компьютерларда ишлатиладиган процессорларга нисбатан ғоятда соддадир. Бундай тўрлардаги ҳар бир процессор фақат даврий равишда ўзи қабул қиладиган ва даврий равишда бошқа процессорларга юборадиган сигналлар билан иш кўради. Шундай бўлсада ўзаро таъсир бошқарувига эга бўлган етарлича катта тўрга бирлашувчи бундай локал содда процессорлар биргаликда етарли даражада мураккаб масалаларни амалга оширади [25].

Бу тушунча фикрлаш давомида мияга келувчи жараёнларни ўрганиш ва бу жараёнларни моделлаштиришга уриниш давомида вужудга келган. Ҳосил бўлган модель сунъий нейрон тўрлари (СНТ) деб аталади [25]. Содда нейрон

тўрлари тасвири 6-расмда келтирилган. Кириш элементлари қора ранг, чиқиш элементлари эса оқ ранг билан тасвирланган.



6-расм . Нейрон тўрлари

Брюс Шнайер ўзининг «Амалий криптография» [14] китобида криптотаҳлилда нейрон тўрларидан фойдаланилишига ишончсизлик билан ёндашади: бузиш жараёни ўрганишга йўл қўймайди: ёки сиз калитни ошкор қиласиз ёки аксинча.

Нейрон тўрлари ўрганишга йўл қўядиган структураланган муҳитда яхши ишлайди. Шундай бўлсада, бу йўналишдаги тадқиқот ишлари давом этмоқда.

[25, 64] мақолада «қора қутининг нейроаниқлагичи» модели қурилишига асосланган анъанавий ва оқимли криптотизимларга «қора қутининг ҳужуми» ишлаб чиқилган. Бу ерда икки мақсад қўйилади: биринчидан, очиқ ва уларга мос келган шифрматнлар асосида калитни аниқлаш, иккинчидан, тадқиқ қилинаётган криптотизимнинг нейро-моделини яратиш. Тизимни идентификация қилиш - «қора қути»нинг кириш ва чиқиш маълумотларига кўра ва номаълум функциясини нейрон тўри модели билан аппроксимация қилишга қараб, тизимни ишлаш қоидасини аниқлашдан иборат бўлади.

Биринчи босқич аниқ архитектураси ва ўргатувчи алгоритми билан характерланувчи нейрон моделни танлашдан иборат. Танлаш синаш ва хатоликлар усули орқали амалга оширилади. Криптограмма ва очиқ матнларнинг маълум жуфтликлар тўплами икки қисм тўпламга бўлинади, улардан бири тўрни ўқитиш учун, иккинчиси эса ҳосил бўлган моделни берилган аниқлик мезонига мослигини текшириш учун ишлатилади.

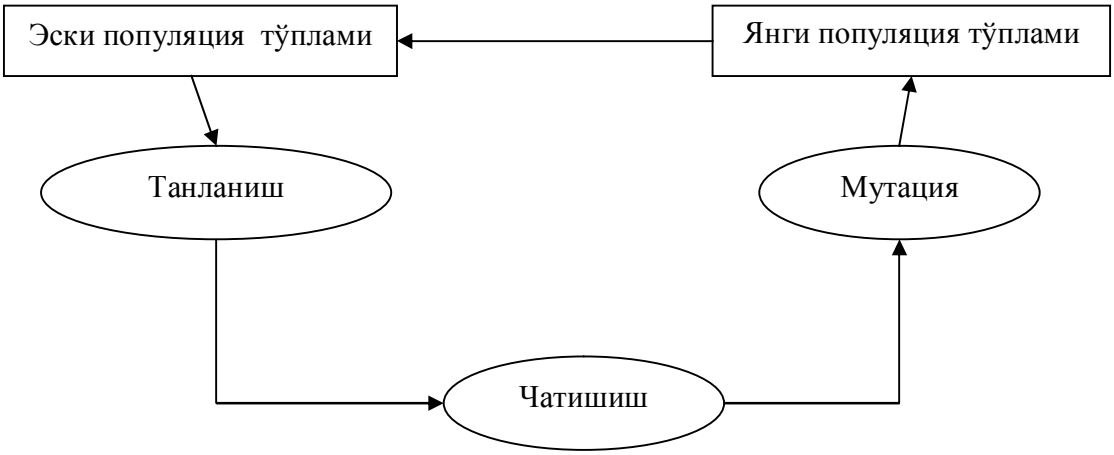
Энг оптимал модель бу энг кам нейронга эга бўлган ва шу билан бирга мезонларни қаноатлантирувчи моделдир. [64] да келтирилган тизим ёрдамида оқимли шифр ва Вижинернинг анъанавий кўп алифболи шифрининг криптотаҳлили амалга оширилган. Хатоликнинг бошланғич ҳолатини $10^{-5}$ даражага қўйилганда 100% аниқлик билан натижа берувчи криптотизим моделини ҳосил қилиш мумкин бўлади. Бошқа замонавий усуллар билан таққослаган ҳолда бундай ёндашувнинг афвзаллигига натижанинг фойдаланилаётган тил ва унинг статистик характеристикаларига боғлиқ эмаслиги киради, чунки билимни олиш учун тизим адаптив ўқитиш жараёнидан фойдаланади. [65] мақолада DESни бузиш учун нейрон тўрларидан фойдаланиш ҳақида гап боради. Ўргатиш жараёнида очиқ матн ва криптограмманинг *2240* та жуфти ишлатилган, оқибатда 98% гача аниқликдаги натижалар олишга эришилган. Муаллифлар ишлаб чиқилган стратегияга асосланиб AESни криптотаҳлил қилишни режалаштирганлар.

***Генетик алгоритмлар***

Рюкзакни тўлдириш ҳақидаги масалага асосланган дастлабки шифрлардан бири Меркли ва Хеллманлар томонидан 1978 йилда таклиф этилган [66]. Бу очиқ калитли шифрлаш тизимини яратишга бўлган илк уринишлардан бири эди. Шунга қарамасдан алгоритмнинг кўпчилик русумлари бардошсизлиги аниқланган. 1983 йилда Брикел зичлиги кам бўлган рюкзакка асосланган криптотизимларни бузиш усулини илгари сурди. Бир йил ўтгандан

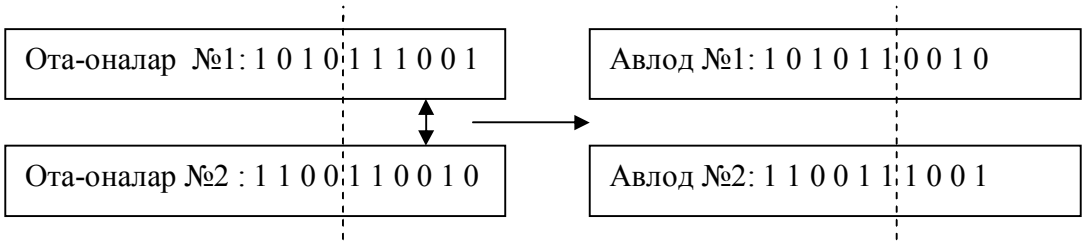
сўнг Шамир рюкзаксимон криптотизим асосига ҳужум уюштиришнинг полиномиал алгоритмини ишлаб чиқди. Шундан кейингина бу муаммога асосланган бошқа кўпчилик тизимлар таклиф қилинган: бир нечта кетма-кет рюкзаклар, Грэм-Шамир рюкзаги ва бошқалар. Ушбу тизимларнинг барчаси учун фош қилиш усуллари яратилган [25].

[25, 67] мақолада рюкзакни тўлдиришга асосланган яна бир криптотаҳлил усули таклиф этилган. Бундай ёндашишнинг фарқли томони унинг универсаллиги, яъни рюкзаксимон криптотизимларнинг барчасига қўллаш имконининг мавжудлиги ҳамда ишлашининг оддийлигидадир. Бу усул генетик алгоритмлардан фойдаланишга асосланган. Генетик алгоритмлар Джон Холланд томонидан яратилган бўлиб, ўзида “эволюцион дастурлаш” деб аталувчи модификацияни номоён қилади. Холланд ғояси биологиядан маълум бўлган табиий танланишга асосланган алгоритм ёки тасодифий излашга “йўналтирилган” алгоритм яратишдан иборат. Процедуранинг бошланиш босқичида мумкин бўлган популяциялар тўплами яратилади. Ушбу тўплам асосида ечимларнинг янги авлодлари келиб чиқади, улар ўз навбатида кейинги авлод учун “бирламчи маълумотлар” вазифасини бажаради ва ҳ.к. Генетик алгоритм циклининг умумий кўриниши 7-расмда келтирилган ва у танланиш, чатишиш ва мутация босқичларини ўз ичига олади.




7-расм. Генетик алгоритм циклининг умумий кўриниши

Популяциянинг яхши вакиллари янги популяция ҳосил қилиш учун саралаб олинади; шу тарзда тахмин бўйича ҳар бир янги популяция олдингисидан яхши ечимларни ўзида мужассам қилиши керак. Кўпчилик ҳолларда бу ҳақиқатга мос келади. Популяция бинар сатрлар тўпламидан ташкил топади. Ҳар бир бинар сатр муаммонинг ечими ҳисобланади ва хромосома деб номланади. Генетик алгоритмнинг дастлабки босқичи танланиш бўлади. Танланиш жараёнида янги популяция яратилишида фойдаланиладиган сатрлар аниқланади ва улар эркин равишда танланадиган “Ота-оналар” нинг янги авлодларини яратишда фойдаланилади. Аммо популяциянинг “энг яхши нусхалари”нинг танланиш имкониятлари юқори бўлади. Шу йўсинда алгоритм излашнинг истиқболли йўналишлари томон силжийди. Кейинги босқич – чатишиш босқичи. Чатишиш шундан иборатки, бунда $r$ узунликдаги танлаб олинган сатрлар жуфтлиги учун ихтиёрий тарзда $s \in \{1, ..., r\}$ сони танланади. “Ота-оналар” $s+1$ дан $r$ гача битларни алмашишади; шу йўсинда хромосомалар авлоди ҳосил бўлади.




8-расм. Хромосомалар авлоди

Якунловчи босқич – мутация. Алгоритмни бошланғич ҳолатдан ишга туширганда хромосомаларнинг қайта ҳосил бўлишига олиб келувчи мутациянинг кичик эҳтимоллиги ўрнатилади (8-расм).

Бу босқичлар циклдан чиқиш шартини қаноатлантирмагунча қайтарилади (Бундай шартларга ечимлар тўпламининг энг юқори сонидан ошиб кетиши мисол бўла олади).

Рюкзак тўлдириш ҳақидаги масалаларнинг аниқ ифодасини кўриб ўтамиз. Турли оғирликдаги предметлар тўплами берилган бўлсин; баъзи бир предметларни оғирлиги маълум қийматга тенг бўладиган қилиб рюкзакка жойлаштириш мумкинлигини аниқлаш талаб этилади. Янада аниқлаштириладиган бўлинса, масала қуйидаги кўринишни олади: $M_1, M_2,..., M_n$ қийматлар тўплами ва $S$ йиғинди қиймат берилган, шундай $b_i$ қийматини ҳисоблаб топиш керакки, бунда $S = b_1M_1 + b_2M_2 +...+ b_nM_n$ бўлсин. Бу ерда $b_i$ 0 ёки 1 бўлиши мумкин. $b_i = 1$ қиймати $i$ – предмет рюкзакка солинишини, $b_i = 0$ эса солинмаслигини билдиради. Бу ердан яққол кўринадики, рюкзак таркиби битлари $b$ нинг қийматларига мос келган хромосома кўринишида бўлади. «Энг яхши хромасома»ни танлаш функцияси танланган рюкзак оғирлигининг берилган сонга яқинлигини баҳолайди. Функция қиймати [*0; 1*] диапазонида жойлашади, бунда *1* қидирилаётган оғирлик билан аниқ мос тушишини англатади. Агар бирор рюкзакнинг оғирлиги $S$ нинг бутун қийматидан $x$ сонга ошиб кетса, бошқа рюкзакнинг оғирлиги аксинча талаб қилинганидан худди

ўша $x$ сонга кичик бўлса, у ҳолда «энг яхшиси» деб охириги рюкзак ҳисобланади. Бу функциянинг яна ҳам формал ифодаси қуйида келтирилган:

1. Ихтиёрий хромосома ва $S$ нинг қидирилаётган қиймати орасида мавжуд бўлиши мумкин бўлган энг катта айирмани топиш: $\Delta_{\max} = \max(S, \widetilde{S} - S)$. Бу ерда $\widetilde{S}$ - рюкзакни жойлаштиришда ишлатилувчи барча компонента лар йиғиндиси.

2. Қаралаётган хромосомага мос келувчи рюкзак оғирлигини топиш ва уни $S'$ деб белгилаб қўйиш.

3. Агар $S' \le S$ бўлса, у ҳолда хромосома «сифати» қуйидаги қиймат билан баҳоланади: $\alpha = 1 - \sqrt{\frac{|\widetilde{S} - S|}{S}}$.

4. Агар $S' > S$ бўлса, у ҳолда $\alpha = 1 - \sqrt{\frac{|\widetilde{S} - S|}{\Delta_{\max}}}$.

Криптотаҳлил учун мақолада қўлланилган рюкзакни тўлдириш ҳақидаги масалаларнинг умумий алгоритми қуйидаги кўринишга эга:

1. Иккилик хромосомаларнинг ихтиёрий популяцияси яратилади.

2. Ҳар бир хромосома учун α (баҳолаш функцияси) қиймати ҳисобланади.

3. Қўлга киритилган коэффициентлар асосида табиий танланиш амалга оширилади.

4. 3-босқичда танлаб олинган турларга чатишиш қўлланилади.

5. Авлодлар мутация жараёнига учрайди.

6. Янги популяциялар тўплами таҳлил қилинади, кейин «энг яхши хромосомалар» ажратилади.

Авлодлар сони берилган маълум миқдордан ошиб кетса, жараён тўхтатилади; «энг яхши хромосомалар» шифрни бузиш учун қўлланилади. Ўрнига қўйишга асосланган шифрлаш учун бу алгоритм яхши натижа берди. Бунда оптимал нуқтага, яъни махфий калитга эришиш учун, алгоритмдан бутун

калитлар фазосининг ўртача 2% кўп бўлмаган қисмини ўрганиш талаб қилинди. Генетик алгоритмлардан ўрнига қўйишга ва ўринлаштиришга асосланган шифрлаш алгоритмларининг криптотаҳлилида муваффақиятли фойдаланилади [25].

***Квант компьютерлари***

Квант компьютерлари ёрдамида бугунги кундаги компьютерларда амалга ошириб бўлмайдиган ҳисоблашларни бажариш мумкин [25]. Квант физикасида зарра ҳолати амплитуда деб номланадиган комплекс қийматларни қабул қилувчи тўлқин функцияси ψ билан характерланади. Тўлқин функциясининг аргументи бўлиб вақт, шунингдек баъзи бир физик параметрлар тўплами (масалан, зарра координаталари) ҳисобланади. Алгоритмлар назариясида чекли объектлар билан амалларни бажариш қабул қилинган. Шунинг учун тўлқин функцияси аргументларини дискрет деб ҳисоблаб, физикада қабул қилинган чексиз ўлчамли моделдан чеклисига ўтилади. Оддийроқ қилиб тушунтириш учун тўлқин функцияси ψ (*x*, *t*) фақат *x* координаталари ва *t* вақтга боғлиқ бўлиб, фиксирланган ҳолат кўрилади. *x 0* ва *1* қийматларни қабул қилади деб фараз қилинади. Бу зарранинг фақат икки хил нуқтада жойлашган ҳолати учун мосдир. Бу ҳолатга бошқа тарафдан қараш мумкин. Фараз қилайлик, [*0; 1*] кесмада жойлашган зарра турган жойи ҳақида маълумотни сақлаш учун фақат бир битга эга бўлинади. *x = 0*, агар у шу кесманинг чап ярмида бўлса ва *x=1*, агар ўнг тарафида бўлса. Икки ёрдамчи функция қараб ўтилади: $|0\rangle$ ва $|1\rangle$. Биринчиси *x = 0* да *1* га ва *x=1* да *0* га тенг, иккинчиси шунинг акси. У ҳолда ихтиёрий тўлқин функцияси ψ (*x*) ни $\lambda_0|0\rangle+\lambda_1|1\rangle$ формула ёрдамида ягона усулда ёзса бўлади. Бу ёзув икки ўлчамли комплекс фазонинг векторини *0* ва *1* базислари бўйича ёйилишига мос келади. Агар базис векторларни ортонормал деб фараз қилинса, у ҳолда тўлқин

функцияси ортонормаллашган базис бўйича ёйилган икки ўлчамли комплекс фазо вектори бўлиб ҳисобланади. Бундай зарра *квант бити* ёки *кубит* деб номланади.

Вақтнинг берилган моментида зарранинг қайси нуқтада жойлашганлигини билишнинг ягона йўли – тўлқин функциясини ўлчашдир. Ўлчаш мос равишда $|\lambda_0|^2$ ва $|\lambda_1|^2$ эҳтимоллик билан $|0\rangle$, $|1\rangle$ векторлардан ихтиёрий бирини беради. Бунда $\lambda_0$ ва $\lambda_1$ - $|\lambda_0|^2+|\lambda_0|^2=1$ (эҳтимоллик йиғиндиси бирга тенг) нормаллаш шарти билан боғлиқ бўлган амплитудалар. *n* та кубитлардан иборат бўлган тизим $2^n$ ўлчамли ҳолатлар фазосига эга. Айнан шу зарра сонига боғлиқ бўлган ҳолатлар фазосининг экспоненциал ўсиши анъанвий компьютерларга нисбатан квант компьютерларида ҳисоблаш тезлигида афзалликка олиб келади. 1994 йилда Питер Шор «чегараланган эҳтимолли» факторлаш алгоритмини [25] кашф этди. Бу алгоритм *N* сонини квант компьютерларида $O((\log N)^3)$ полином вақт давомида $O(\log N)$ жой сарфлаб кўпайтувчиларга ёйиб чиқиш имконини беради. Кўпчилик алгоритмларда, шунингдек Шор алгоритмида ҳам, стандарт усулдан фойдаланиб, ёйиш масаласини функциянинг даврини топиш масаласига келтирилади. Шор квант параллелизмидан бир қадамда функциянинг ҳамма қийматларининг суперпозициясини олиш учун фойдаланади. Кейин у Фурьенинг квантли алмаштиришини амалга оширади. Унинг натижаси Фурьенинг классик алмаштириши каби аргументи даврга тескари бўлган ўлчамга каррали функция бўлади. Ҳолат ўлчами ўз навбатида катта эҳтимоллик билан *N* бутун сонни ёйишга хизмат қилувчи даврни қайтаради. Юқорида келтирилганлар квант алгоритмининг моҳиятини соддалаштирилган кўринишда очиб беради. Муаммо шундан иборатки, Фурьенинг квант алмаштириши тезкор Фурье алмаштиришига асосланган ва шунинг учун ҳам кўп ҳолатларда тахминий натижа беради. Шорнинг сонни кўпайтувчиларга ёйиш алгоритмини квантли ҳисоблаш алгоритмлари соҳасидаги асосий ютуқ деса бўлади. Айнан

шу вақтдан бошлаб квант компьютерларини яратиш ишларига катта молиялаштириш ишлари бошланиб кетди. Шор алгоритмининг самарадорлиги SHARP компаниясидан бўлган япон олимларини шубҳага солди. Гап шундаки, Шорнинг ўзи ҳам, квантли ҳисоблаш алгоритми соҳасида ишловчи бошқа математиклар ҳам, амаллар сони ҳақида сўз юритишади, гарчи амалиётда японлар аниқлаган айнан ҳисоблаш вақти муҳимдир [25]. Фурьенинг дискрет алмаштириши квант компьютерида алоҳида кубитлар устидаги Адамар алмаштириши ва бошқа кубит ҳолатига кўра битта *j* кубитда фазони $\theta = \frac{\pi}{2^{k-j}}$ бурчакка шартли бурилиш амалини навбатма-навбат алмаштириши каби амалга оширилади. Агар кубитлар сони *n* га тенг бўлса, у ҳолда энг кичик бурчак $\frac{\pi}{2^{n-1}}$ га тенг. Бу операцияга $\tau_{\min}$ вақт ажратилган бўлса, у ҳолда қўшни кубитлар учун $\frac{\pi}{2}$ бурчакка буриш амали учун $\tau = \tau_{\min} \cdot 2^n$ тартибдаги вақт кетади. Япон олимлари томонидан қўлга киритилган экспоненциал боғлиқлик Шор алгоритмининг ҳисоблаш вақтидаги ютуғини йўққа чиқаради.

Бироқ ФТИАН ходими Леонид Федичкин 1996 йили чоп этилган фин муаллифларининг ишини кўрсатиб ўтган [25]. Улар ФДА аниқлигига шовқиннинг таъсирини тадқиқ этдилар. [25] да кўрсатилганидек бундай алмаштиришлар $\theta$ бурчакларнинг динамик диапазонини (*n* кубитлар сонига нисбатан) экспоненциал катта бўлишини талаб қилади. Кичик бурчакка бурилиш шовқин орқали беркитилса, нима бўлади? Маълум бўлишича, кубит ҳолатидаги фазовий силжиш операциясидан талаб қилинаётган аниқлик фазонинг кичик бурчакка бурилиш амалини бартараф қилишга рухсат беради. Федичкин ҳисоб-китоби шуни кўрсатадики, бу амални истисно қилиш, Шор алгоритми бажарилиш вақти кубитларнинг *n* миқдорига полиномиал боғлиқлигини сақлаб қолади.

Шор алгоритми фақат квант компьютерларида ишлаганидек, ҳозирги кунда етарлича катта сонни полиномиал вақтда кўпайтувчиларга ёйишга имкон берувчи техник воситалар мавжуд эмас. Шундай экан, энг асосий масала квант компьютерларини яратиш бўлиб қолмоқда. Шор алгоритми жуда оддий бўлиб, универсал квант компьютерига керак бўладигандан кўра, жуда содда аппарат таъминоти билан кифояланади. Шунинг учун эҳтимолки, кўпайтувчиларга ажратувчи квант қурилмаси квант ҳисоблашларининг бутун диапазони технологик жиҳатдан мавжуд бўлгунга қадар қурилади. Бугунги кунда аниқ натижалар мавжуд. IBM компания лабораториясида яратилган Шор алгоритми бўйича сонни факторлаш учун мўлжалланган етти кубитли квант компьютерларини ишлаш жараёнини намойиш этди. Гарчи улар томонидан ечилган масала (15 сонининг бўлувчилари 3 ва 5 сонлари эканлиги тўғри топилган бўлсада) ақлни ҳайрон қолдирмасада, бу квант компьютерлари тарихидаги энг қийин ҳисоблашдир.

## Назорат саволлари

1. Мураккаблик назарияси деганда нимани тушунасиз?
2. Алгоритмнинг мураккаблиги деганда нимани тушунасиз?
3. Вақт билан аниқланадиган мураккаблик ва ҳисоблаш қурилмаси хотираси ҳажми билан боғлиқ бўлган мураккаблик деганда нимани тушунасиз?
4. Алгоритмнинг ҳисоблаш мураккаблиги қандай ифодаланади, унда нималар ҳисобга олинади? Мисоллар келтиринг.
5. Алгоритмлар вақт ва ҳисоблаш мураккабликларига кўра қандай синфларга ажратилади?
6. Доимий, чизиқли, полиномиал алгоритмларнинг бир биридан фарқлари нимада, улар қандай белгиланади?
7. Экспоненциал ва суперполиномиал алгоритмларнинг бир биридан фарқлари нимада, улар қандай белгиланади?

8. Ечиш мумкин бўлган, қийин ечиладиган, ҳисобланиши қийин бўлган ва ечилмайдиган масалаларга таърифлар беринг.

9. Тьюринг машинаси ва Тьюрингнинг эҳтимоллик машинаси тушунчаларининг фарқи қандай?

10. *NP* тўлиқ масала деганда нимани тушунасиз?

11. $P = NP$ деб фараз қилинса, *L* тилни тушунувчи Тьюрингнинг эҳтимоллик машинаси учун қандай мураккабликка эга бўлган алгоритм мавжуд бўлади?

12. АҚШ давлат стандартлари DES, Triple DES, AESнинг криптобардошлилиги қандай белгиланади?

13. Россия Федерацияси давлат стандарти ГОСТ 28147-89 билан DESнинг асосий фарқлари нималарда намоён бўлади?

14. Rijandael алгоритмининг афзалликлари нималардан иборат?

15. ГОСТ Р 34.10-2001, EC-DSA-2000, EC-KCDSA, EC-GDSA ва ДСТУ 4145-2002 алгоритмлари қандай муаммолар мураккаблигига асосланган?

16. Факторлаш ва дискрет логарифмлаш муаммоларининг мураккаблигига асосланган хорижий криптографик алгоритмларнинг бардошлилигининг юқори чегараси кандай белгиланади?

17. ЭЭЧ нуқталари группасида дискрет логарифмлаш муамосини ҳал этиш учун зарур амалларнинг юқори чегараси қандай ифода бўйича топилади?

18. O’z DSt 1092 стандартининг ўзига хос томонлари нималарда намоён бўлади?

19. O’z DSt 1092 стандартининг DSA ва ГОСТ Р 34.10–2001 стандартларига ўхшаш ва ўзига хос фарқли томонлари нималардан иборат?

20. Криптотаҳлилда қандай янги технологиялардан фойдаланилади?

21. Сунъий нейрон тўрлари деб нимага аталади ва уларнинг аҳамияти нималарда намоён бўлади?

22. Генетик алгоритмларнинг криптотаҳлилдаги ўрни қандай?

23. Квант компьютерлари қандай мақсадларда қўлланилади?

# ХУЛОСА

Ҳозирги кунга қадар ахборот хавфсизлигини таъминлашда энг ишончли воситалардан бири *ахборотни криптографик ҳимоя қилиш воситалари* ҳисобланади. Бу ўз навбатида “Криптография ва криптотаҳлил” мутахассисликлари бўйича давлат тилида таълим олаётган талабаларни зарур ўқув қўлланма ва дарсликлар билан таъминлашни тақозо этади.

Тақдим этилаётган “Криптотаҳлил ва унинг махсус усуллари” ўқув қўлланмасида криптотаҳлил асослари, криптографик алгоритмлар бардошлилиги, симметрик ва носимметрик криптотизимлар бардошлилигини таъминловчи тамойиллар ва муаммолар, криптотизимларни криптотаҳлиллашнинг универсал усуллари ва криптотаҳлиллашда янги технологиялардан фойдаланиш бўйича маълумотлар баён этилган.

Шунингдек, ўқув қўлланмада Республикамизда криптология соҳасида эришилган натижаларга ҳам эътибор қаратилган, электрон рақамли имзо бўйича давлат стандартининг хорижий стандартлар билан қиёсий характеристикалари келтирилиб, унинг ўзига хос томонлари кўрсатилган.

Ушбу ўқув қўлланма ахборот хавфсизлиги ва криптография йўналишида таълим олаётган магистрлар учун мўлжалланган бўлиб, ундан ахборот хавфсизлиги йўналишида бакалаврлар тайёрлаш жараёнида ҳамда криптография йўналишида илмий-тадқиқот олиб бораётган аспирант-тадқиқотчилар, илмий ходимлар ва соҳа мутахассислари ҳам фойдаланишлари мумкин.

Мазкур «Криптотаҳлил ва унинг махсус усуллари» ўқув қўлланмасининг чоп этилиши келгусида тегишли ўқув дарсликларининг юзага келиши учун замин яратади.

## ФОЙДАЛАНИЛГАН АДАБИЁТЛАР


1. «Криптографик тизимларни криптотаҳлиллашнинг истиқболли усулларини ишлаб чиқиш ва уларни тадқиқ этиш» мавзуси бўйича бажарилган илмий-тадқиқот ишининг 1-босқич ҳисоботи. – ЎзААА «UNICON.UZ» ДУК Тошкент, 2009.

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

3. Арипов М.М., Пудовченко Ю.Е. Основы криптологии.- Ташкент: 2004. – 136 с.

4. Баричев С.Г., Серов Р.Е. Основы современной криптографии. Учебное пособие. – Москва: Лори Горячая Линия - Телеком, 2002. – 152 с.

5. Алексеев А. Криптография и криптоанализ: вековая проблема человечества. http://www.nvkz.kuzbass.net/hard-soft/soft/other/kripto-analiz.html.

6. «Ошкора калитли криптотизимларни криптотаҳлиллаш учун қурол-воситалар ишлаб чиқиш ва уларни тадқиқ этиш» мавзуси бўйича бажарилган илмий-тадқиқот ишининг 1-8-босқич ҳисоботлари. – ЎзААА ФТМТМ, Тошкент, 2002.

7. Бияшев Р.Г., Горковенко Е.В., Нысаанбаева С.Е. Алгоритмы шифрования сообщений и формирования электронной цифровой подписи с заданной криптостойкостью информации // Институт проблем информатики и управления МОН РК, г. Алма-Ата.

8. Хасанов П.Ф., Исаев Р.И., Назарова М.Х., Хасанов Х.П., Ахмедова О.П. Ахборотнинг криптографик муҳофазаси тарихи (Компьютер криптографияси даври) // Aloqa dunyosi. – Тошкент, 2006, №1 (6). – 59-74 бетлар.

9. Хасанов Х.П. Такомиллашган диаматрицалар алгебралари ва параметрли алгебра асосида криптотизимлар яратиш усуллари ва алгоритмлари. – Тошкент, 2008. 208 б.

10. Каримов И.А. Жаҳон молиявий иқтисодий инқирози. Ўзбекистон шароитида уни бартараф этишнинг йўллари ва чоралари. – Т.: Ўзбекистон, 2009. – 56 б.

11. O‘z DSt 1109:2006 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Атамалар ва таърифлар».

12. Защита информации. Малый тематический выпуск ТИИЭР. – Москва, 1988. – т.76, №5.

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

14. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: издательство ТРИУМФ, 2003 - 816 с.

15. Венбо Мао. Современная криптография. Теория и практика. – Москва - Санкт-Петербург - Киев: Лори Вильямс, 2005.

16. Нильс Фергюсон, Брюс Шнайер. Практическая криптография – Москва: "Диалектика", 2004.

17. ElGamal T. On computing logarithm over finite fields // Advances in cryptology—CRYPTO’85 (Santa Barbara, Calif., 1985). (Lect. Notes in Comput. Sci.; V. 218). – Pp. 396-402.

18. ElGamal T., A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Transactions on Information Theory, 1985, vol. IT-31. – Pp. 469-472.

19. Столлингс В. Криптография и защита сетей. Принципы и практика. Изд.:Лори Вильямс, 2001.

20. Молдовян А.А., Молдовян Н.А. Введение в криптосистемы с открытым ключом. Санкт – Петербург «БХВ-Петербург» 2005.

21. O‘z DSt 1106:2009 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Хэшлаш функцияси».

22. ГОСТ Р 34.11-94. Государственный Стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования.

23. Акбаров Д.Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланишлари. Тошкент. ”Ўзбекистон маркаси “, 2009. – 432 б.

24. Шеннон К. Теория и связи в секретных системах. Работы по теории информации и кибернетике. – М.: Иностранная лит. 1963. – 243 б.

25. Авдошин С.М., Савельева А.А. «Криптоанализ: вчера, сегодня, завтра», Государственный университет – Высшая Школа Экономики. Москва – 2007.

26. Авдошин С.М., Савельева А.А. «Криптоанализ: савременное состояние и перспективы развития», Государственный университет – Высшая Школа Экономики.

27. Жуков А.Е. «Криптоанализ по побочным каналам (Side Channel Attacks)», Пособие по курсу «Криптографические методы защиты информации» Москва – 2004.

28. Савельева А.А. «Исследование эффективности алгоритмов дискретного логарифмирования, ипользующих факторную базу», Государственный университет – Высшая Школа Экономики Москва – 2007.

29. Joux, Antoine. Algorithmic cryptanalysis / Antoine Joux. p. cm. -- (Chapman & Hall/CRC cryptography and network security) Includes bibliographical references and index, 2009.

30. 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.

31. Лунин А.В., Сальников А.А. Перспективы развития и использования асимметричных алгоритмов в криптографии. http: //www.ssl.stu.neva.ru.

32. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. – М., МЦНМО, 2003. – 328 с.

33. Кузнецов М.И., Бурланков Д.Е., Чирков А.Ю., Яковлев В.А. Компьютерная алгебра: Учебник. // Нижегородский Государственный Университет им. Н.И. Лобачевского, 2002. опубликовано: http://www.itlab.unn.ru/archive/docs/coaBook.pdf.

34. Hankerson D., Menezes A., Vanstone S. Guide to Elliptic Curve Cryptography. Springer-Verlag New York, Inc. 2004.

35. Соловьев Ю.П. Рациональные точки на эллиптических кривых //Соросовский образовательный журнал, №10, 1997.

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

37. Алгоритмические основы эллиптической криптографии / Болотов А.А., Гашков С.Б., Фролов А.В., Часовских А.А. – Москва МЭИ, 2000.

38. Элементарное введение в эллиптическую криптографию: алгебраические и алгоритмические основы / Болотов А.А., Гашков С.Б., Фролов А.В., Часовских А.А. – Москва МЭИ, 2006.

39. Коблиц Н. Введение в эллиптические кривые и модулярные формы // Пер с англ. – Москва: Мир, 1988.

40. Коблиц Н. Курс теории чисел и криптографии. – М. Научное изд-во ТВП, 2001г. – 261 с.

41. Кобец А.М. Подмена подписанного документа в новом американском стандарте ЭЦП ECDSA// http: www.bugtrag/ru.

42. ANSI X9.62-1998: Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).

43. ISO/IEC 14888-3:2006. Information technology – Security techniques – Digital signatures with appendix.

44. Горбенко И.Д., Збитнев С.И., Поляков А.А. Криптоанализ криптографических преобразований в группах точек эллиптических кривых

усулом Полларда // Харьковский государственный технический университет радиотехники.

45. Горбенко И.Д., Збитнев С.И., Поляков А.А. Криптографические преобразования в группах точек эллиптических кривых методом Полларда // Радиотехника: Всеукр. межвед. научно-техн. сб. 2001. Вып. 119.

46. Стандарт ЦП Украины на эллиптической кривой. Опубликовано: domarev , On: Nov-19-2004 http://www.security.ukrnet.net.

47. Хасанов П.Ф., Хасанов Х.П. Стойкость Государственного стандарта ЭЦП Республики Узбекистан //«Сервисы удостоверяющих центров. Новые области применения PKI»: Тез. докл. международной научно – практической конференции PKI Forum- 2006, Санкт-Петербург, 7-10 ноября 2006.

48. «Ахборотни криптографик муҳофазалаш тизими бардошлилигини баҳолашнинг замонавий усулларини тадқиқ этиш. Криптографик модулларга оид хавфсизлик талабларини ишлаб чиқиш» мавзуси бўйича бажарилган илмий-тадқиқот ишининг 1-6-босқич ҳисоботлари. – Тошкент, ЎзААА, ФТМТМ, 2005-2006.

49. Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.Г. «Математические и компьютерные основы криптологии» ООО «Новое знание» 2003 г. – 381 с.

50. Молдовян Н.А., Молдовян А.А., Еремеев М.А. Криптография: от примитивов к синтезу алгоритмов. –СПб.: БХВ-Петербург, 2004. - 448 с.

51. O‘z DSt 1105:2006 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Маълумотларни шифрлаш алгоритми».

52. ГОСТ 28147-89. Государственный Стандарт Союза ССР. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

53. Federal Information Processing Standards Publication 197. Advanced Encryption Standard (AES). 2001.

54. Ахмедова О.П. Электрон рақамли имзо учун мавжуд очиқ калитли криптотизимларнинг қиёсий таҳлили. - InfoCOM.UZ, №7, 2005.

55. Хасанов Х.П. Криптографические системы на основе односторонних функций диапреобразования. «Сервисы удостоверяющих центров. Новые области применения PKI»: Тез. докл. международной научно – практической конференции PKI Forum - 2008, Санкт-Петербург, 15-17 октября 2008.

56. Хасанов П.Ф., Хасанов Х.П., Хасанов Ш.П., Хасанов С.П., Хасанов З.П., Ахмедова О.П. Рақамли имзони шакллантириш ва аутентификациялаш усули // Ўзбекистон Давлат патент идораси томонидан берилган IAP 03070-сон патенти.

57. Хасанов П.Ф., Исаев Р.И., Хасанов Х.П. Ахмедова О.П. О государственном стандарте Узбекистана «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Aloqa dunyosi. – Т.: №1 (6), 2006.

58. Еремеев М.А., Молдовян А.А., Романченко А.М.. «Исследование влияния размерности нелинейного преобразования блочных шифров на устойчивость к классическим методам криптоанализа. Вопросы защиты информации, 1(68)/2005.

59. Молдовян А.А., Молдовян Н.А., Гуц Н.Д., Криптография. Скоростные шифры. – Изд.:Лори БХВ - Петербург, 2002.

60. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

61. ДСТУ 4145-2002. Информационные технологии. Криптографическая защита информации. Цифровая подпись, основанная на эллиптических кривых. Формирование и проверка // Научно-практический семинар. – Киев, 2003. – bezpeka.org/ru/activ.html.

62. Немецкие ученые успешно решили проблему дискретного логарифмирования по модулю 530-битного простого числа p // http://www.securitylab.ru.

63. O‘z DSt 1092:2009 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Электрон рақамли имзони шакллантириш ва текшириш жараёнлари».

64. Al-Ubaidy M.K.I. Black-box attack using neuro-identifier // Cryptologia, Oct 2004.

65. Haranadh Gavara, Harendra Kumar Mishra, Surendra Kumar Y. Cryptanalysis using Neural Networks // Available vianetlab.cs.iitm.ernet.in/cs650/2006/TermPapers/Group9.pdf.

66. Merkle R.C., Hellman M.E. Hiding Information and Signatures in Trapdoor Knapsacks // IEEE transactions on Information Theory. V. 24, n. 5, Sep 1978. P. 525-530.

67. Spillman R., Janssen M., Nelson B., Kepner M. Use of a Genetic Algorithm in the Cryptanalysis of Simple Substitution Ciphers // Cryptologia. 17(1), 1993. P. 31-44.

# ИЛОВАЛАР

1-илова

## Факторлаш дастурининг коди

```
#include <stdio.h>
#include <stdlib.h>
#include <time.h>
#include "miracl.h"
#include <windows.h>
#include "omp.h"
#include <string.h>
#include <math.h>
#define LIMIT 15000
#define BTRIES 1000
#define MULT 2310
#define NEXT 13
#define mr_min(a,b) ((a) < (b)?
(a) : (b))
static big *fu,BOOL
*cp,*plus,*minus;
big n;FILE *output;
static BOOL
suppress=FALSE,chiqish =FALSE;
static int PADDING;
static miracl *mip;
void brute(big *n)
{
  big x,y;
  int m,p;
  gprime(LIMIT);
  x=mirvar(0);
  y=mirvar(0);
  m=0;
  p=mip->PRIMES[0];
  forever
  {
    if (subdiv(*n,p,y)==0)
    {
      copy(y,*n);
      printf("Tub faktor
");
      fprintf(output,"%d\n",p);
      if (size(*n)==1) {chiqish
= TRUE; return;}
        continue;
     }
      if (size(y)<=p)
      {
        printf("Tub faktor
");
        cotnum(*n,output);
        chiqish = TRUE;
        return;
      }
      p=mip->PRIMES[++m];
      if (p==0) break;
    }
    if (isprime(*n))
    {
      printf("Tub faktor
");
      cotnum(*n,output);
      chiqish = TRUE;
      return;
    }
    mr_free(x);
    mr_free(y);
    gprime(0);
}
void brent(big *n)
{
  long k,r,i,m,iter;
  big x,y,ys,z,q,c3,t;
  x=mirvar(0);
  y=mirvar(0);
  ys=mirvar(0);
  z=mirvar(0);
  q=mirvar(0);
  c3=mirvar(3);
  t=mirvar(0);
  m=10;
  r=1;
  iter=0;
  do
  {
    convert(1,q);
    do
    {
      copy(y,x);
      for (i=1;i<=r;i++)
      mad(y,y,c3,*n,*n,y);
      k=0;
      do
      {
        iter++;
        if (iter>BTRIES)
        {

printf("\b\b\b\b\b\b\b\b\b\b\b\
b\b\b\b\b");
          fflush(stdout);
          mr_free(t);
          mr_free(x);
          mr_free(y);
          mr_free(ys);
          mr_free(z);
          mr_free(q);
          mr_free(c3);
```

```
          return;
        }
        if (iter%10==0)
        {
          fflush(stdout);
        }
        copy(y,ys);
        for (i=1;i<=mr_min(m,r-
k);i++)
        {
          mad(y,y,c3,*n,*n,y);
          subtract(y,x,z);
          mad(z,q,q,*n,*n,q);
        }
        egcd(q,*n,z);
        k+=m;
      } while (k<r &&
size(z)==1);
      r*=2;
    } while (size(z)==1);
        if (compare(z,*n)==0)
do
        {

mad(ys,ys,c3,*n,*n,ys);
          subtract(ys,x,z);
        } while
(egcd(z,*n,z)==1);

printf("\b\b\b\b\b\b\b\b\b\b\b\b\
b\b\b\b\b");
      fflush(stdout);
      forever
      {
        if (isprime(z))
        {
          printf("Tub faktor
");
          cotnum(z,output);
        }
        else
        {
          if (compare(z,*n)==0)
return;
          printf("Murakkab
(tubmas) faktor ");
          else printf("&");
          cotnum(z,output);
        }
        divide(*n,z,*n);
        divide(y,*n,*n);
       copy(*n,t);
        divide(t,z,z);
        if (size(t)==0)
continue;
        break;
      }
      if (size(*n)==1) {chiqish
= TRUE;return;}
    } while (!isprime(*n));
    printf("Tub faktor     ");
    cotnum(*n,output);
    chiqish = TRUE;
    return;
  }
void marks(long start)
{
  int i,pr,j,k;
  for (j=1;j<=MULT/2;j+=2)
plus[j]=minus[j]=TRUE;
  for (i=0;;i++)
  {
    pr=mip->PRIMES[i];
    if (pr<NEXT) continue;
    if ((long)pr*pr>start)
break;
    k=pr-start%pr;
    for (j=k;j<=MULT/2;j+=pr)
      plus[j]=FALSE;
    k=start%pr;
    for (j=k;j<=MULT/2;j+=pr)
      minus[j]=FALSE;
  }
}
void pollard(int lim1,long
lim2, big *n)
{
  long i,p,pa,interval;
  int phase,m,pos,btch,iv;
  big t,b,bw,bvw,bd,bp,q;
  t=mirvar(0);
  b=mirvar(0);
  q=mirvar(0);
  bw=mirvar(0);
  bvw=mirvar(0);
  bd=mirvar(0);
  bp=mirvar(0);
  gprime(lim1);
  for (m=1;m<=MULT/2;m+=2)
    if (igcd(MULT,m)==1)
    {
      fu[m]=mirvar(0);
      cp[m]=TRUE;
    }
  else cp[m]=FALSE;
  phase=1;
  p=0;
  btch=50;
  i=0;
  convert(3,b);
  forever
  {
    if (phase==1)
    {
       p=mip->PRIMES[i];
       if (mip->PRIMES[i+1]==0)
       {
         phase=2;
```

```
printf("\b\b\b\b\b\b\b\b\b\b\b\
b\b\b\b");
       }
       power(b,8,*n,bw);
       convert(1,t);
       copy(b,bp);
       copy(b,fu[1]);
       for (m=3;m<=MULT/2;m+=2)
       {
         mad(t,bw,bw,*n,*n,t);
         mad(bp,t,t,*n,*n,bp);
         if (cp[m])
copy(bp,fu[m]);
       }
       power(b,MULT,*n,t);
       power(t,MULT,*n,t);
       mad(t,t,t,*n,*n,bd);
       iv=p/MULT;
       if (p%MULT>MULT/2) iv++;
       interval=(long)iv*MULT;
       p=interval+1;
       marks(interval);
       power(t,2*iv-1,*n,bw);
       power(t,iv,*n,bvw);
       power(bvw,iv,*n,bvw);

subtract(bvw,fu[p%MULT],q);
       btch*=100;
       i++;
       continue;
     }
     pa=p;
     while ((lim1/p) > pa)
pa*=p;
     power(b,(int)pa,*n,b);
     decr(b,1,q);
   }
   else
   {
     p+=2;
     pos=p%MULT;
     if (pos>MULT/2)
     {
       iv++;
       interval=(long)iv*MULT;
       p=interval+1;
       marks(interval);
       pos=1;
       mad(bw,bd,bd,*n,*n,bw);

mad(bvw,bw,bw,*n,*n,bvw);
     }
     if (!cp[pos]) continue;
     if (!plus[pos] &&
!minus[pos]) continue;
     subtract(bvw,fu[pos],t);
     mad(q,t,t,*n,*n,q);
   }
   if (i++%btch==0)
   {

printf("\b\b\b\b\b\b\b\b%8ld",p
);
     fflush(stdout);
     egcd(q,*n,t);
     if (size(t)==1)
     {
       if (p>lim2)
       {

printf("\b\b\b\b\b\b\b\b\b\b\b\
b\b\b\b");
         fflush(stdout);
         break;
       }
       else continue;
     }
     if (compare(t,*n)==0)
       break;

printf("\b\b\b\b\b\b\b\b\b\b\b\
b\b\b\b");
     if (isprime(t))
printf("Tub faktor     ");
     else printf("Murakkab
(tubmas) faktor");
     cotnum(t,output);
     divide(*n,t,*n);
     if (isprime(*n))
     {
       printf("Tub faktor
");
       cotnum(*n,output);
       chiqish = TRUE;
       return;
     }
     break;
   }
 }
 gprime(0);
 mr_free(t);
 mr_free(b);
 mr_free(q);
 mr_free(bw);
 mr_free(bvw);
 mr_free(bd);
 mr_free(bp);
 for (m=1;m<=MULT/2;m+=2)
   if (igcd(MULT,m)==1)
mr_free(fu[m]);
}
void williams(int lim1,long
lim2,int ntrys, big *n)
{
 int k,phase,m,nt,iv,pos,btch;
 long i,p,pa,interval;
 big b,q,fp,fvw,fd,fn,t;
```

```
  b=mirvar(0);
  q=mirvar(0);
  t=mirvar(0);
  fp=mirvar(0);
  fvw=mirvar(0);
  fd=mirvar(0);
  fn=mirvar(0);
  gprime(lim1);
  for (m=1;m<=MULT/2;m+=2)
    if (igcd(MULT,m)==1)
    {
      fu[m]=mirvar(0);
      cp[m]=TRUE;
    }
    else cp[m]=FALSE;
    for (nt=0,k=3;k<10;k++)
    {
      convert(k,b);
      convert((k*k-4),t);
      if (egcd(t,*n,t)!=1)
continue;
      nt++;
      phase=1;
      p=0;
      btch=50;
      i=0;
      forever
      {
        if (phase==1)
        {
          p=mip->PRIMES[i];
          if (mip-
>PRIMES[i+1]==0)
          {
            phase=2;
            copy(b,fu[1]);
            copy(b,fp);

mad(b,b,b,*n,*n,fd);
            decr(fd,2,fd);
            negify(b,t);

mad(fd,b,t,*n,*n,fn);
            for
(m=5;m<=MULT/2;m+=2)
            {
              negify(fp,t);

mad(fn,fd,t,*n,*n,t);
              copy(fn,fp);
              copy(t,fn);
              if (!cp[m])
continue;
              copy(t,fu[m]);
            }
            convert(MULT,t);

lucas(b,t,*n,fp,fd);
            iv=p/MULT;
            if (p%MULT>MULT/2)
iv++;

interval=(long)iv*MULT;
            p=interval+1;
            marks(interval);
            convert(iv,t);

lucas(fd,t,*n,fp,fvw);
            negify(fp,fp);

subtract(fvw,fu[p%MULT],q);
            btch*=100;
            i++;
            continue;
          }
          pa=p;
          while ((lim1/p) > pa)
pa*=p;
          convert((int)pa,t);
          lucas(b,t,*n,fp,q);
          copy(q,b);
          decr(q,2,q);
        }
        else
        {
          p+=2;
          pos=p%MULT;
          if (pos>MULT/2)
          {
            iv++;

interval=(long)iv*MULT;
            p=interval+1;
            marks(interval);
            pos=1;
            copy(fvw,t);

mad(fvw,fd,fp,*n,*n,fvw);
            negify(t,fp);
          }
          if (!cp[pos])
continue;
          if (!plus[pos] &&
!minus[pos]) continue;

subtract(fvw,fu[pos],t);
          mad(q,t,t,*n,*n,q);
        }
        if (i++%btch==0)
        {
          egcd(q,*n,t);
          if (size(t)==1)
          {
            if (p>lim2)
              break;
            else continue;
          }
          if (compare(t,*n)==0)
```

```
          break;

printf("\b\b\b\b\b\b\b\b\b\b\b\b\
b\b\b\b");
          if (isprime(t))
printf("Tub faktor     ");
          else
printf("Murakkab (tubmas)
faktor ");
          cotnum(t,output);
          divide(*n,t,*n);
          if (isprime(*n))
          {
            printf("Tub faktor
");
            cotnum(*n,output);
            chiqish = TRUE;
            return;
          }
          nt=ntrys;
          break;
        }
      }
      if (nt>=ntrys) break;
  }
  gprime(0);
  mr_free(b);
  mr_free(q);
  mr_free(t);
  mr_free(fp);
  mr_free(fvw);
  mr_free(fd);
  mr_free(fn);
  for (m=1;m<=MULT/2;m+=2)
    if (igcd(MULT,m)==1)
mr_free(fu[m]);
}
static big ak,t,ww,s1,d1,s2,d2;
void duplication(big sum,big
diff,big x,big z)
{
  nres_modmult(sum,sum,t);
  nres_modmult(diff,diff,z);
  nres_modmult(t,z,x);
  nres_modsub(t,z,t);
  nres_modmult(ak,t,ww);
  nres_modadd(z,ww,z);
  nres_modmult(z,t,z);
}
void addition(big xd,big zd,big
sm1,big df1,big sm2,big df2,big
x,big z)
{
  nres_modmult(df1,sm2,z);
  nres_modadd(z,x,t);
  nres_modsub(z,x,z);
  nres_modmult(t,t,x);
  nres_modmult(x,zd,x);
  nres_modmult(z,z,z);
  nres_modmult(z,xd,z);
}
void ellipse(big x,big z,int
r,big x1,big z1,big x2,big z2)
{
  int k,rr;
  k=1;
  rr=r;
  copy(x,x1);
  copy(z,z1);
  nres_modadd(x1,z1,s1);
  nres_modsub(x1,z1,d1);
  duplication(s1,d1,x2,z2);
  while ((rr/=2)>1) k*=2;
  while (k>0)
  {
    nres_modadd(x1,z1,s1);
    nres_modsub(x1,z1,d1);
    nres_modadd(x2,z2,s2);
    nres_modsub(x2,z2,d2);
    if ((r&k)==0)
    {

addition(x,z,s1,d1,s2,d2,x2,z2)
;
      duplication(s1,d1,x1,z1);
    }
    else
    {

addition(x,z,s1,d1,s2,d2,x1,z1)
;
      duplication(s2,d2,x2,z2);
    }
    k/=2;
  }
}
int kurve=5;
void lenstra(int lim1,long
lim2,int ncurves, big *n)
{
  int
phase,m,nc,iv,pos,btch,u,v;
  long i,p,pa,interval;
  big
q,x,z,a,x1,z1,x2,z2,xt,zt,fvw;
  q=mirvar(0);
  x=mirvar(0);
  z=mirvar(0);
  a=mirvar(0);
  x1=mirvar(0);
  z1=mirvar(0);
  x2=mirvar(0);
  z2=mirvar(0);
  s1=mirvar(0);
  d1=mirvar(0);
  s2=mirvar(0);
  d2=mirvar(0);
  ak=mirvar(0);
```

```
  xt=mirvar(0);
  zt=mirvar(0);
  fvw=mirvar(0);
  t=mirvar(0);
  ww=mirvar(0);
  gprime(lim1);
  for (m=1;m<=MULT/2;m+=2)
    if (igcd(MULT,m)==1)
    {
      fu[m]=mirvar(0);
      cp[m]=TRUE;
    }
    else cp[m]=FALSE;
  prepare_monty(*n);
  for (nc=1;;)
  {
    kurve++;
    u=kurve*kurve-5;
    v=4*kurve;
    convert(u,x);  nres(x,x);
    convert(v,z);  nres(z,z);
    nres_modsub(z,x,a);
    copy(x,t);
    nres_modmult(x,x,x);
    nres_modmult(x,t,x);
    copy(z,t);
    nres_modmult(z,z,z);
    nres_modmult(z,t,z);
    copy(a,t);
    nres_modmult(t,t,t);
    nres_modmult(t,a,t);
    convert(3*u,a); nres(a,a);
    convert(v,ak);
nres(ak,ak);
    nres_modadd(a,ak,a);
    nres_modmult(t,a,t);  /*
t=(v-u)^3.(3u+v) */
    convert(u,a);  nres(a,a);
    copy(a,ak);
    nres_modmult(a,a,a);
    nres_modmult(a,ak,a);   /*
a=u^3 */
    convert(v,ak); nres(ak,ak);
    nres_modmult(a,ak,a);   /*
a=u^3.v */
    nres_premult(a,16,a);
    nres_moddiv(t,a,ak);     /*
ak=(v-u)^3.(3u+v)/16u^3v */
    phase=1;
    p=0;
    i=0;
    btch=50;
    nc++;
    forever
    {
      if (phase==1)
      {
        p=mip->PRIMES[i];
        if (mip-
>PRIMES[i+1]==0)
        {
          phase=2;
          copy(x,xt);
          copy(z,zt);
          nres_modadd(x,z,s2);
          nres_modsub(x,z,d2);

duplication(s2,d2,x,z);
          nres_modadd(x,z,s1);
          nres_modsub(x,z,d1);

nres_moddiv(x1,z1,fu[1]);

addition(x1,z1,s1,d1,s2,d2,x2,z
2);
          for
(m=5;m<=MULT/2;m+=2)
          {

nres_modadd(x2,z2,s2);

nres_modsub(x2,z2,d2);

addition(x1,z1,s2,d2,s1,d1,x,z)
;
            copy(x2,x1);
            copy(z2,z1);
            copy(x,x2);
            copy(z,z2);
            if (!cp[m])
continue;
            copy(z2,fu[m]);

nres_moddiv(x2,fu[m],fu[m]);
          }

ellipse(xt,zt,MULT,x,z,x2,z2);
          nres_modadd(x,z,xt);
          nres_modsub(x,z,zt);
          iv=(int)(p/MULT);
          if (p%MULT>MULT/2)
iv++;

interval=(long)iv*MULT;
          p=interval+1;
          marks(interval);

ellipse(x,z,iv,x1,z1,x2,z2);

nres_moddiv(x1,z1,fvw);

nres_modsub(fvw,fu[p%MULT],q);
          btch*=100;
          i++;
          continue;
        }
        pa=p;
```

```
        while ((lim1/p) > pa)
pa*=p;

ellipse(x,z,(int)pa,x1,z1,x2,z2
);
        copy(x1,x);
        copy(z1,z);
        copy(z,q);
      }
      else
      {
        p+=2;
        pos=(int)(p%MULT);
        if (pos>MULT/2)
        {
          iv++;

interval=(long)iv*MULT;
          p=interval+1;
          marks(interval);
          pos=1;

nres_moddiv(x2,z2,fvw);

nres_modadd(x2,z2,s2);

nres_modsub(x2,z2,d2);

addition(x1,z1,s2,d2,xt,zt,x,z)
;
          copy(x2,x1);
          copy(z2,z1);
          copy(x,x2);
          copy(z,z2);
        }
        if (!cp[pos]) continue;
        if (!plus[pos] &&
!minus[pos]) continue;

nres_modsub(fvw,fu[pos],t);
        nres_modmult(q,t,q);
      }
      if (i++%btch==0)
      {
        egcd(q,*n,t);
        if (size(t)==1)
        {
          if (p>lim2)
            break;
          else continue;
        }
        if (compare(t,*n)==0)
          break;

printf("\b\b\b\b\b\b\b\b\b\b\b\b\
b\b\b\b");
        if (isprime(t))
printf("Tub faktor     ");
        else  printf("Murakkab
(tubmas) faktor");
        cotnum(t,output);
        divide(*n,t,*n);
        if (isprime(*n))
        {
          printf("Tub faktor
");
          cotnum(*n,output);
          chiqish = TRUE;
          return;
        }
        nc=ncurves+1;
        break;
      }
    }
    if (nc>ncurves) break;
  }
  gprime(0);
  mr_free(ww);
  mr_free(t);
  mr_free(q);
  mr_free(x);
  mr_free(z);
  mr_free(a);
  mr_free(x1);
  mr_free(z1);
  mr_free(x2);
  mr_free(z2);
  mr_free(s1);
  mr_free(d1);
  mr_free(s2);
  mr_free(d2);
  mr_free(ak);
  mr_free(xt);
  mr_free(zt);
  mr_free(fvw);
  for (m=1;m<=MULT/2;m+=2)
    if (igcd(MULT,m)==1)
mr_free(fu[m]);
}
#define SSIZE 100000
static big
NN,TT,DD,RR,VV,PP,XX,YY,DG,IG,A
A,BB;
static big *x,*y,*z,*w;
static unsigned int **EE,**G;
static int
*epr,*r1,*r2,*rp,*b,*pr,*e,*has
h;
static unsigned char
*logp,*sieve;
static int
mm,mlf,jj,nbts,nlp,lp,hmod,hmod
2;
static BOOL partial;
static miracl *mip;
int knuth(int mm,int *epr,big
N,big D)
```

```
{
  double dp,fks,top;
  BOOL found;
  int i,j,bk,nk,kk,r,p;
  static int
K[]={0,1,2,3,5,6,7,10,11,13,14,
15,17,0};
  top=(-10.0e0);
  found=FALSE;
  nk=0;
  bk=0;
  epr[0]=1;
  epr[1]=2;
  do
  {
    kk=K[++nk];
    if (kk==0)
    {
      kk=K[bk];
      found=TRUE;
    }
    premult(N,kk,D);
    fks=log(2.0e0)/(2.0e0);
    r=remain(D,8);
    if (r==1) fks*=(4.0e0);
    if (r==5) fks*=(2.0e0);
    fks-
=log((double)kk)/(2.0e0);
    i=0;
    j=1;
    while (j<mm)
    {
      p=mip->PRIMES[++i];
      r=remain(D,p);
      if (spmd(r,(p-1)/2,p)<=1)
      {
        epr[++j]=p;
        dp=(double)p;
        if (kk%p==0)
fks+=log(dp)/dp;
        else
fks+=2*log(dp)/(dp-1.0e0);
      }
    }
    if (fks>top)
    {
      top=fks;
      bk=nk;
    }
  } while (!found);
  return kk;
}
BOOL factored(long lptr,big T)
{
  BOOL facted;
  int i,j,r,st;
  partial=FALSE;
  facted=FALSE;
  for (j=1;j<=mm;j++)
  {
    r=(int)(lptr%epr[j]);
    if (r<0) r+=epr[j];
    if (r!=r1[j] && r!=r2[j])
continue;
    while
(subdiv(T,epr[j],XX)==0)
    {
      e[j]++;
      copy(XX,T);
    }
    st=size(T);
    if (st==1)
    {
      facted=TRUE;
      break;
    }
    if (size(XX)<=epr[j])
    {
      if (st>=MR_TOOBIG ||
(st/epr[mm])>(1+mlf/50)) break;
      if (st<=epr[mm])
      for (i=j;i<=mm;i++)
      if (st==epr[i])
      {
        e[i]++;
        facted=TRUE;
        break;
      }
      if (facted) break;
      lp=st;
      partial=TRUE;
      facted=TRUE;
      break;
    }
  }
  return facted;
}
BOOL gotcha(void)
{
  int r,j,i,k,n,rb,had,hp;
  unsigned int t;
  BOOL found;
  found=TRUE;
  if (partial)
  {
    had=lp%hmod;
    forever
    {
      hp=hash[had];
      if (hp<0)
      {
        found=FALSE;
        break;
      }
      if (pr[hp]==lp) break;
      had=(had+(hmod2-
lp%hmod2))%hmod;
    }
```

```
    if (!found && nlp>=mlf)
return FALSE;
  }
  copy(PP,XX);
  convert(1,YY);
  for (k=1;k<=mm;k++)
  {
    if (e[k]<2) continue;
    r=e[k]/2;
    e[k]%=2;
    expint(epr[k],r,TT);
    multiply(TT,YY,YY);
  }
  if (partial)
  {
    if (!found)
    {
      hash[had]=nlp;
      pr[nlp]=lp;
      copy(XX,z[nlp]);
      copy(YY,w[nlp]);
      for
(n=0,rb=0,j=0;j<=mm;j++)
      {

G[nlp][n]|=((e[j]&1)<<rb);
        if (++rb==nbts)
n++,rb=0;
      }
      nlp++;
    }
    if (found)
    {

mad(XX,z[hp],XX,NN,NN,XX);

mad(YY,w[hp],YY,NN,NN,YY);
      for
(n=0,rb=0,j=0;j<=mm;j++)
      {
        t=(G[hp][n]>>rb);
        e[j]+=(t&1);
        if (e[j]==2)
        {

premult(YY,epr[j],YY);
          divide(YY,NN,NN);
          e[j]=0;
        }
        if (++rb==nbts)
n++,rb=0;
      }
      premult(YY,lp,YY);
      divide(YY,NN,NN);
    }
  }
  else
  {
    printf("\b\b\b\b\b\b ");
    fflush(stdout);
  }
  if (found)
  {
    for (k=mm;k>=0;k--)
    {
      if (e[k]%2==0) continue;
      if (b[k]<0)
      {
        found=FALSE;
        break;
      }
      i=b[k];
      mad(XX,x[i],XX,NN,NN,XX);
      mad(YY,y[i],YY,NN,NN,YY);
      for
(n=0,rb=0,j=0;j<=mm;j++)
      {
        t=(EE[i][n]>>rb);
        e[j]+=(t&1);
        if (++rb==nbts)
n++,rb=0;
      }
    }
    for (j=0;j<=mm;j++)
    {
      if (e[j]<2) continue;
      convert(epr[j],TT);
      power(TT,e[j]/2,NN,TT);
      mad(YY,TT,YY,NN,NN,YY);
    }
    if (!found)
    {
      b[k]=jj;
      copy(XX,x[jj]);
      copy(YY,y[jj]);
      for
(n=0,rb=0,j=0;j<=mm;j++)
      {

EE[jj][n]|=((e[j]&1)<<rb);
        if (++rb==nbts)
n++,rb=0;
      }
      jj++;
      printf("%5d",jj);
    }
  }
  if (found)
  {
    add(XX,YY,TT);
    if (compare(XX,YY)==0 ||
compare(TT,NN)==0) found=FALSE;
    if (!found)
printf("%5d",jj);
  }
  return found;
}
int initv(int d, big *n)
```

```
{
  int i,j,pak,k,maxp;
  double dp;
  NN=mirvar(0);
  TT=mirvar(0);
  DD=mirvar(0);
  RR=mirvar(0);
  VV=mirvar(0);
  PP=mirvar(0);
  XX=mirvar(0);
  YY=mirvar(0);
  DG=mirvar(0);
  IG=mirvar(0);
  AA=mirvar(0);
  BB=mirvar(0);
  nbts=8*sizeof(int);
  copy(*n,NN);
  if (d<8) mm=d;
  else mm=25;
  if (d>20) mm=(d*d*d*d)/4096;

dp=(double)2*(double)(mm+100);

maxp=(int)(dp*(log(dp*log(dp)))
);
  gprime(maxp);
  epr=(int
*)mr_alloc(mm+1,sizeof(int));
  k=knuth(mm,epr,NN,DD);
  if (nroot(DD,2,RR))
  {
    if (isprime(RR))
printf("Tub faktor     ");
    else   printf("Murakkab
(tubmas) faktor ");
    else if (!isprime(RR))
printf("&");
    cotnum(RR,output);
    divide(NN,RR,NN);
    if (isprime(NN))
printf("Tub faktor     ");
    else   printf("Murakkab
(tubmas) faktor ");
    cotnum(NN,output);
    return (-1);
  }
  gprime(0);
  mlf=2*mm;
  r1=(int
*)mr_alloc((mm+1),sizeof(int));
  r2=(int
*)mr_alloc((mm+1),sizeof(int));
  rp=(int
*)mr_alloc((mm+1),sizeof(int));
  b=(int
*)mr_alloc((mm+1),sizeof(int));
  e=(int
*)mr_alloc((mm+1),sizeof(int));
  logp=(unsigned char
*)mr_alloc(mm+1,1);
  pr=(int
*)mr_alloc((mlf+1),sizeof(int))
;
  hash=(int
*)mr_alloc((2*mlf+1),sizeof(int
));
  sieve=(unsigned char
*)mr_alloc(SSIZE+1,1);
  x=(big
*)mr_alloc(mm+1,sizeof(big *));
  y=(big
*)mr_alloc(mm+1,sizeof(big *));
  z=(big
*)mr_alloc(mlf+1,sizeof(big
*));
  w=(big
*)mr_alloc(mlf+1,sizeof(big
*));
  for (i=0;i<=mm;i++)
  {
    x[i]=mirvar(0);
    y[i]=mirvar(0);
  }
  for (i=0;i<=mlf;i++)
  {
    z[i]=mirvar(0);
    w[i]=mirvar(0);
  }
  EE=mr_alloc(mm+1,sizeof(int
*));
  G=mr_alloc(mlf+1,sizeof(int
*));
  pak=1+mm/(MR_IBITS);
  for (i=0;i<=mm;i++)
  {
    b[i]=(-1);

EE[i]=mr_alloc(pak,sizeof(int))
;
  }
  mip->ERCON=TRUE;
  for (i=0;i<=mlf;i++)
  {

G[i]=mr_alloc(pak,sizeof(int));
    if (G[i]==NULL)
    {
      mlf=mm;
      for (j=mm+1;j<i;j++)
mr_free(G[j]);
      break;
    }
  }
  mip->ERCON=FALSE;
  mip->ERNUM=0;
  return 1;
}
```

```
int qsieve(int d, big *n)
{
  unsigned int i,j,a,*SV;
  unsigned char logpi;
  int
k,S,r,s1,s2,s,NS,logm,ptr,thres
hold,epri;
  long M,la,lptr;
  if (initv(d,n)<0) {chiqish =
TRUE;return;}
  hmod=2*mlf+1;
  convert(hmod,TT);
  while (!isprime(TT))
decr(TT,2,TT);
  hmod=size(TT);
  hmod2=hmod-2;
  for (k=0;k<hmod;k++)
hash[k]=(-1);
  M=50*(long)mm;
  NS=(int)(M/SSIZE);
  if (M%SSIZE!=0) NS++;
  M=SSIZE*(long)NS;
  logm=0;
  la=M;
  while ((la/=2)>0) logm++;
  rp[0]=logp[0]=0;
  for (k=1;k<=mm;k++)
  {
    r=subdiv(DD,epr[k],TT);
    rp[k]=sqrmp(r,epr[k]);
    logp[k]=0;
    r=epr[k];
    while((r/=2)>0) logp[k]++;
  }
  r=subdiv(DD,8,TT);
  if (r==5) logp[1]++;
  if (r==1) logp[1]+=2;
  threshold=logm+logb2(RR)-
2*logp[mm];
  jj=0;
  nlp=0;
  premult(DD,2,DG);
  nroot(DG,2,DG);
  lgconv(M,TT);
  divide(DG,TT,DG);
  nroot(DG,2,DG);
  if (subdiv(DG,2,TT)==0)
incr(DG,1,DG);
  if (subdiv(DG,4,TT)==1)
incr(DG,2,DG);
  forever
  {
    r=mip->NTRY;
    mip->NTRY=1;
    do
    {
      do {
        incr(DG,4,DG);
      } while(!isprime(DG));
      decr(DG,1,TT);
      subdiv(TT,2,TT);
      powmod(DD,TT,DG,TT);
    } while (size(TT)!=1);
    mip->NTRY=r;
    incr(DG,1,TT);
    subdiv(TT,4,TT);
    powmod(DD,TT,DG,BB);
    negify(DD,TT);
    mad(BB,BB,TT,DG,TT,TT);
    negify(TT,TT);
    premult(BB,2,AA);
    xgcd(AA,DG,AA,AA,AA);
    mad(AA,TT,TT,DG,DG,AA);
    multiply(AA,DG,TT);
    add(BB,TT,BB);
    multiply(DG,DG,AA);
    xgcd(DG,DD,IG,IG,IG);
    r1[0]=r2[0]=0;
    for (k=1;k<=mm;k++)
    {
      s=subdiv(BB,epr[k],TT);
      r=subdiv(AA,epr[k],TT);
      r=invers(r,epr[k]);
      s1=(epr[k]-s+rp[k]);
      s2=(epr[k]-s+epr[k]-
rp[k]);
      r1[k]=smul(s1,r,epr[k]);
      r2[k]=smul(s2,r,epr[k]);
    }
    for (ptr=(-
NS);ptr<NS;ptr++)
    {
      la=(long)ptr*SSIZE;
      SV=(unsigned int *)sieve;
      for
(i=0;i<SSIZE/sizeof(int);i++)
*SV++=0;
      for (k=1;k<=mm;k++)
      {
        epri=epr[k];
        logpi=logp[k];
        r=(int)(la%epr[k]);
        s1=(r1[k]-r)%epri;
        if (s1<0) s1+=epri;
        s2=(r2[k]-r)%epri;
        if (s2<0) s2+=epri;
        for
(j=s1;j<SSIZE;j+=epri)
sieve[j]+=logpi;
        if (s1==s2) continue;
        for
(j=s2;j<SSIZE;j+=epri)
sieve[j]+=logpi;
      }
      for (a=0;a<SSIZE;a++)
      {
        if (sieve[a]<threshold)
continue;
```

```
        lptr=la+a;
        lgconv(lptr,TT);
        S=0;
        multiply(AA,TT,TT);
        add(TT,BB,TT);
        mad(TT,IG,TT,DD,DD,PP);
        if (size(PP)<0)
add(PP,DD,PP);
        mad(PP,PP,PP,DD,DD,VV);
        absol(TT,TT);
        if (compare(TT,RR)<0)
S=1;
        if (S==1)
subtract(DD,VV,VV);
        copy(VV,TT);
        e[0]=S;
        for (k=1;k<=mm;k++)
e[k]=0;
        if (!factored(lptr,TT))
continue;
        if (gotcha())
        {
          egcd(TT,NN,PP);
          if (isprime(PP))
printf("Tub faktor     ");
          else
printf("Murakkab (tubmas)
faktor ");
          cotnum(PP,output);
          divide(NN,PP,NN);
          if (isprime(NN))
printf("Tub faktor     ");
          else
printf("Murakkab (tubmas)
faktor ");
          cotnum(NN,output);
          chiqish = TRUE;
          return;
        }
      }
    }
  }
}
#define TIMES '*'
#define RAISE '#'
int digits(big *n)
{
  int d;
  t=mirvar(0);
  d=0;
  copy(*n,t);
  while (size(t)!=0)
  {
    subdiv(t,10,t);
    d++;
  }
  mr_free(t);
  return d;
}
```

```
static char *s;
void eval_power (big oldn,big
n,char op)
{
 if (op)
power(oldn,size(n),n,n);
}
void eval_product (big oldn,big
n,char op)
{
  switch (op)
  {
    case TIMES:
    multiply(n,oldn,n);
    break;
    case '/':
    copy(oldn,t);
    divide(t,n,t);
    copy(t,n);
    break;
    case '%':
    copy(oldn,t);
    divide(t,n,n);
    copy(t,n);
  }
}
void eval_sum (big oldn,big
n,char op)
{
  switch (op)
  {
    case '+':
    add(n,oldn,n);
    break;
    case '-':
    subtract(oldn,n,n);
  }
}

void eval (void)
{
  big oldn[3];
  big n;
  int i;
  char oldop[3];
  char op;
  char minus;
  n=mirvar(0);
  for (i=0;i<3;i++)
  {
    oldop[i]=0;
    oldn[i]=mirvar(0);
  }
  LOOP:
  while (*s==' ')
  s++;
  if (*s=='-')
  {
    s++;
```

```
    minus=1;
  }
  else
    minus=0;
  while (*s==' ')
  s++;
  if (*s=='(' || *s=='[' ||
*s=='{')
  {
    s++;
    eval ();
    copy(t,n);
  }
  else
  {
    for (i=0;s[i]>='0' &&
s[i]<='9';i++)
      if (!i)
      {
        printf ("Error -
noto'g'ri son\n");
        exit (20);
      }
      op=s[i];
      s[i]=0;
      lgconv(atol(s),n);
      s+=i;
      *s=op;
    }
    if (minus) negify(n,n);
    do
      op=*s++;
      while (op==' ');
      if (op==0 || op==')' ||
op==']' || op=='}')
      {
        eval_power
(oldn[2],n,oldop[2]);
        eval_product
(oldn[1],n,oldop[1]);
        eval_sum
(oldn[0],n,oldop[0]);
        copy(n,t);
        mr_free(n);
        for (i=0;i<2;i++)
mr_free(oldn[i]);
        return;
      }
      else
      {
        if (op==RAISE)
        {
          eval_power
(oldn[2],n,oldop[2]);
          copy(n,oldn[2]);
          oldop[2]=RAISE;
        }
        else
        {
          if (op==TIMES ||
op=='/' || op=='%')
          {
            eval_power
(oldn[2],n,oldop[2]);
            oldop[2]=0;
            eval_product
(oldn[1],n,oldop[1]);
            copy(n,oldn[1]);
            oldop[1]=op;
          }
          else
          {
            if (op=='+' ||
op=='-')
            {
              eval_power
(oldn[2],n,oldop[2]);
              oldop[2]=0;
              eval_product
(oldn[1],n,oldop[1]);
              oldop[1]=0;
              eval_sum
(oldn[0],n,oldop[0]);
              copy(n,oldn[0]);
              oldop[0]=op;
            }
            else
            {
              printf ("Error -
noto'g'ri amal\n");
              exit (20);
            }
          }
        }
      }
      goto LOOP;
}
void amal(char a[500])
{
  double start, end, vaqt;
  int ip,b,d=250;
  big n;
  b=(d*45)/100;
  #ifndef MR_NOFULLWIDTH
    mip=mirsys(-b,0);
  #else
    mip=mirsys(-b,MAXBASE);
  #endif
  mip->NTRY=100;
  n=mirvar(0);
  ip=0;
  output=stdout;
  cinstr(n,a);
  if (size(n)==0)
  {
    printf("Faktorlash uchun
son kiritilmagan!\n");
    return 0;
```

```
  }
  if (size(n)<0)
  {
    printf("manfiy son!\n");
    return 0;
  }
  if (isprime(n))
  {
    printf("Bu son tub!\n");
    return 0;
  }
  start = omp_get_wtime( );
  Sleep(1000);
  brute(&n);
  if (chiqish) goto oxir;
  brent(&n);
  if (chiqish) goto oxir;
  fu= (big
*)mr_alloc((1+MULT/2),sizeof(bi
g));
  cp=(BOOL
*)mr_alloc((1+MULT/2),sizeof(BO
OL));
  plus=(BOOL
*)mr_alloc((1+MULT/2),sizeof(BO
OL));
  minus=(BOOL
*)mr_alloc((1+MULT/2),sizeof(BO
OL));
  if (digits(&n)>25)
  {

williams(10000,1000000L,1,&n);
    if (chiqish) goto oxir;

pollard(100000,5000000L,&n);
    if (chiqish) goto oxir;
  }
  if (digits(&n)>35)
  {

lenstra(20000,2000000L,10,&n);
    if (chiqish) goto oxir;
    if (digits(&n)>64)
    {

lenstra(20000,2000000L,80,&n);
      if (chiqish) goto oxir;
    }
    if (digits(&n)>72)
    {

lenstra(50000,5000000,300,&n);
      if (chiqish) goto oxir;
    }
  }
  mr_free(minus);
  mr_free(plus);
  mr_free(cp);
  mr_free(fu);
  if (digits(&n)<100)
  {
    qsieve(digits(&n),&n);
    if (chiqish) goto oxir;
  }
  else printf("&");
  cotnum(n,output);
  oxir:
    end = omp_get_wtime( );
  vaqt = end-start;
  mirkill(n);
  printf("Ketgan vaqt:  %lf\n",
vaqt);
  printf("----------------------
------------------------------
\n\n\n");
  }
int main()
{
  static char string[300];
  printf("Faktorlash uchun son
kiriting\n");
  chiqish = FALSE;
  scanf("%s",string);
  amal(string);
    return 0;
}
```

## Факторлашга оид мисоллар

### Факторлаш учун киритилган сон (256 bit)

**115792089210356248762697446949407573530086143415290314195533631308867097853950**

Tub faktor 2
Tub faktor 3
Tub faktor 5
Tub faktor 5
Tub faktor 17
Tub faktor 257
Tub faktor 641
Tub faktor 1531
Tub faktor 65537
Tub faktor 490463
Tub faktor 6700417
Tub faktor 83594504224461495178038995336787794345391692724 1

**Вақт сарфи, секунд: 1.076561**

---

### Факторлаш учун киритилган сон (384 bit)

**39402006196394479212279040100143613805079739270465446667948293404245721771496870**

329047266088258938001861606973112318
Tub faktor 2
Tub faktor 19
Tub faktor 67
Tub faktor 807145746439
Tub faktor
191737902980270981657210531557945289702269345478872327857226729569820460981367196671675197371475260 97

**Вақт сарфи, секунд: 3.515887**

---

### Факторлаш учун киритилган сон (512 bit)

**4069336299675870818389516010816270379624977206068694333302060510585180216426718461730913778103937253948784749378036404928076604915258048355293859123662170**

Tub faktor 2
Tub faktor 5
Tub faktor 3371
Tub faktor 100379
Tub faktor 3951548297
Tub faktor 129128823797
Tub faktor 5853537972529386901
Tub faktor 404484418420506704041
Tub faktor
995431178048194338231270384579874674670905247860038860443457567275232036774407335237 7

**Вақт сарфи, секунд: 85.984315**

---