ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АЛОҚА, АХБОРОТЛАШТИРИШ ВА ТЕЛЕКОММУНИКАЦИЯ ТЕХНОЛОГИЯЛАРИ ДАВЛАТ ҚЎМИТАСИ

ЎЗБЕКИСТОН ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ФАРҒОНА ФИЛИАЛИ

Қўлёзма ҳуқуқида
УДК 004.056.5

Рахматов Одилжон Рахмонбердиевич

DES СТАНДАРТ ШИФРЛАШ АЛГОРИТМИ АКСЛАНТИРИШЛАРИ ТАҲЛИЛИ ВА УНИНГ ДАСТУРИЙ ТАЪМИНОТНИ ЯРАТИШ ҲАМДА ТАРМОҚДА ҚЎЛЛАШ

5А 330201-“Компьютер тизимлари ва уларнинг дастурий таъминоти” (мутахассислиги бўйича магистр даражасини олиш учун диссертацияси)

Илмий раҳбар: доцент Акбаров Д. Е.

Фарғона – 2014

М У Н Д А Р И Ж А

КИРИШ

Мавзунинг асосланиши ва унинг долзарблиги. Ахборот-коммуникация тизимларида маълумотлар алмашинувини самарали амалга оширишни ташкил этиш бугунги ривожланган жамиятда катта аҳамият касб этади. Ахборот технологияларининг жадал ривожланиб бориши, жамият фаолиятининг кенг соҳасида турли ахборот хизматларининг вужудга келишига олиб келди. Айниқса банк ва бошқа тўлов тизимларида, давлат ва жамият манфаатлари билан боғлиқ муҳим маълумотларни алмашиш ҳамда таҳлил қилишда, тез ва ишончли маълумот алмашинуви талаб этиладиган тизимларда ахборот муҳофазаси масалалари долзарб ҳисобланади. Ҳақиқатан ҳам, ҳар қандай маълумот у ёки бу маънода ахборот-коммуникация тизими фойдаланувчиларининг манфаати билан боғлиқ. Ахборот муҳофазасини таъминлаш: ҳуқуқий-меъёрий ҳужжатлар, техник воситалар ва криптографик алгоритмлар ҳамда протоколлар негизида яратилган дастурий, аппарат-дастурий ва аппарат-техник воситаларнинг биргаликда қўллаш билан самарали амалга оширилади.

Ўзбекистон Республикаси Президенти Ислом Абдуғаниевич Каримов ва Ўзбекистон Республикаси Вазирлар Маҳкамасининг қатор фармон ва қарорларида Республикамизда ахборот технологияларини ривожлантиришнинг аниқ йўналишлари белгилаб берилиб, бу соҳа мутахассисларига фаоллик кўрсатиш учун шарт-шароитлар яратилиб берилмоқда.

Инсон тафаккури ривожининг манбаи маълумотлар (ахборотлар) мажмуидан иборатдир. Шак-шубҳасиз ўз вақтида олинган тўла ва ишончли маълумот, шу маълумот билан боғлиқ бўлган ҳолатдан келиб чиқадиган амалий фаолиятларнинг мақсадли кечишларини мувофиқлаштиришда муҳим аҳамият касб этади. Фаолият мақсадларининг турлича бўлиши табиий равишда ахборотлардан турли мақсадларда фойдаланиш асосларига сабаб бўлади. Шунинг учун бугунги, ахборотларни сақлаш ва узатиш тизимлари

бир томондан такомиллашиб мураккаблашган ва иккинчи томондан ахборотлардан фойдаланувчилар учун кенг қулайликлар вужудга келган даврда, ахборотларни мақсадли бошқаришнинг қатор муҳим масалалари келиб чиқади. Бундай масалалар қаторига катта ҳажмдаги ахборотларнинг тез ва сифатли узатиш ҳамда қабул қилиш, ахборотларни ишончлилигини таъминлаш, ахборотлар тизимида ахборотларни бегона шахслардан (кенг маънода) муҳофаза қилиш каби кўплаб бошқа масалалар киради. Ахборот ва ахборот тизимидан фойдаланиш инсоният фаолиятининг барча соҳаларига кириб бориб, муҳим аҳамият касб этиб, ривожланиб бораётган бугунги жамиятда ахборотларни мақсадли бошқариш фаоллашмоқда. Компьютерлар ва компьютер тизимлари ахборот тизимининг муҳим бўғимидир. ИНТЕРНЕТ тармоқлари жамият фаолиятининг барча соҳаларини қамраб олиб, ахборотни тез ва сифатли алмашинувини таъминлаш технологияларининг ривожланишига ижобий манба бўлиб келмокда. Юқоридаги келтирилган асосли мулоҳазалардан келиб чиқиб, ахборотларни асли ҳолидан ўзгартирилган ҳолда, яъни шифрланган ҳолда, сақлаш ва узатиш масалаларининг муҳим эканлигига шубҳа йўқдир. Ахборотларнинг муҳофазасини таъминлаш масалалари инсоният жамиятида қадимдан муҳим бўлиб келган. Айтиш мумкинки, ахборотни муҳофаза қилиш услублари жамиятда дастлабки пайдо бўлган муомала тили ва ёзуви билан узвий боғлиқ ҳамда тенгдошдир. Ҳақиқатдан ҳам, қадимда ёзув муомала воситасидан фақат айрим юқори табақадаги жамият аъзоларигина фойдаланганлар. Қадимий Миср ва Ҳиндистоннинг илоҳий китоблари бунга мисол бўла олади. Эрамиздан аввалги бешинчи асрда яшаб ўтган грек олими Геродотнинг ҳабар беришича, қадимий Мисрда шифрланган ахборотлар ролини, жрецлар, яъни юқори табақадаги етук фикрли кишилар томонидан яратилган муомала тили бажарган. Бунда учта алифбога асосланилган: ёзув, илоҳий ва маҳфий. Ёзув алифбоси оддий ўзаро муомалада қўлланилган, илоҳий алифбо диний муомала воситаси сифатида қўлланилган, маҳфий алифбо эса

маълумотларнинг асл маъносини бегоналардан муҳофаза қилишда ва астриологлар томонидан қўлланилган.

Турли ёзув алифболарининг вужудга келиши ва ривожланиши натижасида *криптография* мустақил йўналишда ривожлана борди.

Криптография – ахборотни аслидан ўзгартирилган ҳолатга акслантириш услубларини топиш ва такомиллаштириш билан шуғулланади. Дастлабки тизимлашган криптографик услублар эрамиз бошида, Юлий Цезарнинг иш юритиш ёзишмаларида учрайди. У бирор маълумотни маҳфий ҳолда бирор кишига етказмоқчи бўлса, алифбонинг биринчи ҳарфини тўртинчи ҳарфи билан, иккинчи ҳарфини бешинчиси билан ва ҳоказо тартибда алмаштириб матнни асл ҳолатидан шифрланган матн ҳолатига ўтказган.

Криптографик тизимлар йўналишидаги изланишлар айниқса биринчи ва иккинчи жаҳон уруши йиллари даврида муҳим аҳамият касб этди ва жадал ривожланди. Урушдан кейинги йилларда, ҳисоблаш техникаларининг яратилиши, уларнинг такомиллашиб, инсоният фаолиятининг барча соҳаларига чуқур ва кенг маънода кириб бориши, криптографик услубларни табиий равишда ривожланиб ва такомиллашиб боришини таъқозо этмоқда.

Криптографик услубларнинг ахборот тизими муҳофазаси масалаларида қўлланилиши, айниқса, ҳозирги кунда фаоллашиб бормоқда. Ҳақиқатан ҳам, бир томондан компьютер тизимларида ИНТЕРНЕТ тармоқларидан фойдаланган ҳолда катта ҳажмдаги давлат ва ҳарбий аҳамиятга эга бўлган, ҳамда, иқтисодий, шахсий ва бошқа турдаги ахборотни тез ва сифатли узатиш, қабул қилиш кенгайиб бормоқда. Иккинчи томондан эса бундай ахборотларнинг муҳофаза қилиниши таъминлаш масалалари муҳимлашиб бормоқда.

Ахборотни муҳофаза қилиш масалалари билан *криптология* (kryptos-маҳфий, logos-илм) фани шуғулланади. Криптология мақсадлари ўзаро

қарама-қарши бўлган иккита йўналишига эга – *криптография* ва *криптотаҳлил.*

Криптографиянинг очиқ маълумотларни шифрлаш масалаларининг математик услублари билан шуғулланиши тўғрисида юқорида айтиб ўтилди.

Криптотаҳлил эса шифрлаш услуби (калити ёки алгоритми)ни билмаган ҳолда шифрланган маълумотни асл ҳолатини (мос келувчи очиқ маълумотни) топиш масалаларини ечиш билан шуғулланади.

Ҳозирги замон криптографияси қуйидаги тўртта бўлимни ўз ичига олади:

1. Симметрик криптотизимлар.
2. Очиқ услубга ёки яна бошқача айтганда очиқ калитлар алгоритмига асосланган криптотизимлар.
3. Электрон рақамли имзо криптографик тизимлари.
4. Криптотизимлар учун криптобардошли калитларни ишлаб чиқиш ва улардан фойдаланишни бошқариш.

Криптографик услублардан фойдаланишнинг асосий йўналишлари: махфий маълумотларни очиқ алоқа канали бўйича муҳофазаланган ҳолда узатиш, уларнинг ҳақиқийлигини таъминлаш, ахборотларни (электрон ҳужжатларни, электрон маълумотлар жамғармасини) компьютерлар тизими хотирасида шифрланган ҳолда сақлаш ва шу каби масалаларнинг ечимларини ўз ичига олади.

Тадқиқотнинг объекти ва предметини белгиланиши. Ахборот-коммуникация тармоқларида алмашинадиган электрон ахборотнинг маҳфийлигини таъминловчи криптографик воситалар – симметрик калитли шифрлаш алгоритмлари тадқиқотнинг объекти ҳисобланади. Ҳусусан симметрик блоклаб шифрлаш алгоритми туркумига кирувчи DES стандарт шифрлаш алгоритми тадқиқотнинг предметини ташкил этади.

Тадқиқотнинг мақсади ва вазифалари. Фейстель тармоғи ва акслантиришлари жадвалларга асосланган симметрик блоклаб шифрлаш

алгоритми туркумига кирувчи DES стандарт шифрлаш алгоритми базавий акслантиришларини сақлаб қолган ҳолда унинг криптобардошлигини ошириш тадқиқотнинг мақсади ҳисобланади. Шу мақсаддан келиб чиқадиган тадқиқот вазифалари: Фейстель тармоғининг ва DES алгоритми базавий акслантиришларининг криптографик хусусиятларини таҳлил қилишдан, унинг калити узунлигини ошириш эвазига криптобардошлигини оширишдан иборат.

Тадқиқотнинг асосий масалалари ва фаразлари;

Магистрлик диссертация ишида тадқиқ қилинадиган асосий масалалар:

–криптографиянинг асосий масалаларининг моҳиятини ёритиш ва уларни ечиш алгоритмлари классификациясини таҳлил қилиш;

–DES стандарт шифрлаш алгоритмининг криптографик таҳлили, уни такомиллаштириш ҳамда дастурий таъминоти асосларини яратиш;

–янги такомиллаштирилган MDES – TDES шифрлаш алгоритмининг криптографик таснифи ва унинг криптобардошлигини баҳолаш.

Тадқиқотнинг гипотезаси (илмий фарази) DES стандарт симметрик блоклаб шифрлаш алгоритми базавий акслантиришлари негизини сақлаб қолган ҳолда ахборот-коммуникация тармоқларида электрон ахборотнинг кафолатли маҳфийлигини таъминловчи MDES – TDES такомиллаштирилган вариантини ишлаб чиқишдан иборат.

Мавзу бўйича қисқача адабиётлар таҳлили ёки муаммонинг ўрганилганлик даражаси. Ахборотнинг криптографик муҳофазаси соҳасидаги илмий ишларнинг муаллифлари, криптография фанининг вужудга келишини қуйдаги учта даврга ажратадилар: 1949 йилгача бўлган қатъий исботсиз – фақат интуиция ва “ишончга” асосланган – илмий асосланмаган криптография даври, 1949 йилдан 1976 йилгача бўлган *илмий асосланган махфий калитли* криптография даври, 1976 йилдан кейинги очиқ *калитли криптография* даври.

К.Э. Шенноннинг 1949 йилда чоп этилган “Махфий тизимларда алоқа назарияси”, деб номланган илмий мақоласи илмий асосланган *махфий*

калитли криптография даврини бошлаб берди. У ўзининг 1948 йилда эълон қилинган – ахборотлар назариясига бағишланган илмий мақоласи негизида махфий алоқа тизими назариясининг асосини яратди. Унинг томонидан эълон қилинган илмий мақолалари катта аҳамиятли бўлсада, криптология соҳасидаги илмий мақолаларнинг сезиларли кўпайишига олиб келмади. Эҳтимол бунга сабаб, Шенноннинг махфий тизимларда алоқа назариясининг махфий калитга асосланган бўлиб, махфий калитни фойдаланувчига етказиш масалалари ечимининг мураккаблиги билан боғлиқлигидадир [1-5]. 1976 йилда У.Диффи ва М.Е.Хеллманнинг “Криптографияда янги йўналиш”, деб номланган мақоласининг эълон қилиниши шу соҳадаги очиқ илмий ишлар ривожини берди. Уларнинг бу ишлари махфий алоқа тизимларида маълумотларни шифрлаш ва шифрни очишда махфий калитнинг тизим фойдаланувчилари орасида махсус муҳофазаланган алоқа канали орқали узатилиши ва қабул қилинишига ҳожат бўлмайдиган илмий-амалий услуб асосларини яратиб, бугунги кунда ҳам ривожланиб ва долзарблашиб бораётган *очиқ калитли криптография даврини* бошлаб берди [6, 7].

Криптография ўтган асрнинг охирларигача давлат органлари алоқа тизимларида алмашинадиган маълумотлар муҳофазасининг таъминланишида қўлланиб келинди. Компьютер тармоқлари ва электрон ҳужжат айланиши технологияларининг ривожланиши, молия, банк ишлари, савдо-сотиқ каби йўналишларда қўлланилиши ахборот муҳофазасининг криптографик усулларини умумжамият фаолиятининг турли соҳаларига кенг кириб боришига сабаб бўлди. Бу кенг қамровли қўлланишлар ахборотни криптографик муҳофазасини таъминлашнинг асосий масалаларини қўйилишини ва уларнинг ечимларини таъминловчи криптографик усул ҳамда воситалар моҳиятини ёритишни, маълумотларни муҳофазасига таҳдид солувчи сабабларни аниқлаш ва бартараф этиш усулларини, криптографик воситаларини қўлланиш моҳиятига кўра туркумланишини, криптографик ҳимоялаш воситаларини танлаш мезонларини, электрон ҳужжат айланиши жараёнлари муҳофазасини таъминлашнинг криптографик хусусиятларини

ёритишни, криптографик ҳимоялаш воситаларини ахборот-коммуникация тизимларида қўллаш усулларини, калитларни муҳофазаланган тақсимоти протоколларини ишлаб чиқишни ва каби соҳалардаги масалалар ечимига бағишланган илмий тадқиқот натижаларини эълон қилинишига сабаб бўлди [8-138].

Янги асрнинг бошларидан криптология элементлари ахборот-коммуникация технологиялари фанлари билан боғлиқ ҳолда кўплаб олий ўқув юртларида у ёки бу ном билан ўрганилиб келинмоқда. Бу соҳада Ўзбекистон Республикаси олимлари томонидан ҳам етарли даражада илмий-тадқиқот ишлари олиб борилмоқда ва бунга Каримов М.М, Акбаров Д.Е, Хасанов П.Ф, Ғаниев С.К, Арипов М.М, Ахмедова О.П, Хасанов Х.П, Мусаев А.И. ва бошқалар томонидан эришилган натижаларни келтириш мумкин.

Ушбу магистрлик диссертация иши ахборот-коммуникация тизимларида алмашиладиган маълумотларни кафолатли криптографик мухофазалашнинг кенг қамровли муаммоларини ўз ичига олган. Ўз навбатида муаммоларни бартараф қилиш ахборот хавфсизлигини таъминлашнинг криптографик воситалари бўлган: шифрлаш, хэш-функция ва электрон рақамли имзонинг мавжуд стандарт алгоритмларини, криптоалгоритмлар учун кафолатли бардошли калитлар ишлаб чиқиш ва уларни бошқариш масалаларининг мавжуд ечимларини шунингдек уларни ахборот-коммуникация тизимларида қўлланилиши услубларини чуқур таҳлил қилишни ва етарли даражада ўрганишни талаб қилади.

Ҳозирда Ўзбекистон Республикаси Ҳукумати раҳбарияти томонидан ахборот-коммуникация тизимларини кафолатли криптографик муҳофазасини таъминлашнинг чора тадбирларини меёрий – ҳуқуқий томонларини ишлаб чиқилиши босқичма босқич амалга оширилмоқда. Аммо бу чора тадбирларни амалга оширувчи миллий кафолатли криптобардошли – криптографик муҳофаза воситалар ишлаб чиқилиши долзарб бўлиб қолмоқда.

Тадқиқотда қўлланилган услубларнинг қисқача тавсифи. Ушбу магистрлик диссертацияда ахборотни маҳфийлигини таъминловчи

симметрик шифрлаш алгоритмларини, хусусан симметрик блоклаб шифрлаш алгоритмларини криптобардошлигини таъминловчи таҳлили: *чизиқсизлик, мувозанатлашганлик, регулярлик, максимал корреляция-иммунлик тартибга эгалик, қатъий кескин ўзгариш самарадорлик тамойилини (критерийсини) ва тарқалиш тамойилини (критерийсини)* қаноатлантириши шартларини текшириш усулларидан фойдаланилган.

Тадқиқот натижаларининг назарий ва амалий аҳамияти.

–криптографик алгоритмларни улар асосини ташкил этувчи акслантиришларнинг хусусиятларига кўра туркумлаш криптотаҳлил усулларини яратишнинг тизимли илмий ёндошувига асос бўлади;

–Фейстел тармоғини такомиллаштириш усули мавжуд стандарт шифрлаш алгоритмларининг бардошлигини ҳисоблаш техника ва технологияларини ривожланишига мос равишда самарали модификациялашни амалга ошириб боришни илмий ҳамда амалий асосини таъминлайди;

–DES стандарт симметрик блоклаб шифрлаш алгоритми базавий акслантиришлари негизини сақлаб қолган ҳолда ишлаб чиқилган янги такомиллаштирилган MDES–TDES шифрлаш алгоритми ахборот-коммуникация тармоқларида электрон ахборотнинг кафолатли маҳфийлигини таъминлайди.

Тадқиқотнинг илмий янгилиги:

–Фейстель тармоқли DES стандарт симметрик блоклаб шифрлаш алгоритми базавий акслантиришлари негизини сақлаб қолган ҳолда ишлаб чиқилган янги такомиллаштирилган MDES–TDES шифрлаш алгоритми ахборот-коммуникация тармоқларида электрон ахборотнинг кафолатли маҳфийлигини таъминлайди;

–Янги такомиллаштирилган MDES–TDES шифрлаш алгоритмини ишлаб чиқишда қўлланилган усуллар Фейстель тармоқли барча симметрик блоклаб шифрлаш алгоритмларини такомиллаштириш учун ҳам ўринли;

–Ҳисоблаш техника ва технологияларини ривожланиб боришига мос равишда таклиф этилган такомиллаштириш усулини қўллаб керакли кафолатли криптобардошликка эга бўлган симметрик блоклаб шифрлаш алгоритмига самарали эришиш мумкин.

Диссертация таркибининг қисқача тавсифи: Диссертация мундарижа, кириш, учта боб, хулоса, 139 та номдаги фойдаланилган адабиётлар рўйхатидан (иловадан иборат). Диссертациянинг асосий ҳажми 87 бет матн, 16 та жадвал ташкил топган.

1-БОБ. КРИПТОГРАФИЯНИНГ АСОСИЙ МАСАЛАЛАРИ ВА УЛАРНИ ЕЧИШ АЛГОРИТМЛАРИ КЛАССИФИКАЦИЯСИ

1.1. Асосий тушунчалар ва ахборот муҳофазасини таъминлашда криптографик масалаларнинг қўйилиши

Ахборот муҳофазасининг криптографик услублари очиқ маълумотларни ўзгартириб, фақат калит маълум бўлгандагина уни асл ҳолатига қайтариш имкониятини беради.

Шифрлаш ва дешифрлаш масалаларига тегишли бўлган, маълум бир алифбода тузилган маълумотлар *матнларни* ташкил этади.

Алифбо - ахборотни кодлаш учун фойдаланиладиган чекли сондаги белгилар тўплами. Мисол сифатида:

- ўттиз олтита белгидан (ҳарфдан) иборат ўзбек тили алифбоси;

- ўттиз иккита белгидан (ҳарфдан) иборат рус тили алифбосии;

- йигирма саккизта белгидан (ҳарфдан) иборат лотин алифбоси;

- икки юз эллик олтита белгидан иборат ASCII ва КОИ – 8 стандарт компьютер кодларининг алифбоси;

- бинар алифбо, яъни 0 ва 1 белгилардан иборат алифбо;

- саккизлик ва ўн олтилик саноқ тизимлари белгиларидан иборат алифболарни келтириш мумкин.

Матн - алифбонинг элементларидан (белгиларидан) ташкил топган тартибланган тузилма.

Шифрлаш - очиқ матн деб аталувчи *дастлабки маълумотни шифрланган маълумот (криптограмма)* ҳолатига ўтказиш жараёни.

Дешифрлаш - шифрлашга тескари бўлган жараён, яъни калит ёрдамида шифрланган маълумотни дастлабки ҳолатга ўтказиш.

Калит - дастлабки маълумотни бевосита шифрлаш ва дешифрлаш учун зарур манба.

Криптографик тизим - очиқ маълумотни шифрлаш ва дешифрлаш жараёнини ташкил этувчи амаллар мажмуи бўлиб, алифбо белгиларини алмаштириш кетма-кетлигидан иборат.

Криптотизимлар икки қисмга бўлинади: *симметрик* ва *асимметрик* - *очиқ калитли.*

Симметрик криптотизимларда шифрлаш учун ҳам ва дешифрлаш учун ҳам бир хил калитдан фойдаланилади.

Очиқ калитли криптотизимларда иккита калитдан фойдаланилади – ўзаро математик жиҳатдан боғлиқ бўлган *очиқ* ва *ёпиқ* калитлардан. Бунда маълумотлар маълумот юборилаётган шахснинг ҳаммага маълум бўлган очиқ калити билан шифрланади ва фақат маълумот юборилаётган шахснинг ўзигагина маълум бўлган ёпиқ калит билан дешифрланади.

Калитларни тақсимлаш ва *бошқариш* – криптобардошли калитларни ишлаб чиқиш (ёки яратиш), уларни сақлаш, ҳамда калитларни фойдаланувчилар орасида муҳофазаланган ҳолда тақсимлаш жараёнларини ўз ичига олади.

Электрон рақамли имзо - электрон матнга илова қилинадиган криптографик алмаштиришдан иборат бўлиб, шу матн жўнатилган шахсга қабул қилинган электрон матннинг ва матнни рақамли имзоловчининг ҳақиқий ёки ноҳақиқийлигини аниқлаш имконини беради.

Криптобардошлилик - шифрлаш калити номаълум бўлган ҳолда шифрланган маълумотни дешифрлашнинг қийинлик даражасини белгилайди. Криптобардошлиликни белгиловчи бир нечта кўрсаткичлар мавжуд, булардан:

- дешифрлаш учун қидирилаётган калитларнинг мумкин бўлган барча имкониятлари сони;

- дешифрлаш учун зарур бўлган ўртача вақт.

Ахборотни муҳофаза қилиш мақсадида шифрлаш сифати калитнинг махфий сақланиши ва шифрлашнинг криптобардошлилик даражасига боғлиқ.

Ахборот-коммуникация тармоқларида ахборотларнинг криптографик муҳофазасини таъминлашнинг асосий масалалари келтирилади [1-15], булар:

- ахборотнинг махфийлигини (конфиденциаллигини) таъминлаш;

- ахборотнинг тўлалигини (ўзгармаганлигини) таъминлаш;

-ахборотнинг аутентификациясини (маълумот субъектларини ҳақиқийлигини) таъминлаш;

- ахборотнинг муаллифини ва муаллифликдан бош тортмаслигини таъминлаш;

- криптографик алгоритмлар учун криптобардошли калитлар ишлаб чиқариш ва уларни тармоқ фойдаланувчиларига муҳофазаланган ҳолда тарқатилишини бошқариш.

Ахборот муҳофазасининг санаб ўтилган масалаларини криптографик усуллар билан ечиш воситаси шифрлаш алгоритмларидир.

Ахборот махфийлигини (конфиденциаллигини) таъминлашнинг асосий мақсади очиқ алоқа тармоғида махфийликни таъминлаган ҳолда махфий маълумотларни алмашинуви масалаласини ечишдан иборат. Ахборот-коммуникация тизимлари очиқ алоқа тармоғи фойдаланувчиларининг маълумотлар мажмуасидан турли мақсадларни, баъзан эса ўзаро қарама-қарши мақсадларни назарда тутиши, махфийлигини кафолатли таъминлаган ҳолда маълумотлар алмашинувини амалга оширишни тақазо этади. Ўзаро қарама-қарши мақсадларни назарда тутувчи томонлар криптотаҳлилчилари бугунги ривожланган ахборот технологиялари ютуқларидан фойдаланиб, алоқа тармоғига боғланиб, маълумотлар алмашинувини кузатиш (мониторингини олиб бориш), шифрлаш алгоритмларини қўллаш билан махфийлиги таъминланган маълумотларга эга бўлиш, уларни дешифрлаш чора - тадбирларини амалга оширишга ҳаракат қилиш имкониятларига эга. Бундай ҳатти-ҳаракатлар (ҳужумлар) икки турда

бўлади: *фаол* (*актив*) ва *фаол бўлмаган* (*пассив*). Фаол бўлмаган ҳужумлар эшитиш, алоқа тармоғида алмашинаётган маълумотларни мазмунини кузатиш ва таҳлил қилиш, шифрланган маълумотларни ёзиб олиш ва дешифрлаш каби хатти-ҳаракатлар билан боғлиқ. Фаол ҳужумлар маълумотлар алмашинуви жараёнига тўсқинлик қилиш, узатилаётган маълумотлар мазмунини ўзгартириш каби хатти-ҳаракатларни ўз ичига олади.

Очиқ маълумот *M*, шифрланган маълумот *C*, шифрлаш алгоритми *E* ва калити k_1, дешифрлаш алгоритми *D* ва калити k_2, деб белгиланса, шифрлаш жараёни $E_{k_1}(M) = C$, дешифрлаш жараёни $D_{k_2}(C) = D_{k_2}(E_{k_1}(M)) = M$ кўринишда ифодаланади.

Турли хусусиятли - ҳужжатли, овозли, тасвирли маълумотларнинг барчасини шифрлаб, алоқа тармоғида узатилиши ва қабул қилинишини кафолатли мухофаза қилинишини самарали кечишини таъминловчи ягона криптографик алгоритм мавжуд эмас. Чунки, криптографик воситалар маълумотларнинг физик хусусиятлари, уларнинг махфийлик даражаси, хажми, сигнал кўринишида ифодаланиш усули, алоқа тармоғида узатилиш технологиялари хусусиятлари, қўлланиладиган техник қурилмаларнинг қиймати, фойдаланишга қулайлиги каби хосликларни ҳисобга олган ҳолда танланади.

Ахборот тўлалигини таъминлашнинг асосий мақсади очиқ алоқа тармоғида маълумотлар алмашинуви жараёнларида рақиб томоннинг алмашинаётган маълумотларни ўз манфаатидан келиб чиққан ҳолда ўзгартиришларини аниқлашнинг имконини берувчи криптографик воситаларни (алгоритмларни) яратишдан иборат. Бунинг учун узатилаётган маълумотга, уни қабул қилувчи томон учун, маълумотни ўзгарган ёки ўзгармаганлигини текшириш имконини берувчи, махсус алгоритм билан ҳисобланадиган - *назорат йиғиндиси* ёки *маълумотнинг аутентификация коди*, деб аталувчи қўшимча қўшилади. Бундай қўшимча қўшиш усулининг кодлаштириш усулидан фарқи, назорат йиғиндиси ҳисобланадиган

криптографик алгоритмнинг махфий калитга боғлиқлигидадир. Махфий калитни билмаган ҳолда узатилаётган маълумотга рақиб томонидан ўзгартириш киритиш эҳтимоллиги деярли йўқ. Шундай эҳтимоллик ўлчови *шифрнинг имитобардошлилиги* – фаол ҳужумларга бардошлилик ўлчови дейилади. Берилган M - маълумотни аутентификациясини (ҳақиқийлигини) текшириш имконини берувчи қайд қилинган узунликдаги қиймат қабул қиладиган назорат йиғиндисини ҳисоблаш алгоритмининг калит деб аталувчи махфий k -параметрга ва M –маълумотга боғлиқ функцияси $h_k(M) = S$ -хэшлаш функцияси деб юритилади. Хэш-функцияга қуйдаги талаблар қўйилади:

- калитни билмаган ҳолда берилган M – маълумотнинг $h_k(M) = S$ қийматини ҳисоблаш мумкин эмас;

- берилган M – маълумот ва унинг хэш - функция қийматини $h_k(M) = S$ билган ҳолда шу M – маълумотдан фарқли $M \neq M_1$, лекин хэш - функция қиймати тенг $h_k(M) = h_k(M_1) = S$ бўлган M_1 - маълумотни топиш имкони йўқ.

Келтирилган биринчи талаб маълумотнинг қалбакилаштирилишига йўл қўймасликни таъминлайди, иккинчи талаб эса бирор маълумотни бошқа маълумот билан алмаштириш имкониятини чекланишини таъминлайди.

Ахборотнинг аутентификацисини (маълумот субъектларининг ҳақиқийлигини) таъминлашнинг мақсади ахборот алмашинуви тўғри ўрнатилганлигини, томонларнинг ҳақиқийлигини, маълумот ва унинг муаллифи каби субъектларнинг ҳақиқийлигини текширишни таъминлашдан иборат.

Ахборот алмашинуви жараёни (сеанси) тўғри ўрнатилганлигини аутентификациси: тармоқ бўғинлари боғланишларининг тўғри амалга оширилганлигини текширишни, рақиб томонидан маълумотларни қайта узатиш имконияти йўқлигини ва маълумотлар алмашинувининг ўз вақтида кечишини таъминлаш каби тадбирларни ўз ичига олади. Бунинг учун

узатилаётган маълумотларга осон текшириладиган қўшимча параметрлар киритишдан фойдаланилади.

Ахборот муаллифлигини ва муаллифликдан бош тортмаслигини таъминлашнинг мақсади бир-бирига ишонмайдиган томонларнинг маълумотлар алмашинуви жараёнларида жўнатувчи маълумотни юборганлигини рад этиб, бу маълумотни олувчининг ўзи тузганлигини даъво қилиши ёки ҳақиқатан ҳам, олувчи ўзи қабул қилиб олган маълумотни ўзгартириши, қалбакилаштириши ва янги маълумот тузиши, сўнгра бу маълумотни жўнатувчидан олганлигини даъво қилиши мумкин бўлган ҳолатларда келиб чиқадиган муаммо ва низоларни тўғри ҳал этишдан иборат. Бундай муаммо ва низоларни ҳал этишнинг фундаментал механизми электрон рақамли имзо (ЭРИ) ҳисобланади. ЭРИ жўнатилаётган маълумотни ташкил этувчиларига ва жўнатувчининг махфий калитига боғлиқ ҳолда ҳисобланиб, жўнатилаётган маълумотга илова қилинадиган рақамли кетма-кетликдан ташкил топади. Маълумотни қабул қилувчи томон қабул қилинган маълумотни бу рақамлар кетма-кетлиги ва жўнатувчининг очиқ калитига боғлиқ ҳисоблашларни бажариб, маълумотнинг аутентификацисини амалга оширади. Шундай қилиб ЭРИ жарёни алгоритми икки қисмдан рақамли имзони ҳисоблаш (шакллантириш) ва рақамли имзони текширишдан иборат. Рақамли имзони ҳисоблаш махфий калитга боғлиқ бўлгани учун ҳам уни фақат маълумотни жўнатувчи (яъни маълумотнинг ҳақиқий муаллифи) тўғри шакллантира олади. Рақамли имзони текшириш очиқ калит орқали амалга оширилади, яъни исталган томон учун унинг тўғрилигини текшира олиш имконияти мавжуд.

Криптобардошли калитлар ишлаб чиқариш мақсади калит блокини ташкил этувчи элементлар (битлар ёки байтларнинг) тасодифийлигини таъминлашдан иборат.

1.2. Шифрлаш алгоритмларининг моҳияти ва улар акслантиришларининг хусусиятлари ҳамда бардошликларига кўра классификациялари

Шифрлаш алгоритмлари асосларини очиқ маълумотни ифодаловчи алифбо белгиларини ёки белгилар бирикмаларини (уларни *шифр қийматлар* деб ҳам аталади [2]) шифрмаълумотни ифодаловчи алифбо белгиларига ёки белгилар бирикмаларига (уларни *шифрбелгилар* деб ҳам аталади [2]) акслантирувчи математик моделлар ташкил этиши юқорида таъкидланган эди. Шунинг учун ҳам шифрлаш алгоритмларини синфларга ажратишнинг бошланғич босқичи, улар негизидаги акслантириш турлари асосида амалга оширилади. Агар шифрлаш жараёнида очиқ маълумот алифбоси белгилари шифр маълумот алифбоси белгиларига алмаштирилса, бундай акслантиришга асосланган шифрлаш алгоритми *ўрнига қўйиш шифрлаш* синфига киради. Агар шифрлаш жараёнида очиқ маълумот алифбоси белгиларининг ўринлари алмаштирилса, бундай шифрлаш алгоритми *ўрин алмаштириш шифрлаш* синфига киради. Кўриниб турибдики, ўрин алмаштириш шифрлаш алгоритмларида очиқ маълумотни ташкил этувчи алифбо белгиларининг маъноси шифр маълумотда ҳам ўзгармасдан қолади. Аксинча, ўрнига қўйиш шифрлаш алгоритмларида шифрмаълумотни ташкил этувчи алифбо белгилари маъноси очиқ маълумотни ташкил этувчи алифбо белгиларининг маъноси билан бир хил бўлмайди. Шифрлаш жараёнида ўрнига қўйиш ва ўрин алмаштириш акслантиришларининг комбинацияларидан биргаликда фойдаланилса, бундай шифрлаш алгоритми *композицион шифрлаш* туркумига киради. Демак, шифрлаш алгоритмлари акслантириш турларига қараб *ўрнига қўйиш*, *ўрин алмаштириш* ва *композицион шифрлаш* синфига бўлинади.

Умумий тасаввурга кўра, ўрнига қўйиш шифрлаш алгоритмлари акслантиришларининг математик моделлари кўп қийматли функциялар билан ифодаланади. Бундай ҳолат дешифрлаш жараёнида турли ноқулайликларни келтириб чиқаради. Шунинг учун бир қийматли (тескариси

мавжуд бўлган) функциялар билан ифодаланувчи акслантиришларни қўллаш қулайлик туғдиради. Шундай қилиб, табиий равишда, ўрнига қўйиш шифрлаш алгоритмлари *бир қийматли* ва *кўп қийматли шифрлаш* синфига бўлинади. Бир қийматли шифрлаш алгоритмларида очиқ маълумот алифбоси белгиларининг ҳар бирига шифр маълумот алифбосининг битта белгиси мос қўйилади. Кўп қийматли шифрлаш алгоритмларида очиқ маълумот алифбоси белгиларининг ҳар бирига шифр маълумот алифбосининг иккита ёки ундан ортиқ чекли сондаги белгилари мос қўйилади, яъни очиқ маълумот алифбосининг бирор x_i белгисига шифр маълумот алифбосининг чекли $\{y_{i1}, y_{i2}, ..., y_{it}\}$ тўпламдан олинган бирор y_{ij} , $(1 \le j \le t)$, белгиси мос қўйилади.

Шифрлаш алгоритмлари, калитлардан фойдаланиш турларига кўра, *симметрик* ва *асимметрик* синфларга бўлинади. Агар шифрлаш ва дешифрлаш жараёнлари бир хил калит билан амалга оширилса, бундай шифрлаш алгоритми симметрик шифрлаш алгоритми синфига киради. Агар шифрлаш жараёни бирор k_1 калит билан амалга оширилиб, дешифрлаш жараёни $k_2 \neq k_1$ бўлган k_2 калит билан амалга оширилиб, k_1 калитни билган ҳолда k_2 калитни топиш ечилиши мураккаб бўлган масала билан боғлиқ бўлса, бундай шифрлаш алгоритми асимметрик шифрлаш алгоритми синфига таалуқли бўлади.

Шифрлаш жараёни очиқ маълумотни ифодаловчи элементар (масалан: бит, ярим байт, беш бит, байт) белгиларни шифрмаълумотни ифодаловчи элементар белгиларга акслантириш асосида амалга оширилса, бундай шифрлаш алгоритми *узлуксиз(оқимли) шифрлаш* синф туркумига киради.

Шифрлаш жараёни очиқ маълумот алифбоси белгиларининг икки ва ундан ортиқ чекли сондаги бирикмаларини шифрмаълумот алифбоси белгиларининг бирикмаларига акслантиришга асосланган бўлса, бундай шифрлаш алгоритми *блокли шифрлаш* синфига киради.

Шифрлаш жараёнида очиқ маълумот алифбосининг бирор алоҳида олинган a_i белгиси ҳар доим шифрмаълумот алифбосининг бирор

фиксирланган b_j белгисига алмаштирилса, бундай шифрлаш алгоритми *бир алифболи шифрлаш* синфига киради. Агар шифрлаш жараёнинг ҳар хил босқичларида очиқ маълумот алифбосининг бирор алоҳида олинган a_i белгиси шифрмаълумот алифбосининг ҳар хил b_j, b_l, ..., b_t белгиларига алмаштирилса, бундай шифрлаш алгоритми *кўп алифболи шифрлаш* синфига киради.

Шифрлаш жарёнида очиқ маълумот алифбоси белгилари ёки алифбо белгилари бирикмалари бирор амал бажариш билан шифрмаълумот алифбоси белгилари ёки уларнинг бирикмаларига алмаштирилса, бундай шифрлаш алгоритми *гаммалаштирилган шифрлаш* синфига киради.

Адабиётлар рўйҳатида келтирилган [1, 139] манбааларда шифрлаш алгоритмларининг акслантиришлари асослари хусусиятларига ва криптохужумларга бардошликлари бўйича туркумларининг (синфлари) тўла таснифи алоҳида-алоҳида кўриб чиқилган.

Бирор алфавитда берилган очиқ маълумотни, шифрмаълумот алфавити белгиларига оддий акслантиришлар композициялари билан амалга оширилиб – шифрлаб, шифрлаш акслантиришлари ошкор этилмаса – шифрлаш алгоритми номаълум бўлса, бундай шифрларни дешифрлашни амалга ошириш етарли даражада мураккаб масала ҳисобланади. Аммо, криптграфик воситалар асосидаги алгоритмларнинг сир тутилиши бу воситаларга ишончсизликни туғдиради. Ҳақиқатан ҳам, улар асосидаги криптоалгоритмларни бу воситаларни ишлаб чиқувчининг билиши, фойдаланувчиларнинг эса билмаслиги ёки моҳиятига тушиниб етмаслиги ахборот муҳофазасини таъминлашнинг мантиғига тўғри келмайди. Шунинг учун ахборот муҳофазасини таъминлашнинг криптографик воситалири алгоритмлари барча фойдаланувчиларга маълум бўлиб, унинг криптобардошлиги фақат алгоритмда ишлатиладиган калитнинг маҳфий сақланишини ўзига боғлиқ бўлиши Кирхгоф таъмоили сифатида бундан икки аср муқаддам такидланган [1-3]. Ҳозирда айнан шу таъмоилга роя қилинади

ва амалда фойдаланиб келинаётган криптографик алгоритмларнинг хусусиятлари илм-фан, ҳисоблаш техника ҳамда технологияларининг ютуқлари асосида доимий равишда криптобардошлилик даражаси таҳлил қилиб борилмоқда.

Ушбу параграф криптоалгоритмларнинг асосидаги акслантиришларнинг хусусиятларига кўра криптобардошлилик даражасини илмий тасдиқловчи фактлар нечоғли ишончли эканлигини аниқлаш ва туркумлаш масалаларининг таҳлили ҳақида.

Криптоалгоритмлар криптобардошлик даражасининг ишончлилигига кўра: *мутлақо бардошли*, *ишончли бардошли* ва *бардошли* турларга ажратилади.

Мутлақо бардошли криптоалгоритмлар шифрлаш алгоритми калитини топиш мумкин эмаслиги исботланган теоремаларга асосланган бўлади. Шубҳасиз бардошли криптоалгоритмлар туркумига: "*бир марталик блокнот*" усули билан шифрлаш алгоритми, калити бир марта ишлатиладиган *Вернам* шифрлаш алгоритми, аниқмасликнинг квант механикаси тамоилларига асосланган – *квант криптографияси* тизимлари мисол бўла олади.

Ишончли бардошли криптоалгоритмлар мутахасислар томонидан ечилиши мураккаб деб тан олинган математик масалага асосланади. Ишончли бардошли криптоалгоритмлар туркумига: характеристикаси етарли катта бўлган чекли майдонда дискрет логарифмлаш масаласининг мураккаблигига асосланган Диффи-Хеллиман ва электрон рақамли имзо (ЭРИ) алгоритмлари, етарли катта сонни туб кўпайтувчиларга ажратишнинг вақт билан ва ҳисоблаш техникаси хотираси билан боғлиқ мураккабликларига асосланган RSA ҳамда ЭРИ алгоритмлари, эллиптик эгри чизиқда тартиби етарли катта бўлган рационал координатали нуқталарни топиш ҳамда уларни эллиптик эгри чизиқда қўшишнинг вақт билан ва

ҳисоблаш техникаси хотираси билан боғлиқ мураккабликларга асосланган алгоритмлар мисол бўлади.

Бардошли алгоритмлар чуқур таҳлил қилиниб ўрганилган масалаларга келтириб бўлмайдиган математик масаланинг мураккаблигига асосланган. Бардошли криптоалгоритмлар туркумига: *AES-FIPS 197*, *ГОСТ 28147-89*, *DES*, *FEAL* ва бошқа блоклаб шифрлаш алгоритмлари киради.

Мутлақо бардошли криптотизимларни ишончлилигини юқори бўлиши билан бир қаторда амалдаги татбиқида ноқулайликлар ҳам мавжуд. Хусусан, шифрлаш калитининг бир марта қўлланилишидан келиб чиқадиган катта хажмга эга бўлишлик хоссасига кўра унинг муҳофазасини кафолатли таъминланган ҳолда сақлашни амалга оширишдир. Квант криптографияси тизими қиммат сарф-ҳаражатлар билан боғлиқ оптик толали алоқа каналининг бўлишини талаб этади ҳамда унинг ишончлилигини исботи физика фани ютуқларига таянган ҳолда қиммат тажриба-синовлар кўрсатилади.

Ишончли бардошли криптоалгоритмларнинг ютуғи улар асосидаги ечилиши мураккаб деб тан олинган математик масаланинг чуқур ўрганилганида. Криптобардошликни ошириш зарурияти туғилганда унинг алгоритм параметрларини тезкор ўзгартиришни амалга оширишнинг имкониятини чегараланганлиги бундай алгоритмларнинг камчилиги ҳисобланади. Айниқса бундай алгоритмларга асослан криптографик аппарат қурилмаларга асосланган ахборот-коммуникация тармоқларида бундай ўзгартиришларни тезкор амалга ошириш ҳар доим ҳам қулай бўлавермайди.

Бардошли криптоалгоритмлар асосидаги акслантиришларнинг ечилиши мураккаб бўлган математик масалалар билан боғлиқлик хусиятлари чуқур таҳлил қилинмаган бўлсада, бу акслантиришлар криптобардошлилик самарадорлигини тезкор амалга оширишнинг имкониятлари қулайдир.

Ахборотнинг криптографик муҳофазасини таъминлашнинг асосий масалалари қуйидагилардан иборат [1-4]:

– ахборотнинг махфийлигини (конфиденциаллигини) таъминлаш;

–ахборотнинг бутунлигини (ўзгармаганлигини) текшириш имкониятини таъминлаш;

–ахборотнинг аутентификациясини (маълумот субъектларини ҳақиқийлигини) текшириш имкониятини таъминлаш;

– ахборотнинг муаллифини ва муаллифликдан бош тортмаслигини таъминлаш;

– криптографик алгоритмлар учун криптобардошли калитлар ишлаб чиқариш ва уларни тармоқ фойдаланувчиларига кафолатли муҳофазаланган ҳолда тарқатилишини таъминлаш ҳамда бошқариш.

Ахборотнинг криптографик муҳофазасини таъминлаш масалаларининг криптографик усуллар билан ечиш воситаси шифрлаш алгоритмларидир.

Шифрлаш ва дешифрлаш алгоритмлари орқали аборотнинг маҳфий алмашинуви таъминланади.

Ахборотнинг бутунлигини (ўзгармаганлигини) текшириш имконияти калитли ёки калитсиз хеш-функция (ХФ) алгоритмларидан фойдаланиб таъминланади.

Ахборотнинг аутентификациясини (маълумот субъектларини ҳақиқийлигини) текшириш имконияти, унинг муаллифини ва муаллифликдан бош тортмаслигини электрон рақамли имзо (ЭРИ) алгоритмлари билан таъминланади.

Ахборот-коммуникация тармоқларида маълумотлар алмашинувининг маҳфийлигини, бутунлигини текшириш ва аутентификациясини амалга ошириш имкониятларини таъминлашнинг криптографик воситалари ахборот муҳофазасининг криптотизимини ташкил этади.

Криптотизимга криптоаналитик томонидан амалга ошириладиган криптохужумлар қанчалик самарасиз бўлса, криптотизим шунчалик *бардошли* ҳисобланади ва аксинча. Криптотизимнинг бардошлилик тушинчасининг мазмун-моҳияти криптоаналитикнинг мақсади ва мақсадини

амалга ошириш имкониятидан келиб чиққан ҳолда белгиланади. Криптоаналитикни асосий мақсади шифрланган маълумотни шифрлаш алгоритмини ва дешифрлаш калитини топишдан иборат.

Шифрлаш алгоритмлари акслантиришларининг математик моделлардан иборатлиги шифрмаълумотларни таҳлил қилиш натижасида шифрлаш алгоритмини аниқлаш, шифрлаш алгоритми маълум бўлганда эса калитни топиш, калит номаълум бўлганда ҳам шифрмаълумотни дешифрлашга эришиш каби уринишларни математик усулларини амалга ошириш имкониятларига манбаа бўлади.

Криптоалгоритмнинг бардошлигини ифодаловчи сонли ўлчов криптоаналитикнинг ўз мақсадига эришишга олиб келадиган энг яхши алгоритм мураккаблиги каби аниқланади. Криптоаналитикнинг олдига қўйган мақсади ва мақсадини амалга ошириш имкониятига кўра криптоалгоритм бардошлилиги тушинчаси моҳияти келиб чиқилади.

Криптоалгоритмнинг унинг калити билан боғлиқ бардошлигнингқуйидаги турлари бор:

−энг самарали натижа берувчи алгоритмдан фойдаланиб дешифрлаш калитини топиш мураккаблиги билан аниқланувчи − *калит бардошлиги*;

−*калитсиз ўқий олишга − дешифрлашга бардошлилик;*

−*калитга боғлиқ ҳолда* энг самарали натижа берувчи алгоритмдан фойдаланиб ҳақийқий бўлмаган ахборотни ҳақийқий каби тақдим этиш имкониятининг мураккаблиги билан аниқланувчи − *имитабардошлик;*

−*калит бадошлигига боғлиқ бўлмаган ҳолда* ҳақийқий бўлмаган ахборотни ҳақийқий деб тақдим этиш (RSA алгоритмида шундай имконият мавжуд) каби.

Криптографик воситалар турларига кўра: *криптоалгоритмларнинг акслантиришларига боғлиқ бардошлиги, криптографик протоколлар бардошлиги, калитларни ишлаб чиқиш ва тарқатиш алгоритмларининг бардошлиги* каби криптотаҳлил масалалари мавжуд

Криптобардошлилик даражаси криптоаналитик ва фойдаланувчи Криптобардошлилик даражаси криптоаналитик ва фойдаланувчи имкониятиларига боғлиқ. Криптоаналитик эга бўлган манбааларга кўра криптотаҳлил турлари:

− криптоаналитик шифрматинларга эга бўлиб, очиқ матн ҳақида маълумотга эга эмас;

− криптоаналитик шифрматинларга ва уларга мос очиқ матнларга эга;

− криптоаналитик шифрматинларга ва уларга мос махсус танлаб олинган очиқ матнларга эга.

Криптобардошли деб тан олинган ва амалда қўлланиб келинаётган ҳамда янги яратилган алгоритмларни криптотаҳлил қилиш долзарб масала ҳисобланади. Чунки, илм-фан, ҳисоблаш техника ва технологияларининг

ютуқларига таяниб, бу ютуқларни криптографик алгоритмларнинг бардошсизлик хусусиятларни очишга қўлланиши ўз вақтида бардошсиз алгоритмларни топиш ва уларни такомиллаштириш ёки алмаштириш каби чора-тадбирларни белгилайди. Бунинг учун эса маълум бўлган криптотаҳлил усулларини такоммиллаштириб бориш ва янгиларини яратиб бориш лозим.

Криптотаҳлил усуллари математика фанининг криптографик масалаларини ечиш билан боғлиқ соҳадаги ютуқларга таяниши мумкин, масалан:

− етарли катта сонни туб кўпайтувчиларга ажратиш усулларини RSA шифрлаш алгоритмида маҳфий калитни топиш учун қўллаш мумкин:

− характеристикаси етарли катта бўлган чекли майдонда дискрет логарифмлашни амалга ошириш усулларини Эль-Гамал шифрлаш алгоритмида, DSA ва ГОСТ Р 34.10 стандарт электрон рақамли имзо алгоритмларида маҳфий калитни топиш учун тадбиқ этилади;

− эллиптик эгри чизиқда рационал координатали юқори тартибли нуқтани топишни ва рационал координали нуқталарни қўшишни рационал усулларини эллиптик эгри чизиқда шифрлаш алгоритмларида, ECDSA-2000 ва ГОСТ Р 34.10-2001 стандарт электрон рақамли имзо алгоритмларида маҳфий калитни аниқлашда ишлатилади.

Криптотаҳлил шунингдек, DES, AES FIPS-197, ГОСТ 28147-89, O’z DSt 1106 : 2006 каби стандарт шифрлаш алгоритмлари акслантиришлари криптографик хусусиятларини таҳлил қилиш билан боғлиқ математик натижаларга асосланади.

Кўп ҳолларда, криптотаҳлил усуллари масаланинг қўйилиши ва ечилиши билан боғлиқ бўлган барча маълумотларга таяниб ўтказилган ҳамда ўтказиладиган сонли ҳисоб-китоб натижаларининг статистик баҳоларини ўрганишни ҳамда таҳлил қилишни талаб этади. Шунинг учун криптотаҳлил алгоритмлари эҳтимоллар назарияси ютуқларидан самарали фойдаланади.

Шундай қилиб, криптоалгоритмлар акслантиришларининг хусусиятларига кўра криптобардошлилик даражасини тасдиқловчи

фактларнинг нечоғли ишончли эканлигини илмий асослаш ва туркумлаш масалаларининг таҳлили кўриб ўтилди.

1.3. Стандарт шифрлаш алгоритмлари ва уларга қўйиладиган талаблар

1972 йилда АҚШнинг Стандарт ва Технологияларнинг Миллий Институти (National Institute of Standards and Technology, NIST) алоқа ва компьютер тармоқларининг маълумотларини муҳофазасини таъминлаш дастури билан чиқиб, стандарт сифатида қабул қилиниши мумкин бўлган криптографик алгоритмга қўйилган талабларни эълон қилди. Стандарт лойиҳасини баҳолашнинг бир нечта критерийларини келтирди:

– алгоритм юқори криптобардошлиликни таъминлаши керак;

– алгоритм тўлалигича аниқ ва тушинарли бўлиши керак;

–алгоритмнинг криптобардошлилиги унинг маҳфий сақланишига боғлиқ бўлмай фақат унинг калитини маҳфий тутилишига асосланиши керак;

– алгоритм барча фойдаланувчиларга маълум бўлиши керак;

–алгоритм аппарат-техник, аппарат-дастурий, дастурий ва бошқа амалий қўлланиш технологиялари учун қулай ҳамда иқтисодий самарали бўлиши керак;

– алгоритмни тўғри ёки нотўғри ишлашини текшириш имконияти бўлиши керак;

–алгоритм экспорт учун рухсат этиладиган бўлиши керак.

1974-1976 йилларда маълумотларни симметрик шифрлаш алгоритми ***DES*** (Data Encryption Standard) ишлаб чиқилиб, 1980 йилда NIST (National Institute of Standards and Technolody) томонидан стандарт (FIPS PUB 46) сифатида қабул қилиниб, ҳар беш йилда қайта сертификацияланиши такидланди.

1983, 1985 ва 1993 йиларда ***DES*** алгоритми ҳеч қандай ўзгаришсиз қайта сертификацияланган.

1997 йида ***DES*** алгоритмининг акслантиришларини бардошлилигидан ташқари қуйидаги кўрсаткичлар:

– калит узунлигини етарли эмаслиги;

– замонавий микропрцессорларда қўлланиш имкониятларининг чекланганлиги;

– тезлиги ва бошқа хусусиятлари;

сабаблари бўйича эскирган ҳисобланиб, NIST томонидан ҳукумат миқиёсидаги муҳим маълумотларни муҳофазасини таъминлашнинг янги стандарт шифрлаш алгоритми учун танлов эълон қилинди.

Танлов бўйича қуйидаги талаблар қуйилди:

– криптоалгоритм очиқ эълон қилинган бўлиши керак;

– криптоалгоритм симметрик блокли шифр бўлиб, 128, 192 ва 256 битли калитлардан фойдаланиш имкониятларига эга бўлиши керак;

–криптоалгоритм самарали аппарат ҳамда дастурий қўлланиш имкониятига эга бўлиши керак;

–криптоалгоритм патентланмаган бўлиб, ихтиёрий кўринишда фойдаланиши мумкин бўлиши керак;

–криптоалгоритм ушбу кўрсаткичлар бўйича текширилиб ва ўрганиб чиқилади: **криптобардошлилик, амалий қўлланилишга кенг қулайлик, смарт - карталарда қўлланиш имкониятлари.**

Танловда 12 та давлатдан 15 та алгоритм қатнашди.

2000 йилнинг октябрида танлов охирига етказилиб, ўзининг **криптобардошлилиги, самарадорлиги, қулай амали қўлланишларга эгалиги, оз миқдорда хотира талаб этишига** кўра Бельгиялик мутахассислар томонидан таклиф этилган RIJNDAEL алгоритми ғолиб деб топилди.

2002 йилнинг 26 майида RIJNDAEL алгоритми асосида Фейстел тармоғига асосланмаган янги сандарт шифрлаш алгоритми **AES FIPS - 197** қабул қилинди. Бу алгоритм барча раун акслантиришлари математик асосини ташкил этувчи функцияларнинг тескариси мавжуд бўлиб, асосий криптографик хусусиятларидан бири раунд калитлари узунликларининг 128 (такомиллашган вариантларида 192 ва 256) бит эканлигидир.

1978 йилда СССР ДҲҚ илмий техник кенгашида маълумотларни стандарт шифрлаш алгоритмини яратиш бўйича гуруҳ тузилиб, яратилиши керак бўлган алгоритмга ушбу талаблар қўйилди:

–алгоритмда қўлланиладиган амаллар компьютер имкониятлари билан мос бўлиши керак (мисол учун, маълумотларнинг қийматлари ва алгоритмда бажариладиган ҳисоблашлар натижалари қийматларининг иккилик саноқ системасидаги ифодаси 32 битдан кўп бўлмасин);

–алгоритм очиқ (маълум) бўлиб, унинг криптобардошлилиги алгоритмни маҳфий сақланишига боғлиқ бўлмай фақат калитнинг маҳфий тутилишига боғлиқ.

Бу талабларнинг биринчиси 32 разрядли процессорларга асосланган компьютерларда амаллар бажариш жарёнларига мос бўлиб, алгоритмнинг тез ишлашини таъминлашга асос бўлади. Иккинчиси эса алгоритм криптобардошлигига шубҳа бўлмаслигини таъминлаш чора ва тадбирлари масалаларини ечимлари билан боғлиқ.

1983 йилда Фейстел тармоғига асосланган калит узунлиги 256 бит бўлган **ГОСТ 28147-89** симметрик блокли шифрлаш алгоритмининг микросхемаси ишлаб чиқилди. Алгоритм муаллифи – Заботин Иван Александрович.

Мутахасисларнинг фикрича **ГОСТ 28147-89** симметрик блокли шифрлаш алгоритми ҳозирдаги барча криптографик талабларга жавоб беради.

DES шифрлаш алгоритми акслантиришларининг криптобардошликларига эътирознинг йўқлиги, унинг узоқ вақт миллий стандарт сифатида бенуқсон ишлатилиб келинганлиги, бой криптографик хусусиятларга эга – Фейстель тармоғи деб ном олган аппарат қурилма яратишга қулай архитектуравий конструкцияга эгалиги, камчилиги унинг калити узунлигининг етарли эмаслиги, бу алгоритмни такомиллаштиришга ундайди. Алгоритмнинг базавий акслантиришларини сақлаб қолган ҳолда унинг калитини етарли узун қилиб олиб амалий тадбиқларига эришиш муаммосини ечиш ушбу магистрлик диссертация ишининг мақсади ҳисобланади.

Хозирда Украина, Белорусия, Қозоғистон, Ўзбекистон Давлатлари ҳам ўзларининг стандарт шифрлаш ва электрон рақамли имзо алгоритмларига эга.

1 - боб бўйича хулоса.

1. Ахборот муҳофазасини таъминлашнинг асосий тушунчалари таснифи ва криптографик усуллар билан ечиши керак бўлган: маълумотнинг маҳфийликни таъминлаш, унинг бутунлигини (ўзгармаганлигини текширишни) таъминлаш, маълумот манбаасини, авторлигини (аутинтификациясини) ва авторликдан бош тортмаслигини таъминлаш масалаларининг қўйилиши тадқиқи ёритилди.

2. Ахборот муҳофазасини таъминлашнинг криптографик усулининг воситаси – шифрлаш алгоритмларининг ечилиши керак бўлган масалаларга қўлланиши бўйича моҳияти, улар асосидаги акслантиришларнинг хусусиятлари ва криптохужумларга бардошлиги бўйича туркумлари тадқиқи тизимли келтирилди.

3. Стандарт шифрлаш алгоритмларига заруриятнинг келиб чиқиши асосланди. DES, AES FIPS-197, ГОСТ 28147-89, O’z DSt 1106 : 2006 каби стандарт шифрлаш алгоритмлари таснифи ва моҳияти тизимли баён этилди.

2-БОБ. DES СТАНДАРТ ШИФРЛАШ АЛГОРИТМИНИНГ КРИПТОГРАФИК ТАҲЛИЛИ, УНИ ТАКОМИЛЛАШТИРИШ ҲАМДА ДАСТУРИЙ ТАЪМИНОТИ АСОСЛАРИНИ ЯРАТИШ

2.1. Фейстель тармоқли симметрик блоклаб шифрлаш алгоритмларининг криптографик хусусиятлари таҳлили

Ўрнига қўйиш шифрлаш жараёнида очиқ маълумотни ташкил этувчи алифбо белгиларини айрим (алоҳида) олинган ҳолда, шифрмаълумот алифбосининг айрим (алоҳида) олинган белгиларига алмаштириш, ёки, ўрин алмаштириш шифрлаш жараёнида очиқ маълумотни ташкил этувчи алифбо белгиларини айрим (алоҳида) олинган ҳолда ўринларини алмаштириш амалга оширилган бўлсин. Бундай ҳолатда шифрлаш жараёни алгоритмининг криптобардошлилигини ошириш учун калит узунлиги шифрланиши керак бўлган маълумот узунлиги даражасида бўлиши зарур бўлади. Мисол учун, шартли равишда, бирор алифбода тузилган ушбу “$x_1 x_2 \dots x_N$” – очиқ маълумотдан, уни ташкил этувчи алифбо белгиларининг ўринларини алматириш натижасида “$x_{i_1} x_{i_2} \dots x_{i_N}$” –шифрмаълумот ҳосил қилинган бўлса, у ҳолда калитни ифодаловчи $1 \to i_1$, $2 \to i_2$, …, $N \to i_N$ - ўрин алмаштиришлар сони очиқ маълумотни ташкил этувчи алифбо белгиларининг сони билан тенг. Худди шу каби, ўрнига қўйиш шифрлаш алгоитмларидан фойдаланишда очиқ маълумот частотавий хусусиятларининг шифрмаълумотга кўчмаслигини таъминлаш учун кўп алифболи шифрлаш алгоритмларидан фойдаланилади, бунга эришиш учун эса, юқорида кўрилганидек шифрлаш жараёни босқичларида бир хил белгиларни ҳар хил белгиларга алмаштириш, яъни калит узунлигини ошириш зарурияти туғилади. Шифрланиши керак бўлган маълумот ҳажмининг ортиши билан, шифрлаш жарёнини амалга оширишда қўлланиладиган алгоритмнинг калити узунлигини мос равишда ортиб бориши, криптобардошлиликни таъминлаш нуқтаи назаридан самарали бўлсада, бундай ҳолат алгоритмларнинг амалда қўлланишлари нуқтаи назаридан: калитларни сақлашда, уларни тарқатишда, аппарат-техник

таъминотларни амалга оширишда ва бошқа шу каби ҳолатларда ноқулайликлар туғдиради. Шунинг учун шифрланиши керак бўлган маълумотни, уни ташкил этувчи алифбо белгиларининг маълум бир узунликдаги бирикмалари (блоклари) бирлашмаси (конкатенацияси) кўринишда ифодалаб, ана шу блокларнинг алоҳида-алоҳида самарали ва криптобардошли шифрланишини амалга ошириш масаласи келиб чиқди. Бу масала симметрик блокли шифрлаш алгоритмлари орқали амалга оширилди. Симметрик блокли шифрлаш алгоритмларининг асосини очиқ маълумот блокларини юқори даражада *аралаштириш* ва *тарқатиш* (ёйилиш, таралиш) хоссаларига эга бўлган акслантиришлар ташкил этади [1,2,3,8,15]. *Самарали аралаштириш* берувчи ($\oplus$, $\bmod 2^n$, *ўрин алмаштириш жадваллари*, *циклик суришлар* ва ҳокозо) амаллар *коррелияцион иммунстлик* – шифрланиши керак бўлган ёки калит блокларини ташкил этувчи алифбо белгиларидан бирининг ўзгариши, акслантириш натижасида олинган шифрблокни ташкил этувчи алифбо белгиларининг фақат биргина мос белгиси ўзгаришига таъсир қилиб, бошқа қисмига таъсир этмаслигини таъминловчи ўрин алмаштириш шифрлаш акслантиришларидан иборат. *Самарали тарқатиш* берувчи бир алифболи ва кўп алифболи ўрнига қўйиш акслантиришларга асосланган S – блок акслатиришлари *чизиқсизликни* - шифрланиши керак бўлган ёки калит блокларини ташкил этувчи алифбо белгиларидан бирининг ўзгариши, акслантириш натижасида олинган шифрблокни ташкил этувчи алифбо белгиларининг икки ва ундан ортиқ қисмига таъсир этишини таъминловчи ўрнига қўйиш шифрлаш алгоритмлари акслантиришларидан иборат.

Аралаштирувчи акслантиришлар очиқ маълумот ва унга мос келувчи шифрмаълумот блокларининг частотавий (статистик) ва аналитик боғлиқлик хусусиятларини ўрнатишни мураккаблаштирса, тарқатувчи акслантиришлар очиқ маълумот блоки битта белгисининг ўзгаришини мос шифрмаълумот блокининг кўп белгилари ўзгаришига таъсир қилишини ифодалаб, очиқ маълумотнинг частотавий (статистик) хусусиятларини шифрмаълумотга кўчмаслигини таъминлайди.

Симметрик блокли шифрлаш алгоритмлари бир нечта босқичлардан (раундлардан) иборат бўлиб, ҳар бир раунд аралаштирувчи ва тарқатувчи акслантиришлардан тузилган. Бундай асосда тузилиш тамоили, ҳар бир раунд шифрлаш жараёнини ҳар хил калитлар билан бир хил турдаги акслантиришларни амалга оширишга, ҳамда, дешифрлаш жараёнини раунд акслантиришлари ва калитларини тескари тартибда қўллашнинг самарали имконини беради. Алгоритм асосини ташкил этувчи, раунд шифрлаш жараёнини амалга оширувчи, аралаштириш ва тарқатиш хусусиятларига эга бўлган функциялар *асосий акслатиришлар* дейилади. *Асосий акслантириш*ларнинг аппарат-техник жиҳатдан қулай қўлланиш модели сифатида тескари боғлиқликка эга бўлган силжитиш регистларини келтириш мумкин [1,2, 3, 8, 15]. Бунда тарқатувчи акслантириш тескари боғлиқликни таъминловчи функция билан, аралаштирувчи акслантириш эса, регистрдаги маълумотларни силжитиш билан амалга оширилади.

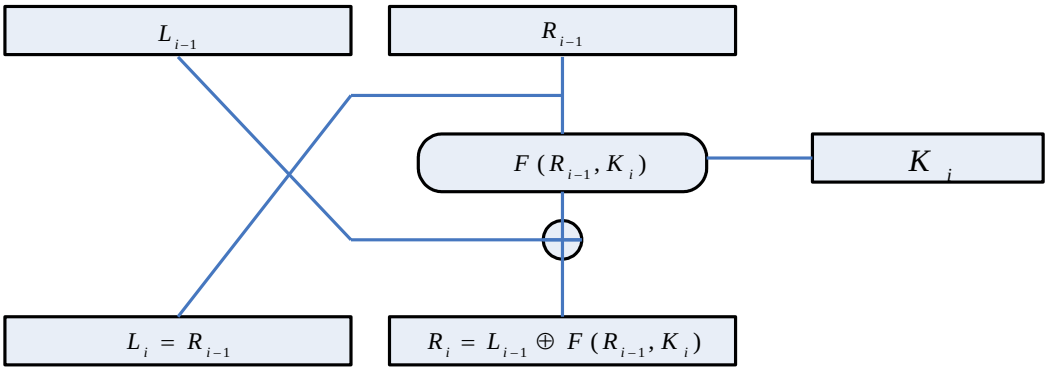
Шифрланиши керак бўлган маълумот блокини силжитиш регистрларига киритиб (юклаб), регистрдаги маълумотни шартли равишда чап ва ўнг қисмблок векторларига бўлиб, улар устида ҳар хил калитлар билан бир хил турдаги акслантиришларни босқичма-босқич амалга оширишга асосланган – *Фейстел тармоғи* деб аталувчи шифрлаш жараёни функционал қурилмасига асосланган алгоритмлар кенг тарқалган.

Такидлаш жоизки, ўтган асрнинг 70-йиллари бошида электрон маълумотларни компьютер тармоқларида узатиш технологияларининг ривожланиши билан уларни муҳофазалаш масалаларини ечиш зарурияти келиб чиқди. Бутун дунёга машҳур бўлган IBM– International Business Machines компанияси ахборот-коммуникация тармоқларида алмашинадиган маълумотларни муҳофазалашга бағишланган илмий тадқиқот ишлари дастурини ишлаб чиқиб уни бажаришга киришди. Бундай тадқиқот ишларининг олиб борилиши ахборот-коммуникация тармоқлари технологияларининг бошқа соҳаларининг ривожланишига ҳам ижобий таъсир қилди. IBM компанияси электрон маълумотлар муҳофазаси билан

боғлиқ илмий тадқиқот ишлари дастурида қўйилган масалаларни ечишга Станфорд университети ва Массачусетс технология институтининг мутахассисларини жалб этди. Чунки бу мутахассислар ахборот муҳофазасини таъминлашнинг криптографик усуллари қўлланиладиган соҳаларда фаолият кўрсатиб келар эди.

Симметрик калитли шифрлаш тизимларини тадқиқ қилиш олимлар жамоасини доктор Хорст Файстель бошқарди. У Bell Laboratories компаниясида Клод Шеннон билан ҳамкорликда ишлаб, таниқли криптограф сифатида танилган эди.

Тескариси мавжуд криптобардошли мураккаб акслантиришларни яратиш кўп сарф-ҳаражатлар, ҳисоб-китоблар талаб қилиб, уларнинг амалий қўлланишлари самарадорлиги юқори бўлмаган алгоритмларни ишлаб чиқишга олиб келди. Шу сабабга кўра Файстель тескариси мавжуд криптобардошли акслантиришларни тадқиқ қилмай, бундай акслантиришлар қатнашмаган криптобардошлилиги юқори бўлган шифрлаш тизимларини топиш масаласини ечимига киришди. У бу масаланинг ечимини қуйидагича ҳал этди. Шифрланадиган блок иккита L_0, R_0 қисмларга ажратилади. Фейстел тармоғи $i-$раунди итератив блокли шифрлаш қуйидаги схема бўйича аниқланади:



Фейстел тармоғи $i-$***раунди.***

Бу ерда $X_i = (L_{i-1}, R_{i-1})-$ i -раунд учун L_{i-1} ва R_{i-1} қисмларга ажратилган кирувчи маълумот, $Y_i = (L_i, R_i)$ эса X_i ни $i-$раунд калити K_i билан F акслантириш натижасида ҳосил бўлган шифрмаълумот.

Фейстел тармоғи i – раундининг шифрлаш жараёни математик модели қуйидагича ифодаланади:

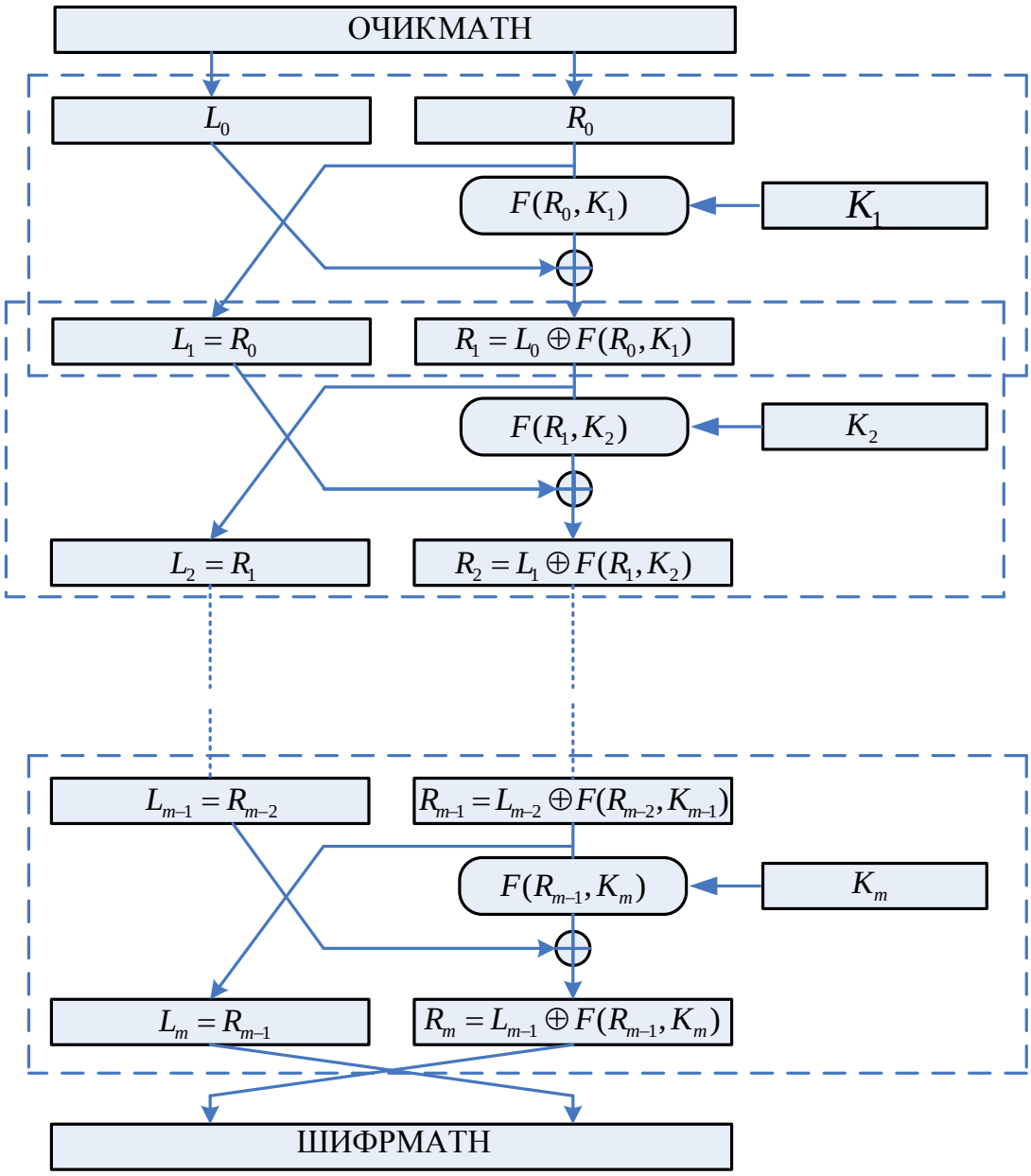
$$\begin{cases} L_i = R_{i-1}, \\ R_i = L_{i-1} \oplus F(R_{i-1}, K_i). \end{cases}$$

Бундай тармоққа асосланган алгоритмлар бир неча итерациядан ташкил топган K_i калитларда шифрланадиган акслантиришлардан (функциялардан) ташкил топган.

Фейстел тармоғи акслантиришларининг асосий хоссаси F -раунд функцияси тескариси мавжуд бўлмаса ҳам, Фейстел тармоғи бу акслантиришларини тескарисини топиш имконини беради. Ҳақиқатан ҳам, шифрлаш жараёни i – раунд математик моделидаги $\oplus$ - модуль 2 бўйича иккилик санок тизимида қўшиш амали хоссасидан фойдаланган ҳолда қуйидаги тенгликка эга бўлинади:

$$\begin{cases} R_{i-1} = L_i, \\ L_{i-1} = R_i \oplus F(L_i, K_i). \end{cases}$$

Бу тенгликлар Фейстел тармоғи асосида қурилган шифрлаш алгоритмларини дешифрлашининг математик моделини ифодалайди. Умумий ҳолатда m – раундли Фейстел тармоғининг функционал схемаси қуйидагича ифодаланади:



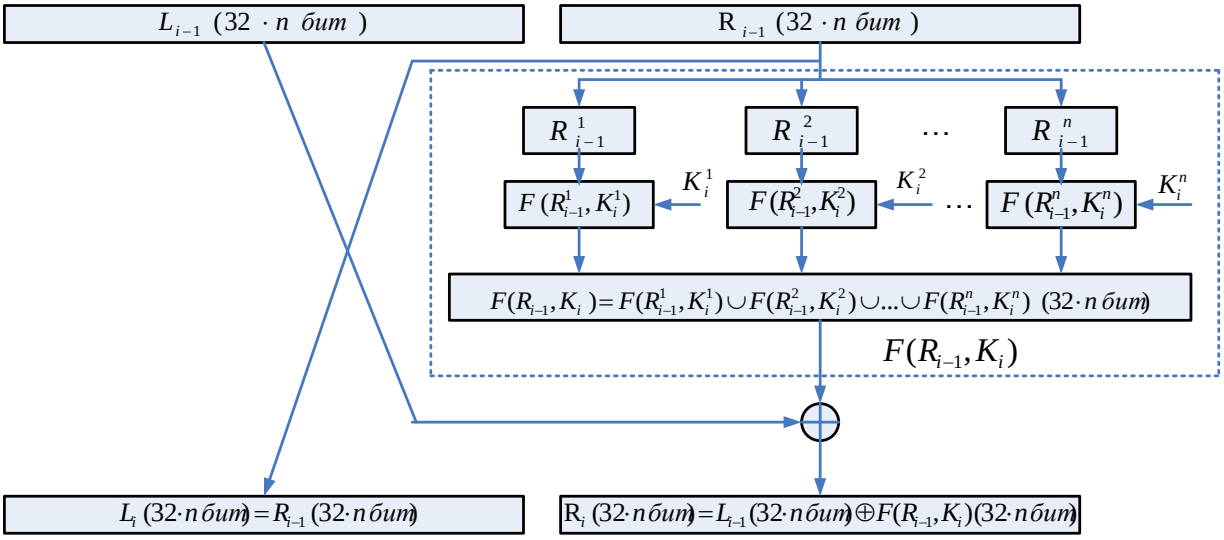
Раундлари сони m бўлган Фейстел тармоғи

Фейстел тармоғи асосида қурилган шифрлаш алгоритмларида шифрлаш ва дешифрлаш учун бир хил алгоритм, акслантириш ва амаллардан фойдаланилиб, фақат раунд калитларининг қўлланилиши тескарисига ўзгаради, яъни дешифрлашда 1-раундда K_m, 2-раундда K_{m-1} ва ҳакозо охирги раундда K_1 ишлатилади. $F(R_{i-1}, K_i)$ функция тескариси мавжуд бўлмаса ҳам, дешифрлаш самарали амалга оширилади.

2.2. Фейстель тармоғини ва унга асосланган алгоритмларни такомиллаштириш

Ҳисоблаш техникалари қурилмаларининг такомиллашуви натижасида, бугунги кунда стандарт сифатида қўлланилиб келинаётган шифрлаш алгоритмларининг бардошлилиги, уларда қўлланилалиган акслантиришларга боғлиқ бўлмаган ҳолда, улар калитларининг узунликларига нисбатан камаяди. Юқорида санаб ўтилган Фейстел тармоғига асосланган шифрлаш алгоритмлари бугунги кунда ҳам стандат сифатида бенуқсон қўлланилиб келинаётганлиги, бундай алгоритмлар акслантиришларини сақлаб қолган ҳолда, уларнинг калитларини узайтириш масаласининг долзарблиги келиб чиқади. Қуйида Фейстел тармоғига асосланган барча шифрлаш алгоритмларини такомиллаштириш учун умумий бўлган қоида келтирилади.

Бугунги кунда кўплаб амалда қўлланилиб келинаётган компьютерлардаги арифметик амалларни бажарувчи қурилма иккилик саноқ тизимида 32 разряд билан ифодаланувчи сонлар учун мўлжалланган. Келажакда компьютер фойдаланувчилари учун бундан ҳам катта 64, 128 ва хоказо разрядли сонлар устида арифметик амаллар бажариш имкониятини берувчи тезкор қурилмалар яратилиши табиий ҳол. Шуларни ҳисобга олиб, Фейстел тармоғига асосланган шифрлаш алгоритмларини акслантириш асосларини сақлаб қолган ҳолда, K-калит узунликларини ошириш масаласи ечилади. Мана шундай масалани ечиш учун Фейстел тармоғи қуйидагича такомиллаштирилади:



Такомиллашган Фейстел тармоғи i **–** ***раунди.***

Бу ерда:

1. Шифрланиши керак бўлган очиқ маълумот блоклари узунлиги $64m$ *бит*га тенг.
2. Калит узунлиги $|K| \cdot n$ *бит*га тенг.
3. $K_i = K_i^1 K_i^2 ... K_i^n$ – i -раунд қисм калитлари бирлашмаси.
4. Фейстел тармоғи R – ўнг ва L – чап қисмлари узунликлари: $|L| = |R| = 32 \cdot n$ *бит*га тенг.
5. $L_{i-1}(32 \cdot n \text{ бит})$ – i -раунд чап қисми.
6. $R_{i-1}(32 \cdot n \text{ бит})$ – i -раунд ўнг қисми.
7. $L^1_{i-1}(32 \text{ бит})$, $L^2_{i-1}(32 \text{ бит})$,..., $L^n_{i-1}(32 \text{ бит})$ – i -раунд чап қисмнинг 32 *бит*лик бўлаклари.
8. $R^1_{i-1}(32 \text{ бит})$, $R^2_{i-1}(32 \text{ бит})$,..., $R^n_{i-1}(32 \text{ бит})$ – i -раунд ўнг қисмнинг 32 *бит*лик бўлаклари.
9. $F(R^1_{i-1}, K^1_i)$, $F(R^2_{i-1}, K^2_i)$,..., $F(R^n_{i-1}, K^n_i)$ – i -раунд Фейстел функциясининг мос акслантиришлари.

Такомиллашган Фейстел тармоғи i – раунди математик модели қуйидагича ифодаланади:

$$\begin{cases} L_i(32 \cdot n \text{ бит}) = R_{i-1}(32 \cdot n \text{ бит}) \\ R_i(32 \cdot n \text{ бит}) = L_{i-1}(32 \cdot n \text{ бит}) \oplus F(R_{i-1}, K_i)(32 \cdot n \text{ бит}) \end{cases}$$

Юқорида такомиллашган ва асосий Фейстел тармоғи схемасидан кўриниб турибдики, такомиллашган Фейстел тармоғида такомиллаштириш параметри n га боғлиқ бўлган ҳолда бир нечта $F(R_{i-1}^1, K_i^1)$, $F(R_{i-1}^2, K_i^2)$,..., $F(R_{i-1}^n, K_i^n)$ Фейстел функциялари учрайди. Бу эса n га боғлиқ ҳолда бир неча Фейстел тармоғига асосланган алгоритмлар функцияларидан ёки бир неча **S**-блоклардан фойдаланиш имконини беради. Шунингдек, n га боғлиқ равишда калит узунликлари ҳам ортиб боради, яъни $n = 1$ да калит узунлиги 256 бит бўлса, $n = 2$ да калит узунлиги 512 ва ҳаказо бўлади. Калит узунлиги ва такомиллаштириш параметри n орасида қуйидагича боғлиқлик ўрнатиш мумкин:

$$l_1 = l \cdot n$$

бу ерда l – асосий алгоритм калити узунлиги, l_1 – такомиллашган алгоритм калити узунлиги.

Фейстел тармоғига асосланган такомиллашган ва асосий алгоритмларнинг шифрлаш ва дешифрлаш тезлиги тенг, чунки $n = 1$ да алгоритм блок узунлиги 64 га тенг бўлиб, алгоритм тезлиги 20 тактдан иборат бўлса, $n = 2$ да такомиллашган алгоритм блок узунлиги 128 бит бўлиб, тезлиги 40 тактдан иборат бўлади.

Демак, такомиллашган Фейстел тармоғи қуйидаги афзалликларга эга:

1) Такомиллаштириш параметри n га боғлиқ ҳолда шифрлаш алгоритми хоссалари ва бардошлилигини сақлаб қолган ҳолда алгоритм калити узунлигини ошириб бориш имконияти мавжуд. Бу эса, ўз навбатида, ҳисоблаш техникаси қурилмаларининг такомиллашуви натижасида алгоритм калити узунлиги тўлиқ танлаш усулига бардошсиз бўлиб қолишининг олдини олади.

2) Алгорим тезлиги такомиллаштириш параметри n га боғлиқ эмас, яъни Фейстел тармоғига асосланган такомиллашган ва асосий алгоритм тезликлари тенг. Бу хосса ўз навбатида алгоритм тезлигини сақлаб қолган ҳолда такомиллаштириш имкониятини беради.

Қуйида Фейстел тармоғига асосланган DES симметрик блокли шифрлаш алгоритми акслантиришлари таҳлили ва уни такомиллаштириш масаласи ечими тадқиқ этилади.

2.3. DES стандарт шифрлаш алгоритми акслантиришларининг таҳлили

Юқорида такидланганидек, DES стандарт шифрлаш алгоритми Америка Қўшма Штатлари (АҚШ) “Миллий Стандартлар Бюроси” томонидан 1977 йилда эълон қилинган. 1980 йилда АҚШнинг “Стандартлар ва Технологиялар Миллий Институти” бу алгоритмни давлат ва савдо-сотиқ молияси соҳасидаги махфий бўлмаган, аммо муҳим бўлган маълумотларни рухсат этилмаган жисмоний ва юридик шахслардан муҳофаза қилинишида шифрлаш алгоритми сифатида қўллаш стандарти деб қабул қилди.

DES алгоритмида: дастлабки 56 битли калитдан раунд калитларини ҳосил қилишнинг мураккаб эмаслиги, раунд асосий акслантиришларининг аппарат-техник ва дастурий таъминот кўринишларида қўлланилишини таъминлашнинг қулайлиги, ҳамда, улар криптографик хоссаларининг самарадорлиги – криптобардошлилигининг юқорилиги, бу алгоритмнинг асосий хусусиятларини белгилайди.

Шифрлаш жараёни 64 битли очиқ маълумот блокларини алгоритмда берилган *IP* –жадвал бўйича ўрин алмаштириш, унинг натижасини дастлабки 56 битли калитдан алгоритмда келтирилган жадваллар билан битларнинг ўринларини алмаштириш, циклик суриш ва баъзи битларни йўқотиш акслантиришларидан фойдаланиб ҳосил қилинадиган 48 битли раунд калитлари ҳамда асосий акслантиришлари билан 16 марта шифрлаш, шифрлаш натижаси блоки битларини берилган IP^{-1} – жадвал бўйича ўринларини алмаштиришдан иборат.

Алгоритм акслантиришларини ёритиш учун қуйидаги белгилашлар киритилади:

L_i ва R_i –ҳар бири 32 битли блоклар бўлиб, Фейстел тармоғини чап ва ўнг қисимларини ифодалайди, $i = 0,1,...,16$;

$\oplus$ – битлар блоклари векторлари кординаталарини $\bmod 2$ бўйича қўшиш;

K_i – 48 битли раунд калитлари;

F – Фейстел тармоғи асосий акслантиришлари функцияси;

IP – ўрин алмаштириш жадвали.

Навбатдаги Т –блокни шифрлаш жараёни бу блок битларини қуйидаги бошланғич *IP* – ўрин алмаштириш жадвали:

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

асосида акслантириш билан бошланади *T* – блокнинг 58-бити 1-бит ўрнига, 50-бити 2-бит ўрнига ва ҳоказо қолган битлар ҳам жадвалда кўрсатилган ўринларга ўтказилади. Сўнгра, олинган натижа иккита 32 битлик L_0 ва R_0 - қисмларга ажратилиб, 16 раундлик Фейстел тармоғи асосий акслантиришлари функцияси билан ҳар хил 48 битлик калитларда шифрланади. Яъни раунд натижаси, $T_{i-1} = L_{i-1}R_{i-1}$ $(i-1)$ деб белгиланса, у ҳолда, юқорида таъкидланганидек, i -раунд натижаси қуйидаги тенгликлар:

$$\begin{cases} L_i = R_{i-1}, \\ R_i = L_{i-1} \oplus F(R_{i-1}, K_i), \quad i = 1,2,...,16; \end{cases}$$

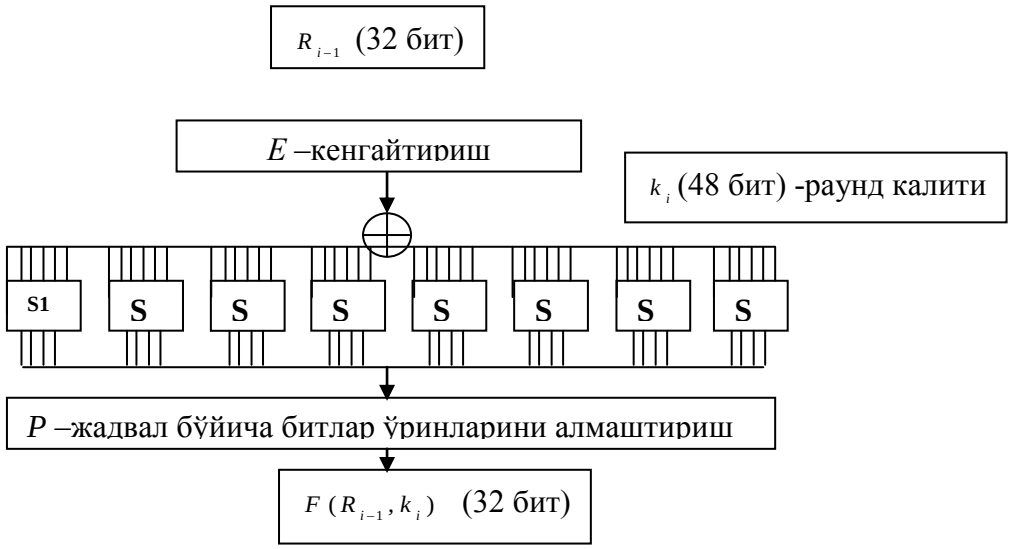
билан топилади. Бу ерда, $F(R_{i-1}, K_i)$ - 32 битли R_{i-1} ва 56 битли дастлабки калитни акслантириш натижасида олинган 48 битли K_i векторларнинг Фейтель тармоғи асосий акслантиришларининг функциясини ифодалайди. Охирги итерация-раунд натижаси $T_{16} = R_{16}L_{16}$ - блок бўлиб, бу блок битлари устида *IP* –жадвал бўйича IP^{-1} –тескари ўрин алмаштириш акслантириши бажарилади: T_{16} -блокнинг 1-бити 58-бит ўрнига, 2-бити 50-бит ўрнига ва хоказо қолган битлар ҳам жадвалда кўрсатилган ўринларга ўтказилади.

Дешифрлашда шифрлаш жараёнида бажарилган акслантиришлар тескари тартибда бажарилади, бунда ушбу:

$$\begin{cases} R_{i-1} = L_i, \\ L_{i-1} = R_i \oplus F(L_i, K_i), \quad i = 16,15,...,1; \end{cases}$$

муносабатлардан фойдаланилиб, ҳар бири 32 битли бўлган L_{16} ва R_{16} шифрмаълумот блокларини кетма-кет акслантириш, L_0 ва R_0 блоклар олиш, 64 битли $L_0 R_0$ блок устида IP^{-1} - акслантиришни бажариш орқали, T -очиқ маълумот блоки олинади.

DES алгоритми Фейстел тармоғи асосий акслантиришларининг $F(R_{i-1}, K_i)$ -функциясини ҳисоблаш схемаси қўйидагича:



$E(R_{i-1})$ -кенгайтириш функцияси R_{i-1} - 32 битли блокнинг 1, 4, 5, 8, 9, 12, 13, 16, 17, 20, 21, 24, 25, 28, 29 ва 32 – битларини икки мартадан такрорлаш, ҳамда, қуйидаги жадвал:

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

бўйича жойлаштириш натижасида ҳосил бўлган 48 битли $E(R_{i-1})$ -блокнинг ҳар бир битини K_i - 48 битли раунд калитининг мос битларига $\oplus$ - XOR

(mod2 бўйича) амали билан қўшилиб, натижа саккизта олти битлик $B_1,\ldots, B_8$, блоклар кўринишида ифодаланади: $E(R_{i-1}) \oplus k_i = B_1\ B_2 \ldots B_8$.

Сўнгра ҳар бир B_j - олти битлик блок S – блокнинг мос жадвалли S_j - блоки орқали акслантирилиб, тўрт битли блок билан алмаштирилади. S_j - блоклар ўлчами 4×16 бўлган саккизта ўзгармас жадвалдан иборат:

(S_1)

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

(S_2)

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

(S_3)

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

(S_4)

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

(S_5)

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

(S_6)

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

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

(S_7)

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

(S_8)

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

Ҳар бир $B_j = b_1(j)b_2(j)\ldots b_7(j)b_8(j)$, j=1,…,8; блоклар мос S_j -блокнинг $b_1(j)b_8(j)$-битлар билан аниқланувчи сатри ва $b_2(j)\ldots b_7(j)$-битлар билан аниқланувчи устунларининг кесишувида жойлашган соннинг иккилик саноқ тизимида ифодаланувчи $z_1(j)z_2(j)z_3(j)z_4(j)$ -тўрт битлик ифодаси билан алмаштирилади. Ҳосил бўлган 32 - битлик $z_1(1)z_2(1)z_3(1)z_4(1)\ldots z_1(8)z_2(8)z_3(8)z_4(8)$ -блок битлари ўринлари алгоритмда берилган *P* - жадвал асосида алмаштирилади, унинг кўриниши қуйидагича:

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

P –жадвал

Дастлабки 56 битли блок 7 битли қисмблокларга ажратилиб, 8, 16, …, 64 позицияларга, ҳар бир байтдаги бирлар сони тоқ бўладиган қилиб битлар қўшилади. Бу битлар шифрлаш жараёнида ишлатилмайди, улар калитларни

узатиш ва сақлашда хатоликларга йўл қўймасликни назорат қилиш учун ишлатилади. Шундай қилиб ҳосил қилинган 64 - битли калит блокининг 56 та битлари ўринлари алгоритмда кўрсатилган жадвал бўйича алмаштирилади. Бундай алмаштириш ифодаси қуйидаги жадвалда келтирилган.

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Бу жадвалнинг юқоридаги тўртта сатри $С_0$ ва кейинги тўртта сатри $Д_0$, деб белгиланади. Сўнгра, 56 битли $С_0$ $Д_0$ - блокдан ушбу: 9, 18, 22, 25, 35, 38, 43, 54 ўринларда турган битлар ўчирилиб, 48 битли блок ҳосил қилиниб, шу блок битлари ўринларини яна алгоритмда берилган қуйидаги:

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

жадвал асосида алмаштирилиб 1-раунднинг k_1 - калити олинади.

$С_i$ ва $Д_i$ жадваллар улардан олдинги $С_{i-1}$ ва $Д_{i-1}$ (i=1,2,…,16), жадваллардан алгоритмда кўрсатилган:

I	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Силжитиш сони	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

жадвал бўйича 1 ёки 2 битга циклик суриш, ҳамда, ҳосил бўлган 56 битли блокдан ушбу: 9, 18, 22, 25, 35, 38, 43, 54 ўринларда турган битлар ўчирилиб,

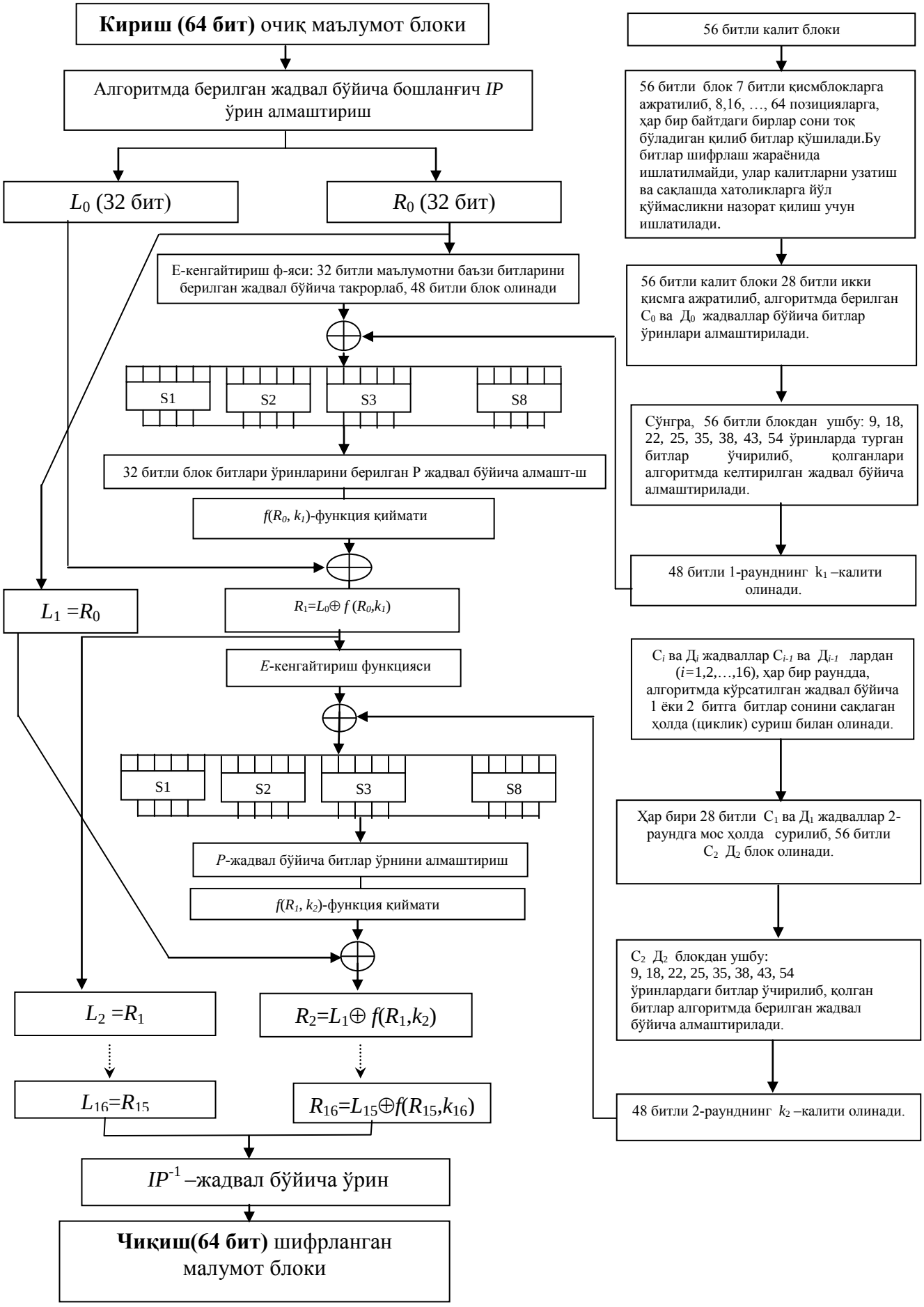
48 битли блок ҳосил қилиниб, шу блок битлари ўринлари яна алгоритмда берилган

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

жадвал асосида алмаштирилиб i -раунднинг k_i –калити ҳосил қилинади.

DES шифрлаш алгоритми АҚШда 1998 йилнинг 31 декабргача стандарт шифрлаш алгоритми деб ҳисобланган. Бу алгоритмда қўлланилган акслантиришлар криптографик нуқтаи назардан бардошли, аммо дастлабки 56 - битли калитнинг узунлиги, бугунги кун ҳисоблаш техника ва технологияларининг ютуқларидан фойдаланилганда, мумкин бўлган барча 2^{56} та калитларни тўла танлаб чиқиш имкониятини сезиларли қисқартиради.

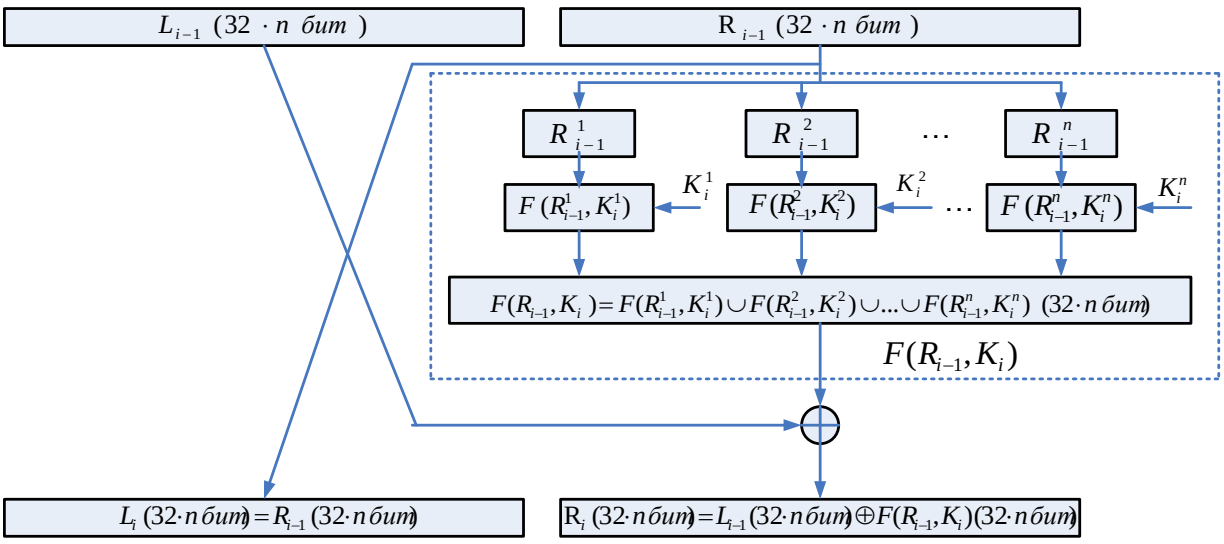
Қуйида DES шифрлаш алгоритмининг блок схемаси келтирилган.



2.4. DES шифрлаш алгоритмини такомилаштириш ва янги такомиллаштирилган DES (MDES–TDES) шифрлаш алгоритмининг функционал схемаси

Шу бўлимнинг 1- ва 2-параграфларида Фейстель тармоғининг криптографик хусусиятлари ва уни такомиллаштиришнинг умумий усули атрофлича ёритилди. 3-параграфда DES шифрлаш алгоритми акслантиришлари ўзига хосликлари батафсил кўриб чиқилди. Ушбу параграфда юқоридаги санаб ўтилган параграфлардаги натижаларни DES шифрлаш алгоритмини такомиллаштиришга тадбиқи масаласи ечими кўрилади.

DES шифрлаш алгоритмларини акслантириш асосларини сақлаб қолган ҳолда, *K*-калит узунликларини ошириш масаласи юқорида олинган илмий асосли натижаларга таяниб қуйидагича ечилади. Фейстел тармоғининг юқорида келтирилган ушбу такомиллаштирилган:



Такомиллашган Фейстел тармоғи i ***– раунди.***

умумий схемасида унинг - DES шифрлаш алгоритмининг базавий акслантиришларидан фойдаланиш кифоя, яъни:

1) Шифрланиши керак бўлган очиқ маълумот блоклари узунлиги $64m$ *бит*га тенг.
2) Калит узунлиги $|K| \cdot n$ *бит*га тенг.

3) $K_i = K_i^1 K_i^2 \ldots K_i^n - i$ -раунд қисм калитлари бирлашмаси.

4) Фейстел тармоғи R – ўнг ва L – чап қисмлари узунликлари: $|L| = |R| = 32 \cdot n$ *бит*га тенг.

5) $L_{i-1}(32 \cdot n \text{ бит}) - i$ -раунд чап қисми.

6) $R_{i-1}(32 \cdot n \text{ бит}) - i$ -раунд ўнг қисми.

7) $L_{i-1}^1(32 \text{ бит})$, $L_{i-1}^2(32 \text{ бит})$,..., $L_{i-1}^n(32 \text{ бит}) - i$ -раунд чап қисмнинг 32 *битлик;*

8) $R_{i-1}^1(32 \text{ бит})$, $R_{i-1}^2(32 \text{ бит})$,..., $R_{i-1}^n(32 \text{ бит}) - i$ -раунд ўнг қисмнинг 32 *битлик;*

9) $DES\ (R_{i-1}^1, K_i^1)$, $DES\ (R_{i-1}^2, K_i^2)$,..., $DES\ (R_{i-1}^n, K_i^n) - i$ -раунд DES алгоритми базавий акслантиришлари.

Такомиллашган DES, яъни **MDES - TDES** i – раунди математик модели қуйидагича ифодаланади:

$$\begin{cases} L_i(32 \cdot n \text{ бит}) = R_{i-1}(32 \cdot n \text{ бит}) \\ R_i(32 \cdot n \text{ бит}) = L_{i-1}(32 \cdot n \text{ бит}) \oplus DES\ (R_{i-1}, K_i)(32 \cdot n \text{ бит}) \end{cases}$$

Такомиллаштириш параметри n га боғлиқ бўлган ҳолда бир нечта $DES\ (R_{i-1}^1, K_i^1)$, $DES\ (R_{i-1}^2, K_i^2)$,..., $DES\ (R_{i-1}^n, K_i^n)$ акслантиришларидан фойдаланилади. Бу эса n га боғлиқ ҳолда бир неча Фейстел тармоғига асосланган алгоритмлар функцияларидан ёки бир неча **S**-блоклардан фойдаланиш имконини беради. Шунингдек, n га боғлиқ равишда калит узунликлари ҳам ортиб боради, яъни $n = 1$ да калит узунлиги 256 бит бўлса, $n = 2$ да калит узунлиги 512 ва ҳаказо бўлади. Калит узунлиги ва такомиллаштириш параметри n орасида қуйидагича боғлиқлик ўрнатиш мумкин:

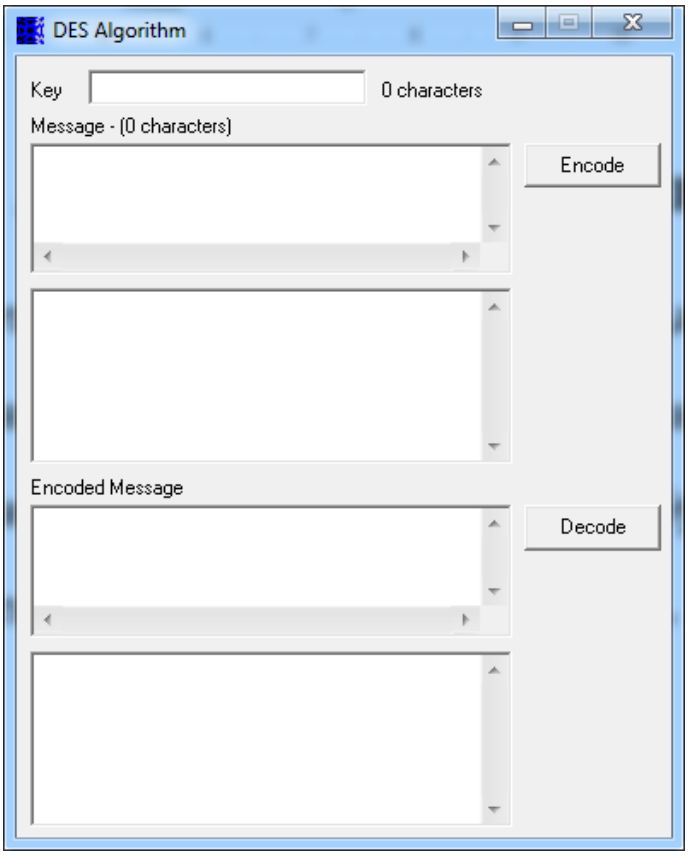
$$l_1 = l \cdot n$$

бу ерда l – асосий калити узунлиги, l_1 – такомиллашган калити узунлиги.

Такомиллашган **MDES - TDES** ва **DES** асосий алгоритмларнинг шифрлаш ва дешифрлаш тезлиги тенг, чунки $n = 1$ да алгоритм блок узунлиги 64 га тенг бўлиб, алгоритм тезлиги 20 тактдан иборат бўлса, $n = 2$ да такомиллашган алгоритм блок узунлиги 128 бит бўлиб, тезлиги 40 тактдан иборат бўлади.

2.5. DES шифрлаш алгоритмини дастурий таъминотини яратиш

DES стандарт шифрлаш алгоритмининг дастурий таъминотни Delphi дастурлаш тилининг имкониятларидан фойдаланилган ҳолда яратилди. Бу дастурнинг кўриниши қуйидаги кўринишда бўлиб, унда маълумотларни шифрлаш имкониятини кенг равишда кўрсатилган.



Юқорида кўрсатилган дастурнинг асосий ойнаси бўлиб, унда асосан Delphi дастурлаш тилининг компоненталари TLabel, TEdit, TMemo ва TButton лардан кенг фойдаланилган. DES стандарт шифрлаш алгоритми асосан шифрланаётган маълумотлардаги битларнинг устида амал бажаради. Дастур DES стандарт шифрлаш алгоритмининг асоси бўлган битларни ҳам фойдаланувчи кўзи билан кўриш имкониятини яратиб беради. Дастурни тузишни кўриб чиқамиз.

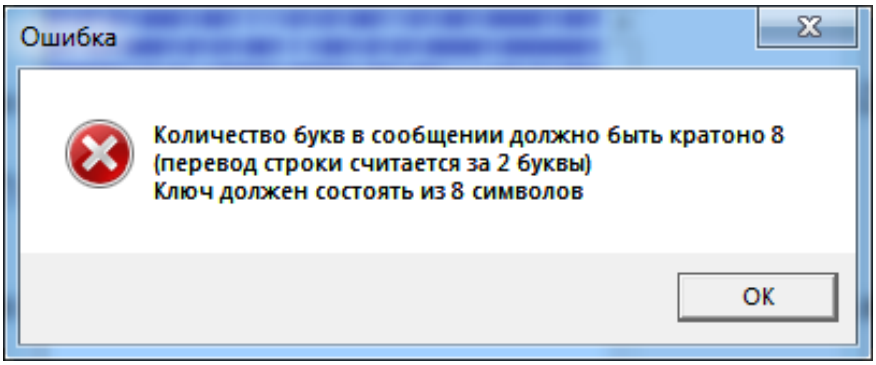
Биринчи навбатда, дастурнинг асосий формасига Delphi компоненталарини юқоридаги ойнадаги каби жойлаштириб чиқамиз. Бу

формада 4 та TLabel компонентаси, 1 та TEdit компонентаси, 4 та TMemo компонентаси ва 2 та TButton компоненталарин жойлаштирамиз. 4 та TLabel компонентаслар изоҳлар ва маълумотларни тахлиллаш учун керак бўлади. 1 та TEdit компонентаси калит вазифасини бажарувчи сўзни киритиш учун хизмат қилади. 4 та TMemo компонентасининг 2 таси маълумотларни киритиш ва шифрланган маълумотни кўрсатиш учун хизмат қилади, 2 таси маълумотларни битлардаги кўринишини кўрсатиб беради. 2 та TButton типига тегишли компонентаслар маълумотни шифрлаш ва шифрланган маълумотни очиш учун хизмат қилади. Калит сифатида фойдаланаётган сўзнинг узунлиги 8 сонига каррали бўлиши керак. Шифрланаётган маълумотнинг узунлиги ҳам калит сўзи каби 8 сонига каррали бўлиши лозим. Агар калит сўзни ёки шифрланаётган маъулумот 8 сонига каррали бўлмаса дастур фойдаланувчини огоҳлантиради. Масалан, қуйидаги сўзни шифрлаб кўрамиз:

Калит сўзи: TATUFF

Шифрланаётган маълумот: TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

Калитнинг узунлиги 6 та белгидан иборат. Шифрланаётган маълумотнинг узунлиги эса 45 та белгидан иборат. Бу маълумотлар шифрлаш алгоритми шартига мос келмайди. Дастур фойдаланувчини огохлантиради. Огоҳлантириш қуйидаги берилган.



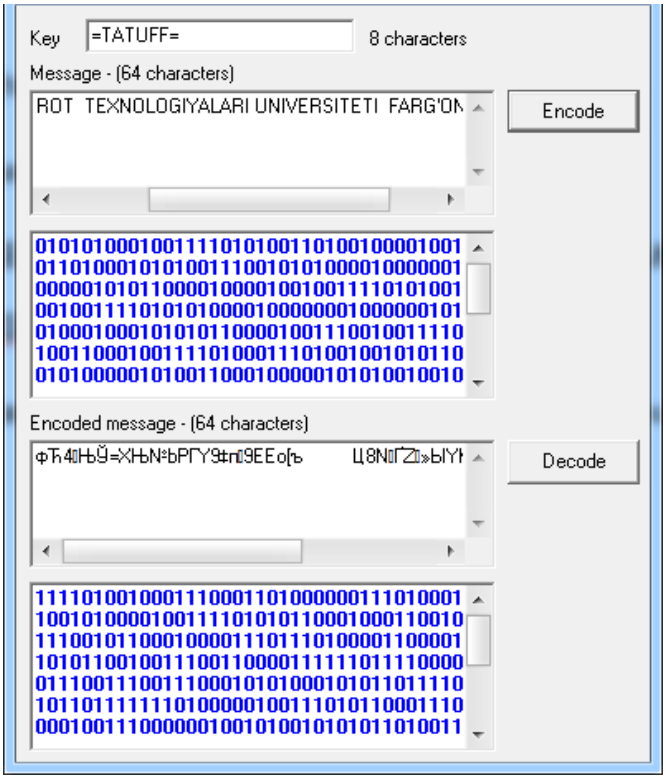
Энди юқорида берилган калит ва маълумотни қуйидаги кўринишда шифрлаймиз.

Калит сўзи: =TATUFF=

Шифрланаётган маълумот:

TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI FARG’ONA FILIALI

Дастурнинг ойнаси қуйидаги берилган ойнада кўрсатилган.



Калитни киритишимиз керак бўладиган майдонда бирон бир ўзгариш бўладиган бўлса, калитнинг узунлигини санаб бизга бу сонни қайтариб туриш учун TEdit компонентасининг OnChange ходисасига қуйидаги кодни ёзишимиз керак бўлади.

```
procedure TForm1.Edit1Change(Sender: TObject);
begin
        Label4.Caption:=IntToStr(Length(Edit1.Text))+' characters';
end;
```

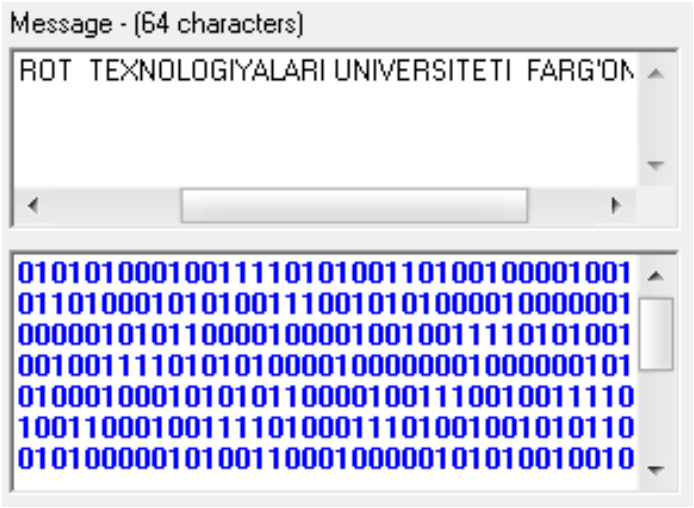
Бу код қуйида кўрсатилган ойнанинг қисми учун фойдаланилган.

Киритилаётган маълумотни узунлигини санаш ва ҳар бир белгини махсус кодини кўрсатиб бериш учун қуйидаги код ёзилади.

```
procedure TForm1.Memo1Change(Sender: TObject);
begin
        IF Memo1.Text<>'' Then
```

```
            Memo3.Text:=BinToStr(AnsiStrToBin(Memo1.Text))
        Else
            Memo3.Clear;
        Label2.Caption := 'Message - (' + IntToStr(Length(Memo1.Text)) +
' characters)' ;
end;
```

Бу коддан дастурнинг қуйидаги қисми учун фойдаланамиз.



Энди маълумотларни шифрлашга буйруқ берадиган код билан танишамиз.

```
procedure TForm1.Button1Click(Sender: TObject);
Var
        I:Integer;
        S:String;
begin
        IF ((Length(Memo1.Text)mod 8 <> 0) OR (Length(Edit1.Text)mod 8 <> 0))
Then
        Begin
            MessageBox(Handle,
 'Количество букв в сообщении должно быть кратоно 8 (перевод строки
считается за 2 буквы)'+
 #10#13'Ключ должен состоять из 8 символов',
 Nil,MB_ICONSTOP);
             Exit;
        End;
        SetLength(Data,0);
        I:=1;
        While I<=Length(Memo1.Text) Do
        Begin
            S:=Copy(Memo1.Text,I,8);
            Data:=ConcatBits([Data,DESEncode(S,Edit1.Text)]);
            I:=I+8;
```

```
        End;
        Memo2.Text:=BinToAnsiStr(Data);
end;
```

Бу кодда Delphi дастурлаш тилининг стандарт бўлмаган функцияларидан фойдаланилган. Бу функциялар DES стандарт шифрлаш алгоритмининг функциялари ҳисобланади. DES шифрлаш алгоритми биламизки ўзгармас массивлардан иборат. Бу массивларни ва шифрлаш функцияларини алоҳида файлларда сақланади. Массивлар қуйидагича эълон қилинади.

```
        DES_PC1:Array[0..55] Of Byte = (57,49,41,33,25,17,9,
                                       1,58,50,42,34,26,18,
                                       10,2,59,51,43,35,27,
                                       19,11,3,60,52,44,36,
                                       63,55,47,39,31,23,15,
                                       7,62,54,46,38,30,22,
                                       14,6,61,53,45,37,29,
                                       21,13,5,28,20,12,4);
        DES_PC2:Array[0..47] Of Byte = (14,17,11,24,1,5,
                                       3,28,15,6,21,10,
                                       23,19,12,4,26,8,
                                       16,7,27,20,13,2,
                                       41,52,31,37,47,55,
                                       30,40,51,45,33,48,
                                       44,49,39,56,34,53,
                                       46,42,50,36,29,32);
        DES_IP:Array[0..63] Of Byte = (58,50,42,34,26,18,10,2,
                                      60,52,44,36,28,20,12,4,
                                      62,54,46,38,30,22,14,6,
                                      64,56,48,40,32,24,16,8,
                                      57,49,41,33,25,17,9,1,
                                      59,51,43,35,27,19,11,3,
                                      61,53,45,37,29,21,13,5,
                                      63,55,47,39,31,23,15,7);
        DES_E:Array[0..47] Of Byte = (32,1,2,3,4,5,
                                     4,5,6,7,8,9,
                                     8,9,10,11,12,13,
                                     12,13,14,15,16,17,
                                     16,17,18,19,20,21,
                                     20,21,22,23,24,25,
                                     24,25,26,27,28,29,
                                     28,29,30,31,32,1);
        S_BOXES:Array[0..7,0..3,0..15]Of Byte = (
```

```
((14,04,13,01,02,15,11,08,03,10,06,12,05,09,00,07),
  (00,15,07,04,14,02,13,01,10,06,12,11,09,05,03,08),
  (04,01,14,08,13,06,02,11,15,12,09,07,03,10,05,00),
  (15,12,08,02,04,09,01,07,05,11,03,14,10,00,06,13)),
((15,01,08,14,06,11,03,04,09,07,02,13,12,00,05,10),
        (03,13,04,07,15,02,08,14,12,00,01,10,06,09,11,05),
        (00,14,07,11,10,04,13,01,05,08,12,06,09,03,02,15),
        (13,08,10,01,03,15,04,02,11,06,07,12,00,05,14,09)),
((10,00,09,14,06,03,15,05,01,13,12,07,11,04,02,08),
        (13,07,00,09,03,04,06,10,02,08,05,14,12,11,15,01),
        (13,06,04,09,08,15,03,00,11,01,02,12,05,10,14,07),
        (01,10,13,00,06,09,08,07,04,15,14,03,11,05,02,12)),
((07,13,14,03,00,06,09,10,01,02,08,05,11,12,04,15),
        (13,08,11,05,06,15,00,03,04,07,02,12,01,10,14,09),
        (10,06,09,00,12,11,07,13,15,01,03,14,05,02,08,04),
        (13,15,00,06,10,01,13,08,09,04,05,11,12,07,02,14)),
((02,12,04,01,07,10,11,06,08,05,03,15,13,00,14,09),
        (14,11,02,12,04,07,13,01,05,00,15,10,03,08,09,06),
        (04,02,01,11,10,13,07,08,15,09,12,05,06,03,00,14),
        (11,08,12,07,01,14,02,13,06,15,00,09,10,04,05,03)),
((12,01,10,15,09,02,06,08,00,13,03,04,14,07,05,11),
        (10,15,04,02,07,12,09,05,06,01,13,14,00,11,03,08),
        (09,14,15,05,02,08,12,03,07,00,04,10,01,13,11,06),
        (04,03,02,12,09,05,15,10,11,14,01,04,06,00,08,13)),
((04,11,02,14,15,00,08,13,03,12,09,07,05,10,06,01),
        (13,00,11,07,04,09,01,10,14,03,05,12,02,15,08,06),
        (01,04,11,13,12,03,07,14,10,15,06,08,00,05,09,02),
        (06,11,13,08,01,04,10,07,09,05,00,15,14,02,03,12)),
((13,02,08,04,06,15,11,01,10,09,03,14,05,00,12,07),
        (01,15,13,08,10,03,07,04,12,05,06,11,00,14,09,02),
        (07,11,04,01,09,12,14,02,00,06,10,13,15,03,05,08),
        (02,01,14,07,04,10,08,13,15,12,09,00,03,05,06,11))
);
DES_P:Array[0..31] Of Byte = (16,7,20,21,
                        29,12,28,17,
                        1,15,23,26,
                        5,18,31,10,
                        2,8,24,14,
                        32,27,3,9,
                        19,13,30,6,
                        22,11,4,25);
DES_REVERSE_IP:Array[0..63] Of Byte = (40,8,48,16,56,24,64,32,
        39,7,47,15,55,23,63,31,
        38,6,46,14,54,22,62,30,
        37,5,45,13,53,21,61,29,
```

```
            36,4,44,12,52,20,60,28,
            35,3,43,11,51,19,59,27,
            34,2,42,10,50,18,58,26,
            33,1,41,9,49,17,57,25);
    DES_LSH:Array[0..15] Of Byte = (1,1,2,2,2,2,2,2,1,2,2,2,2,2,2,1);
```

Бу массивлардан фойдаланган ҳолда шифрлашлар амалга оширилади.

2 - боб бўйича хулоса

1. Фейстель тармоқли симметрик блоклаб шифрлаш алгоритмларининг криптографик хусусиятлари таҳлил қилинди.

2. Фейстель тармоғини ва унга асосланган алгоритмларни такомиллаштиришнинг универсал усули ёритилди.

3. DES стандарт шифрлаш алгоритми акслантиришларининг криптографик хусусиятлари таҳлил этилди.

4. DES шифрлаш алгоритмини такомилаштириш ва янги такомиллаштирилган DES (MDES–TDES) шифрлаш алгоритмининг функционал схемаси келтирилди

3-БОБ. ЯНГИ ТАКОМИЛЛАШТИРИЛГАН MDES - TDES ШИФРЛАШ АЛГОРИТМИНИНГ КРИПТОГРАФИК ТАСНИФИ ВА УНИНГ КРИПТОБАРДОШЛИГИНИ БАҲОЛАШ

3.1. Такомиллаштирилган MDES - TDES шифрлаш алгоритми акслантиришларининг криптобардошлик хусусиятлари кўрсаткичлари

Бардошли криптоалгоритмлар асосидаги акслантиришлар ечилиши мураккаб бўлган математик масалалар билан боғлиқ бўлмайди. Фейстель тармоқли ва узликсиз шифрлаш ҳамда хеш-функция алгоритмлари ааксланти ришларида биртомонламалик, самарали аралаштириш ва тарқатиш хусусиятлари чуқур таҳлил қилинмаган бўлсада, бу акслантиришлар дастлабки калитдан хосил этилган оралиқ калитлар билан итератив ҳолда бир неча марта қўлланилиши криптобардошлилик самарадорлигини тезкор ва қулай амалга оширишни таъминлайди.

Бу туркумдаги криптоалгоритмлар криптобардошлигини таъминловчи етарлилик шарти критерийларини бирортаси унинг акслантиришлари учун бажарилмаслиги ёки қисман бажарилмаслиги криптохужум учун замин яратади [139] .

Фестел тармоқли симметрик блоклаб шифрлаш алгоритмлари акслантиришлари учун:

1) *Алгоритмнинг очиқ (маълум) бўлмаслиги, ундан фойдаланувчиларда криптобардошлигига шубҳа туғдиради, бу эса унинг кенг миқиёсда қўлланилишини чеклайди. Алгоритм шифрлаш калити узунлигининг 128 битдан кам бўлиши бугунги кун фан - техника ва технологиялари ютуқларидан фойдаланган ҳолда мумкин бўлган барча калитларни танлаб чиқиш криптохужум турини самарали амалга оширишга қулайлик туғдиради. Чунки бундай тур алгоритмлар содда ва тез ҳисоблашларни амалга оширувчи акслантиришлардан иборат.*

2) *Акслантирилувчи блок узунлиги қиймати иккининг даражалари кўринишида бўлмаслиги, яъни* 2^t, $t = 6,7,\ldots < \infty$ *бўлмаслиги, криптабардошликни ошириш учун зарурият туғилганда унинг аппарат қурилмаларини яратилишига қулайлик туғдирадиган ва тез ишлашини таъминлайдиган базавий акслантиришларини тузилишини сақлаб қолган ҳолда калит узунлигини ошириб самарали модификациялаш имкониятини бермайди;*

3) *Асосий акслантиришларининг самарали аралаштириш ва тарқатиш хусусиятига эга эмаслиги алгоритм акслантиришларининг чизиқли ва дифференциал криптотаҳлил усулларига бардошли бўлмаслигига олиб келади;*

4) *Базавий акслантиришлари чизиқсизлик, мувозанатлашганлик, регулярлик, қатъий кескин ўзгариш самарадорлик, корреляцияга мосланувчанлик каби хоссаларга эга бўлмаса, чизиқли, дифференциал ва бошқа криптохужум усулларини қўллаб шифрлаш калитини топиш эҳтимоллиги ортади;*

5) *Базавий акслантиришларининг биртомонламалик хусусиятига эга бўлмаслигиалгоритм акслантиришларига тескари акслантиришлардан фойдаланиб амалга оширилиши мумкин бўлган криптоҳужумларга кенг шароит яратади.*

Таклиф этилган такомиллаштирилган янги **MDES - TDES** шифрлаш алгоритми санаб ўтилган криптохужум турларига бардошлидир.

Такомиллашган **MDES - TDES** шифрлаш алгоритми афзалликлари:

1) Такомиллаштириш параметри n га боғлиқ ҳолда шифрлаш алгоритми хоссалари ва бардошлилигини сақлаб қолган ҳолда алгоритм калити узунлигини ошириб бориш имконияти мавжуд. Бу эса, ўз навбатида, ҳисоблаш техникаси қурилмаларининг такомиллашуви натижасида алгоритм калити узунлиги тўлиқ танлаш усулига бардошсиз бўлиб қолишининг олдини олади.

2) Алгоритм тезлиги такомиллаштириш параметрига боғлиқ эмас, яъни такомиллашган **MDES - TDES** ва **DES** асосий алгоритм тезликлари тенг. Бу хосса ўз навбатида алгоритм тезлигини сақлаб қолган ҳолда такомиллаштириш имкониятини беради.

Бардошли криптоалгоритмлар туркумидаги шифрларни дешифрлашнинг моделлари ва уларни автоматлаштириш.

Бардошли криптоалгоритмлар туркумига: симметрик блоклаб шифрлаш, узлуксиз шифрлаш ва хэш-функция алгоритмлари киради.

Симметрик блоклаб шифрлаш алгоритмлари: Фейстель тармоқли ва унга асосланмаган асосий (базавий) акслантиришларни очиқ маълумот блоки ҳамда раунд калитлари устида бир неча марта такрорлашдан-интерациялашдан иборат бўлган моделларни ўз ичига олади.

Симметрик блоклаб шифрлаш алгоритмлари шифрларини дешифрлаш жараёнини автоматлаштиришда калитларни танлаш ва очиқ матн статистик хусусиятларидан фойдаланиш усулини қўллаш.

Бунинг учун:

1. $C=c_1c_2\ldots c_м$ – шифрмаълумотнинг дешифрланиши керак бўлган блоки киритилади.

2. $К_j=k^j_1\ k^j_2\ldots k^j_м$ – танлаб олинган калит, j - қадамда.

3. $D_k(C)=T_j$ – шифрматнга тегишли алгоритм бўйича дешифрлашни амалга ошириш натижасида олинган мумкин бўлган очиқ матнлар.

4. T_j – мумкин бўлган очиқ матнни k – граммаларини маълумотлар базасидаги k – граммалар билан солиштириш ва шартли энтропия усулларидан фойдаланиб топилади.

5. Агар мумкин бўлган очиқ матн (МБОМ) T_j ларда бирортаси T^0_j учун, унинг k – граммаларини маълумотлар базаси (МБ) мос k – граммаларидан фарқини ифодаловчи

$P(T^0_j)$=P(МБОМ k-граммалари МБ мос k-граммалари) эҳтимоллик қиймати бирга тенг ёки бирга етарли яқин бўлса, яна бошқача ифодалаганда бунга эквивалент бўлган ушбу эҳтимоллик

$P(T^0_j)$=P(МБОМ k-граммалари МБ мос k-граммалари) қиймати ноль ёки нолга етарли яқин бўлса, уни очиқ матн деб эълон қилиш мумкин ва жараён тўхтатилади. Агар бу шартлар бажарилмаса, кейинги қадамга ўтилади.

6. Бу жараён барча калитларни ёки калитларни бир қисмини танлаб чиқилгандан сўнг ҳосил қилинган МБОМ тўпламидан ёки эҳтимоллик қийматларини қаноатлантирувчи T^0_j – мумкин бўлган очиқ матнни танлаш билан якунланади.

Симметрик блоклаб шифрлаш алгоритмлари шифрларини дешифрлашни автоматлаштиришда калитларни танлаш ва матнларни тўқнашуви усулларини биргаликда қўллаш.

Симметрик блоклаб шифрлаш алгоритмларида (СБША) да шифрлаш ва дешифрлаш учун битта калитдан фойдаланилиб, фақат раунд калитлари кетма-кетлиги тескарисига қўлланилиши таъкидланган эди:

1. Шифрлаш модели умумий ифодаси СБША $(T, K_1, K_2, ..., K_n)=C$;

2. Дешифрлаш модели умумий ифодаси СБШАД $(C, K_n, K_{n-1},..., K_1)=T$; бу ерда T - шифрланадиган маълумот, C - шифрмаълумот, K_1 - раунд калитлари, n - раундлар сони.

Бунда:

1. $C_0=c^0_1c^0_2\ldots c^0_м$ - дастлабки шифрмаълумот киритилади.

2. $K_0=k^0_1k^0_2\ldots k^0_м$ - танлаб олинган дастлабки калит.

3. СБШАД $(C_0,K^0_n,K^0_{n-1},\ldots,K^0_1)=D_k(C_0)=T_0$ – шифрматнга тегишли алгоритм бўйича дешифрлашни амалга ошириш натижасида олинган мумкин бўлган очиқ матн. Криптоаналитик томонидан T_0 – мумкин бўлган очиқ матн бевосита кўзда кечирилиб ёки юқорида келтирилган статистик усул билан, унинг очиқ матн ёки очиқ матн эмаслиги текширилади. Агар T_0 – очиқ матн бўлса жараён тўхтатилиб $K_0=k^0_1k^0_2\ldots k^0_м$ – изланаётган калит деб қабул қилинади. Акс ҳолда кейинги қадамга ўтилади.

4.$K_1=k^1_1k^1_2\ldots k^1_м$ - янги калит танлаб олинади.

5. СБША $(T_0,K^1_1,K^1_2,\ldots K^1_n)=E_{k1}(T_0)=C_1$ – шифр матн ҳосил қилинади.

6. Агар $C_1=C_0$ бўлса, T_0 - изланаётган очиқ матн, K_1 - изланаётган калит деб қабул қилинади ва жараён тўхтатилади. Акс ҳолда кейинги қадамга ўтилади.

7. Навбатдаги янги $K_2=k^2_1k^2_2\ldots k^2_м$ – калит танланиб, $K_1=K_2$ ва $T_0=C_1$ деб 5 - қадамга ўтилади. Жараён калитларнинг барчаси ёки бир қисмини кўриб чиқилгандан сўнг тўхтатилади.

Симметрик блоклаб шифрлаш алгоритмлари шифрларини дешифрлашни автоматлаштиришда калитларни танлаш ва дифференциялларни (фарқларни) таҳлил қилиш усулларини комбинациялаш.

Бу усулни бундан олдинги усулнинг давоми деб ҳам қараш мумкин.

Бунда:

1. $C_0=c^0_1c^0_2\ldots c^0_м$ - дастлабки шифрмаълумот киритилади.

2. $K_0=k^0_1k^0_2\ldots k^0_м$ - танлаб олинган дастлабки калит.

3. СБШАД $(C_0, K^0_n, K^0_{n-1},\ldots, K^0_1)=D_{k0}(C_0)=T_0$ – шифрматнга тегишли алгоритм бўйича дешифрлашни амалга ошириш натижасида олинган мумкин бўлган очиқ матн ҳосил қилинади. Криптоаналитик томонидан T_0 – мумкин бўлган очиқ матн бевосита кўздан кечирилиб ёки юқорида келтирилган статистик усул билан, унинг очиқ матн ёки очиқ матн эмаслиги текширилади. Агар T_0 – очиқ матн бўлса жараён тўхтатилиб $K_0=k^0_1k^0_2\ldots k^0_м$ – изланаётган калит деб қабул қилинади. Акс ҳолда кейинги қадамга ўтилади.

4. $K_1=k^1_1k^1_2\ldots k^1_м$ - янги калит танлаб олинади.

5. СБША $(T_0,K^1_1,K^1_2,\ldots,K^1_n)=E_{k1}(T_0)=C_1$ – шифрматн ҳосил қилинади.

Кейинги қадамлар бошқа бардошлик туркуми алгоритмларига қўлланилган шу усулнинг қадамлари каби айнан давом эттирилади.

6. C_1, C_2 блоклар фарқи ҳисобланади:

T_1 фарқлаш амали $C_0=F$ - фарқ

Матнларнинг иккилик саноқ системаси-битлар ифодаси блоклари устида амаллар бажарилаётган бўлса, фарқлаш амали сифатида XOR-иккилик саноқ системасида қўшиш амалидан фойдаланиш мумкин.

Матнлар ўзига хос алфавит белгиларидан иборат бўлса, улар блокларидаги белгиларнинг мос ўриндагиларини бир хил эмаслиги билан фарқланиши мумкин. Фарқи ҳисобланаётган блокларда мос ўриндаги белгиларнинг қанчалик кўп қисми бир хил бўлса, фарқ шунчалик кам, қанчалик кўп қисми бир хил бўлмаса, фарқ шунчалик катта қийматга эга бўлади.

7. Шундай қилиб, агар F=0 бўлса, $C_1=C_2$ бўлиб T_0 - очиқ матн деб эълон қилинади ва жараён тўхтатилади. Акс ҳолда кейинги қадамга ўтилади.

8. Навбатдаги янги $K_2=k^2_1k^2_2\ldots k^2_м$ – калит танланиб, $K_1=K_2$ ва $T_0=T_1$ деб, 5 - қадамга ўтилади. Жараён калитлар барчасини ёки бир қисмини кўриб чиқилгандан сўнг тўхтатилади:

8.1. Фарқни ифодаловчи эҳтимоллик

P(F)=P(T_1 фарқлаш амали C_0=F)= мос ўриндаги бир-хил белгилар сони/солиштирилаётган блок барча белгилари сони қиймати бирга тенг ёки бирга етарли яқин бўлса, яна бошқача ифодалаганда бунга эквивалент бўлган ушбу эҳтимоллик

P(F)=P(T_1 фарқлаш амали C_0=F)= мос ўриндаги бир-хил белгилар сони/солиштирилаётган блок барча белгилари сони қиймати ноль ёки нолга етарли яқин бўлса, T_1 - очиқ матн деб эълон қилиш мумкин ва жараён тўхтатилади. Агар бу шартлар бажарилмаса, кейинги қадамга ўтилади.

8.2. Бу жараён барча калитларни ёки калитларнинг бир қисмини танлаб чиқилгандан сўнг ҳосил қилинган (F_1) – фарқлар тўпламидан

max_F P(F_j)=max_F (хар хил T_1 ва C_0 блоклар мос ўриндаги бир хил белгилари сони)/(солиштирилаётган блок барча белгилари сони)=P(F_0) ёки min_F P(F_j)=min_F (хар хил T_1 ва C_0 блоклар мос ўриндаги бир хил бўлмаган белгилари сони)/(солиштирилаётган блок барча белгилари сони)=P(F_0) эҳтимоллик қийматларини қаноатлантирувчи F_0 – фарқ билан аниқланувчи мос T_1 – мумкин бўлган очиқ матнни танлаш билан якунланади.

3.2. Ахборот муҳофазасини таъминлашда MDES - TDES шифрлаш алгоритмининг криптографик масалаларни ечишдаги моҳияти ва қўлланиш самарадорлиги

Таклиф этилган такомиллаштирилган янги **MDES - TDES** шифрлаш алгоритми бардошли шифрлаш алгоритми туркумига тегишли бўлиб, шу туркум алгоритмлари билан ечиладиган қуйидаги криптографик масалаларни ечишда қўлланилади:

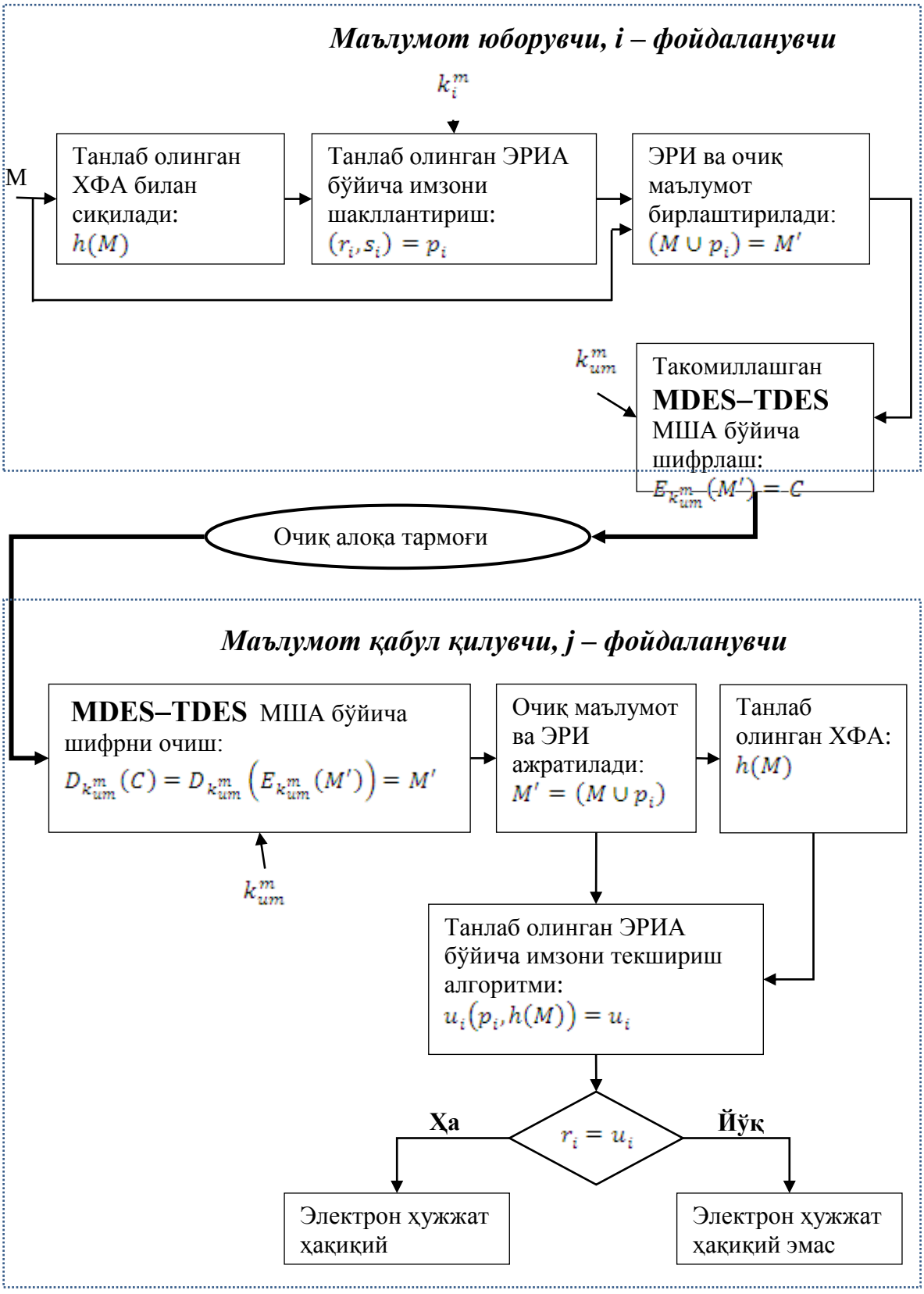
1) Ахборот-коммуникация тармоқларида алмашинадиган маълумотларнинг маҳфийлигини таъминлашда;

2) Хэш-функция алгоритми билан биргаликда электрон хужжат алмашинувида унинг бутунлигини (ўзгартирилмаганлигини) ва маҳфийлигини таъминлайди;

3) ЭРИ алгоритми билан биргаликда электрон хужжат алмашинувида унинг манбаасини, авторини (аутинтификациясини) аниқлашда, авторликдан бош тортмасликни ва маҳфийлигини таъминлайди;

4) Хэш-функция ва ЭРИ алгоритмлари билан биргаликда муҳофазаланган электрон хужжат алмашинувини таъминлайди.

Бу келтирилганларни **MDES - TDES** алгоритмини қўллаган ҳолда амалга оширишнинг функцияси қуйидагича бўлади:


Маълумот юборувчи, i – фойдаланувчи
k_i^m
M
Танлаб олинган ХФА билан сиқилади:
$h(M)$
Танлаб олинган ЭРИА бўйича имзони шакллантириш:
$(r_i, s_i) = p_i$
ЭРИ ва очиқ маълумот бирлаштирилади:
$(M \cup p_i) = M'$
k_{um}^m
Такомиллашган **MDES–TDES** МША бўйича шифрлаш:
$E_{k_{um}^m}(M') = C$
Очиқ алоқа тармоғи
Маълумот қабул қилувчи, j – фойдаланувчи
MDES–TDES МША бўйича шифрни очиш:
$D_{k_{um}^m}(C) = D_{k_{um}^m}\left(E_{k_{um}^m}(M')\right) = M'$
k_{um}^m
Очиқ маълумот ва ЭРИ ажратилади:
$M' = (M \cup p_i)$
Танлаб олинган ХФА:
$h(M)$
Танлаб олинган ЭРИА бўйича имзони текшириш алгоритми:
$u_i(p_i, h(M)) = u_i$
$r_i = u_i$
Ҳа
Йўқ
Электрон ҳужжат ҳақиқий
Электрон ҳужжат ҳақиқий эмас

Симметрик блоклаб шифрлаш алгоритмлари шифрларини дешифрлашни автоматлаштиришда калитларни танлаш ва чизиқли криптотаҳлил усулларини комбинациялаш.

Чизиқли криптотаҳлил усулини қўллашда асосан дешифрлаш калитининг ташкил этувчи элементларини: битлари, байтлари, битлар ва байтлар бирикмалари, биграмма, k-граммалари кетма-кет тикланади. Бунинг фиксирланган C_0 – шифрматн блоки олиниб, фарқни ифодаловчи ушбу муносабат

T_1 фарқлаш амали $C_0=F_1$ фарқ асосида таҳлил олиб борилади.

1. Очиқ матннинг фиксирланган узунликдаги T_j – очиқ маълумот блокининг мумкин бўлган барчаси ёки етарли катта сондаги тўплами билан, танлаб олинган K_j – калитлар орқали СБША $(T_j, K^j_1, K^j_2,\ldots, K^j_n)=E_k(T_j)=C_1$ – шифрматнлар ҳосил қилинади. Сўнг айнан юқоридаги туркум алгоритмларидаги каби шифрматнлар фарқи:

C_j фарқлаш амали $C_0=F_j$ – фарқ ҳосил қилинади. Бу фарқни ифодаловчи эҳтимоллик

$P(F_j)=P(C_j$ фарқ амали $C_0=F_j)=C_j$ ва C_0 блоклар мос ўриндаги бир хил белгилар сони / солиштирилаётган блокдаги барча белгилар сони– солиштириш блоки узунлиги қиймати бирга тенг ёки бирга етарли яқин бўлса, яна бошқача ифодалаганда бунга эквивалент бўлган ушбу эҳтимоллик $P(F_1)=P(C_j$ фарқ амали $C_0=F_j)=C_j$ ва C_0 блоклар мос ўриндаги бир хил бўлмаган белгилар сони/солиштирилаётган блокдаги барча белгилар сони қиймати ноль ёки нолга етарли яқин бўлса, ана шу ноль ёки нолга яқин қиймат берувчи F_0 – фарқ билан аниқланувчи K_0 –калит ёки калитнинг бир қисми деб эълон қилиш мумкин ва жараён тўхтатилади. Агар бу шартлар бажарилмаса, кейинги қадамга ўтилади.

2. Бу жараён барча калитларни ёки калитларнинг бир қисмини танлаб чиқилгандан сўнг ҳосил қилинган (F_j) – фарқлар тўпламидан $\max_F P(F_j)=\max_F$ (хар хил C_1 ва C_0 блоклар мос ўриндаги бир хил белгилари сони)/(солиштирилаётган блок барча белгилари сони)=$P(F_0)$ ёки $\min_F$

$P(F_j)=\min_F$ (хар хил C_1 ва C_0 блоклар мос ўриндаги бир хил бўлмаган белгилари сони)/(солиштирилаётган блок барча белгилари сони)=$P(F_0)$ эҳтимоллик қийматларини қаноатлантирувчи F_0 – фарқ билан аниқланувчи мос K_0 – мумкин бўлган калит ёки калитнинг бир қисми деб қабул қилинади.

Бундай ёндошув усулини такомиллаштириш мумкин. Бунда: $T_j=t^j_1t^j_2\ldots t^j_d$, $K_j=k^j_1k^j_2\ldots k^j_d$, $C_j=c^j_1c^j_2\ldots c^j_d$, $F_j=f^j_1f^j_2\ldots f^j_d$ - блокларнинг тузувчилари бўлган t^j_i, k^j_i, c^j_i, f^j_i – элементлардан ва улар бирикмалари ўзгаришлари қонуниятларини алгоритм алгоритм акслантиришлари хусусиятларидан келиб чиққан ҳолда моделлаштириш лозим.

Раунд калитларини тиклаш.

Раунд калитларини тиклашда ҳам юқоридаги усулларнинг барчасидан фойдаланиш мумкин. Шифрланаётган блок ва раунд калити узунлигининг бутун шифрмаълумот узунлигидан кўп ҳолларда катта миқдорда қисқалиги самарали натижалар бериши эҳтимоллигини оширади.

Бунда:

1. Дешифрланиши керак бўлган С-шифрматн сифатида охирги n-раунд натижасини ифодаловчи $C_n=c^n_1c^n_2\ldots c^n_м$ – блок олинади: $C=C_n$

2. Юқоридаги усуллардан фойдаланиб $K_n=k^n_1k^n_2\ldots k^n_м$ n-раунднинг мумкин бўлган калити тикланади.

3. Бу тикланган K_n – калит билан C_n – шифрблок n-раунд акслантиришларига нисбатан тескари акслантиришни амалга оширувчи акслантиришлар асосида дешифрланади ва унинг натижаси шифрлаш жараёнининг (n-1)-раунд натижасини ифодаловчи $C_{n-1}=c^{n-1}_1c^{n-1}_2\ldots c^{n-1}_м$ – оралиқ шифрблок деб қабул қилинади.

4. $C=C_{n-1}=c^{n-1}_1c^{n-1}_2\ldots c^{n-1}_м$ деб 2-ва 3-қадамлар такрорланиб $K_{n-1}=k^{n-1}_1k^{n-1}_2\ldots k^{n-1}_м$ - (n-1)-раунднинг мумкин бўлган калити ҳамда шифрлаш жараёнининг (n-2)-раунд натижасини ифодаловчи $C_{n-2}=c^{n-2}_1c^{n-2}_2\ldots c^{n-2}_м$ – оралиқ шифрблок деб қабул қилинувчи блоклар ҳосил қилинади. Худди шу каби кетма-кет навбатдаги: K_{n-2}, K_{n-3},…,K_1 - раунд калитлар ва C_{n-3}, C_{n-4},…,C_1, T_1 – оралиқ шифрблоклар ва очиқ матн блоки T_1 ҳосил қилинади.

5. Раунд калитлари тиклангандан сўнг шифрлаш алгоритми калитини тиклашга имконият туғилади. Бу имконият самарали амалга оширилса тикланган калит билан дешифрланиши керак бўлган шифрмаълумотнинг қолган блокларини ҳам дешифрлаш мумкин бўлади.

Узлуксиз шифрлаш алгоритмлари шифрларини дешифрлаш жараёнини автоматлаштириш.

Узлуксиз шифрлаш алгоритмлари нисбатан қисқа, аммо бугунги кунда калитни ташкил этувчи белгилари сони 128 тадан кам бўлмаган, дастлабки калит билан етарли узун (ташкил этувчи белгилари сони етарли кўп) ва ҳадлари даврий бўлмаган (ташкил этувчи белгиларининг такрорланиши бирор қонуниятга асосланмаган) псевдотасодифий кетма-кетлик ишлаб чиқариш имкониятини берувчи акслантиришлар асосида яратилади. Ишлаб чиқилган кетма-кетлиги белгилари билан, мутлақо бардошли шифрлаш алгоритмларидаги каби, очиқ маълумот мос белгилари устида бирор амал бажариш орқали шифрлаш жараёни акслантиришлари амалга оширилади.

Узлуксиз шифрлаш алгоритмлари шифрларини дешифрлаш жараёнларини автоматлаштириш моделларини калитларни танлаш ва очиқ матн статистик хусусиятларидан фойдаланиш, матнларни тўқнашуви, дифференциал ва чизиқли таҳлил усулларини қўллаш билан ишлаб чиқиш мутлақо бардошли шифрлаш алгоритмлари туркумидаги каби хусусиятларга эга.

Хеш-функция алгоритмларига криптоҳужум уюштириш усуллари.

Хеш-функция алгоритмлари ихтиёрий чекли узунликдаги матн ташкил этувчи белгилари сони 256 тадан кам бўлмаган фиксирланган блокка биртомонламалик, самарали аралаштириш ва хусусиятига эга асосий (базавий) акслантириш матн блокларига такроран қўллаш билан (итерациялаш билан) амалга ошириладиган жараёндир. Калитли ва калитсиз туркумларга бўлинади. Мутахассислар томонидан тан олинган стандарт хеш-функция алгоритмлари калитсиздир. Шундай бўлиши моҳитан тўғри, чунки калитсиз бўлиши ва алгоритмнинг очиқ бўлиши фойдаланувчилар орасида

ўзаро ишончсизликка олиб келувчи ҳолатларни келтириб чиқармайди. Бундан ташқари хешланадиган матннинг энг охирги хешланувчи блоклари сифатида унга қуйидагилар бириктирилади:

1. **Тўлдириш битларини қўшиш** - агар охирги блок узунлиги 256 битдан кичик бўлса, 256 битгача ноль ёки бўшлиқ белгиси билан тўлдирилади;

2. **Маълумот узунлигини қўшиш** - тўлдириш битлари билан биргаликда битлар сони билан аниқланадиган маълумот узунлигини билдирувчи блок-тўлдирилган маълумотнинг битлар сони чекли mod 2^{256} майдонда ҳисобланиб, ҳосил бўлган қиймат 256 битлик блок кўринишида бирлаштирилади;

3. **Назорат йиғиндисини қўшиш** – 2 - босқич натижасига берилган маълумотнинг назорат йиғиндисини билдирувчи 256 битлик блок бирлаштирилади. Назорат йиғиндисини билдирувчи блок, охирги тўлиқ бўлмаган блок ноль ёки бўшлиқ белгиси билан тўлдирилгандан кейин, маълумот узунлигини ифодаловчи блок бирлаштирилгандан сўнг ҳосил бўлган кенгайтирилган матннинг барча блоклар қийматларининг ўнлик саноқ системасидаги йиғиндисини mod 2^{256} – бўйича ҳисобланиб ҳосил қилинади ва у охирги хешланадиган блок сифатида бириктирилади.

Бу бириктириладиган қўшимча блоклар хеш-функциянинг коллизияга бардошлигини оширади.

Хеш функцияларга қуйидаги криптоҳужум турлари мавжуд (1-6):

1.Хеш функция алгоритмида қатнашган акслантиришлар бўйича криптоҳужум;

2.Алгоритм акслантиришларининг дифференциал криптотаҳлил усулига бардошлилиги;

3.Матнларнинг тўқнашуви усули асосидаги криптоҳужум;

4.Барча мумкин бўлган очиқ матн вариантларни танлаш асосидаги ҳужум.

Бу криптоҳужумларни амалга ошириш симметрик блоклаб шифрлаш алгоритмларига хос хусусиятларни ҳисобга олган ҳолда амалга оширилади.

1. Шифрларни очиш жараёнларини моделлаштириш ва автоматлаштириш масалаларининг қўйилиши ва ечилишига тизимли ёндашув усуллари асослари ишлаб чиқилди. **Модель, моделлаштириш, алгоритм** тушунчаларининг моҳиятлари ва уларнинг ўзаро боғлиқлиги қисқача ифодаланади.

2. Дешифрлаш жараёнларини автоматлаштиришда биринчи навбатда ечилиши керак бўлган масалалардан бири-очиқ матнни моделлаштириш ва унга таянган ҳолда статистик қиёслаш усулларининг асослари ишлаб чиқилди.

3. Мутлақо бардошли криптоалгоритмларга тегишли шифрларни дешифрлаш жараёнларини моделлашириш ҳамда автоматлаштиришда: калитларни танлаш ва очиқ матн статистик хусусиятларидан фойдаланиш, матнларни тўқнашуви, дифференциал ва чизиқли криптотаҳлил усулларини қўллаш асослари ишлаб чиқилди.

4. Ишончли бардошли алгоритмларини дешифрлаш жараёнларини: етарли катта натурал сонни туб кўпайтувчиларга ажратиш, ҳарактеристикаси етарли катта бўлган чекли майдонда дискрет логарифмлаш, чекли майдонда аниқланган эллиптик эгри чизиқ нуқталарини қўшишнинг ҳисоблаш мураккабликлари билан боғлиқ биртомонламалик хусусиятли акслантиришларга асосланганлигини эътиборга олган ҳолда моделлаштириш ва автоматлаштириш масалалари ечимларига 3-бандда келтирилган усулларни қўллаш алгоритмлари яратилди.

5. Бардошли криптоалгоритмлар туркумига кирувчи: симметрик блоклаб шифрлаш, узлуксиз шифрлаш ва хеш-функция алгоритмларига калитларни танлаш ва очиқ матн статистик хусусиятларидан фойдаланиш, матнларни тўқнашуви, дифференциал ва чизиқли криптотаҳлил ҳужум усулларининг қўлланилишини моделлаштириш ҳамда уларни амалга оширишни автоматлаштириш алгоритмлари асослари ишлаб чиқилди.

3 - боб бўйича хулоса

1. Такомиллаштирилган MDES - TDES шифрлаш алгоритми акслантиришларининг криптобардошлик хусусиятлари кўрсаткичлари келтирилди.

2. Ахборот муҳофазасини таъминлашда MDES–TDES шифрлаш алгаритмининг криптографик масалаларни ечишдаги моҳияти ва қўлланиш самарадорлиги, ахборот-коммуникация тармоқларида ХФ ва ЭРИ алгоритмлари билан биргаликда криптографик муҳофазаланган электрон хужжат алмашинувини таъминлашда қўлланишининг функционал блок схемаси таклиф этилди.

ХУЛОСА

1. Криптографиянинг асосий масалаларининг моҳиятини ёритиш ва уларни ечиш алгоритмларининг акслантиришлари асосларининг хусусиятларига кўра ва криптохужумларга бардошлиги бўйича турлари классификацияси тахлил қилинди.

2. Фейстель тармоғининг ва DES алгоритми базавий акслантиришларининг криптографик хусусиятлари таҳлил қилинди, унинг калити узунлигини ошириш эвазига криптобардошлигини ошириш мумкинлиги асосланди.

3. Фейстель тармоғи ва акслантиришлари жадвалларга асосланган симметрик блоклаб шифрлаш алгоритми туркумига кирувчи DES стандарт шифрлаш алгоритми базавий акслантиришларини сақлаб қолган ҳолда унинг криптобардошлигини ошириш масаласи ечилди.

4. Такомиллаштирилган MDES - TDES шифрлаш алгоритми акслантиришларининг криптобардошлик хусусиятлари кўрсаткичлари келтирилди.

5. Ахборот муҳофазасини таъминлашда MDES - TDES шифрлаш алгоритмининг криптографик масалаларни ечишдаги моҳияти ва қўлланиш самарадорлиги, ахборот-коммуникация тармоқларида ХФ ва ЭРИ алгоритмлари билан биргаликда криптографик муҳофазаланган электрон хужжат алмашинувини таъминлашда қўлланишининг функционал блок схемаси таклиф этилди.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙХАТИ

1. Акбаров Д. Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши – Тошкент, «Ўзбекистон маркаси», 2009 – 434 бет.

2. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии: Учебное пособие, 2-е изд. –М.: Гелиос АРВ, 2002.- 480 с.

3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: издательство ТРИУМФ, 2003 - 816 с.

4. Шенон К. Э. Теория связи в секретных тизимх. В кн.: Шенон К.Э. Работы по теории информации и кибернетике. М.: ИЛ, 1963, том 1. - С. 333-402.

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

6. Diffie W. and Hellman M.E. «New directions in cryptography» IEEE Trans. Informat. Theory, vol. IT-22, pp. 644-654, Nov. 1976.

7. R. C. Merkle «Secure communication over insecure channels», Comm. ACM, pp. 294-299, Apr. 1978.

8. Харин Ю. С., Берник В.И., Матвеев Г. В., Агиевич С. Г. «Математические и комьютерные основы криптологии» ООО «Новое знание» 2003 г. 381 стр.

9. Ростовцев А. Г., Маховенко Е. Б., Теоретическая криптография. НПО «Профессионал», Санкт-Петербург. 2004г. - 478 стр.

10. Молдовян А. А., Молдовян Н. А., Советов Б. Я.. Криптография. – Санкт-Петербург, Изд. «Лань», 2001. – 224 с.

11. Венбо Мао. Современная криптография. Теория и практика. – Москва–Санкт-Петербург–Киев: Лори Вильямс, 2005. –768 с.

12. Коблиц Н. Курс теории чисел и криптографии. – М. Научное изд-во ТВП, 2001г. – 261 стр.

13. Акбаров Д.Е., Ахмадалиев Ш.Ш., Нуриев Ш.З. Криптология асосларида математика. Ўқув қўлланма. – Фарғона, 2003. – 48 б.

14. Акбаров Д. Е., Ясинский. Математика в становлении науки криптологии. – Киев. “Политехника”. 2001. – 42с.

15. Хасанов Х. П. Такомиллашган диаматрицалар алгебралари ва параметрли алгебра асосида криптотизимлар яратиш усуллари ва алгоритмлари. –Тошкент, 2008. -208 б.

16. Rueppel R. A. Stream ciphers // Contemporary Cryptology, The Science of Information Integrity. - New York, 1992. - P.p. 65-134.

17. Shamir A. On the generation of cryptografically strong pseudo-random sequences // ACM Trasaction on Computer Systems. 1983. vol. 1. - Pp. 38-44.

18. Siegenthaler T. Correlation-immunity of nonlinear combining functions for cryptographic applications // IEEE Trans. Inform. Theory. 1984. - Pp. 776-780.

19. Siegenthaler T. Decrypting a class of stream ciphers using ciphertext only // IEEE Trans. Comput. 1985. vol. C-34, - P.p. 81-85.

20. Арипов М., Пудовченко Ю. Основы криптологии. -Т.:НУУ, 2004. - 136 с.

21. Арипов М., Пудовченко Ю. Современные суперкомпьютеры и проблемы криптографической силовой атаки // - Т., НУУ, 2000. - 16 с.

22. Каримов М.М. Организация корпоративных компьютерных сетей с интегрированной системой защиты информации // Дис. на соискание доктора техн.наук. - Т.: ТашГТУ, 2003.

23. Каримов М.М., Сапарова Т.А. Шифрлашнинг блокли ва оқимли тизимларида махфий калитли замонавий криптография тенденциялари // ТАТУ хабарлари. - Т., 2008. - №4. - Б.35-39.

24. Агибалов Г.П. 50 лет криптографии в Томском государственном университете // Прикладная дискретная математика. 2009. - №2. - С.104-126.

25. Аграновский А.В., Хади Р.А. Практическая криптография. - М.: СОЛОН-Пресс, 2002. - 254 с.

26. Асосков А.В., Иванов М.А., Мирский А.А. Поточные шифры. - М.: Кудиц-Образ, 2003. - 336 с.

27. Винокуров А. Современность практической криптографии // Системы безопасности связи и телекоммуникаций. 2003. - №10. - С.218-221.

28. Гатчин Ю.А., Коробейников А.Г. Основы криптографических алгоритмов. Учебное пособие. - СПб.: ГИТМО(ТУ), 2002. - 29 с.

29. Щеглов А.Ю. Защита копьютерной информации от несанкционированного доступа. - СПб.: Наука и Техника, 2004. - 386 с.

30. Дернова Е.С., Костина А.А., Молдовяну П.А. Конечные группы матриц как примитив алгоритмов цифровой подписи // Вопросы защиты информации. - М., 2008. - №3(82). - С. 8-11.

31. Докучаев Д. Неслучайные числа. Взлом генератора случайных чисел -ULTIMATE-БАГ движка PHP // Хакер. - М., 2008. - №119. - С.58-59.

32. Дударев Д.А., Панасенко С.П. Аппаратные шифраторы фирмы «Анкад» гарантия надежной защиты данных // Вопросы защиты информации. - М., 2006. - №2(73). - С. 12-14.

33. Дуйков Е.А., Сотский С.В., Щербаков А.Ю., Кирин В.И. Формулирование требований к защищенному электронному документообороту // Вопросы защиты информации. - М., 2008. -№4(83). - С. 28-32.

34. Жельников В. Криптография от папируса до компьютера. - М.: ABF, 1997. - 336 с.

35. Жуков И.Ю., Иванов М.А., Осмоловский С.А. Принципы построения криптостойких генераторов псевдослучайных кодов // Проблемы информационной безопасности компьютерных систем.-М.,2001.№1. -С.55-65.

36. Жўраев И., Назаров А., Тешабекова Х. Ўзбекистон Республикаси давлат ахборот ресурслари: уларнинг ҳолати ва ривожлантириш йўллари // InfoCOM.UZ. - Т., 2008. - №3. - Б. 28-29.

37. Завгородний В.И., Комплексная защита информации в компьютерных системах. Учебное пособие. - М.: Логос, 2001. - 264 с.

38. Задонский А.Ю. Защита от утечек конфиденциальной информации в центрах обработки и хранилищах данных // Защита информации. INSIDE. - М., 2007. - №5. - С. 41-45.

39. Мусаев А.И. Криптобардошли алгоритмларни комбинациялашга асосланган узлуксиз шифрлаш алгоритми // ТАТУ хабарлари. - Т., 2010. - №2. - Б.21-24.

40. Мусаев А.И. Узлуксиз шифрлаш алгоритмларидан универсал криптобардошли хеш-функция яратиш // ТАТУ хабарлари. - Т., 2010. - №2. - Б.15-19.

41. Коробейников А.Г., Гатчин Ю.А. Математические основы криптологии. Учебное пособие. - СПб.: ИТМО, 2004. - 106 с.

42. Косов А.В. Современные методы тестрования криптографических программных средств // Защита информации. INSIDE.-М.,2007.-№6.-С.64-66.

43. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. - М.: Постмаркет, 2001. - 323 с.

44. Куприянов А.О. Основы методологии проведения аудита информационной безопасности // Вопросы защиты информации. - М., 2006. - №4(75). - С. 2-5.

45. Минаси М. Шифровальщик Cipher // Windows IT Pro/RE. - М., 2008. - №3. - С. 94-95.

46. Моисеева П.Ю. Оценка возможностей организации по проектированию безопасных систем на основе стандарта ISO/IEC 21827 // Вопросы защиты информации. - М., 2006. - №3(74). - С.26-36.

47. Молдовян Н.А. Проблематика и методы криптографии. - СПб.:БХВ-Петербург, 1998. - 212 с.

48. Молдовян Н.А., Нгуен Л.М., Хо Н.З. Синтез поточных шифров на основе блочных преобразований : метод латинских квадратов // Вопросы защиты информации. - М., 2008. -№1(80). - С. 27-34.

49. Молдовян Н.А., Щилков М.В., Филиппов Д.М. Реализация процедуры усложнения ключа в скоростных шифрах на основе управляемх подстановочно-перестановочных сетей // Вопросы защиты информации. - М., 2007. - №4(79). - С.2-7.

50. Молдовян П.А., Дернова Е.С., Молдовян Д.Н. Синтез конечных расширенных полей для криптографических приложений // Вопросы защиты информации. - М., 2008. - №3(82). - С.12-16.

51. Молдовян Н. А., Молдовян А. А., Еремеев М. А. Криптография: от примитивов к синтезу алгоритмов. –СПб.: БХВ-Петербург, 2004. - 448 с.

52. Молдавян А. А., Молдавян Н. А., Гуц Н. Д., Изотов Б.В. Криптография. Скоростные шифры. –Санкт-Петербург. «БХВ-Петербург» 2002г. – 439 стр.

53. Молдавян А. А., Молдавян Н.А. Введение в криптосистемы с открытым ключом. Санкт – Петербург «БХВ-Петербург» 2005г. – 288с.

54. Зензин О. С., Иванов М. А.. Стандарт криптографической защиты – AES. Конечные поля /Под ред. М. А. Иванова – М.: КУДИЦ-ОБРАЗ, 2002. - 176 с.

55. Акбаров Д. Е. Криптография, Стандарты алгоритмов криптографической защиты информации и их приложения. –Ташкент, 2007. -188 с.

56. Иванов М. Криптографические методы защиты информации в компьютерных системах и сетях. – М., «Кудиц-Образ», 2001, –368с

57. Мухачев В.А., Хорошко В.А. Методы практической криптографии. Киев: Полиграф-Консалтинг, 2005. - 215 с.

58. Ожиганов А.А. Основы криптоанализа симметричных шифров. Учебное пособие. - СПб.: ИТМО, 2008. - 44 с.

59. Панасенко С.П. Защита от несанкционированного доступа // Вопросы защиты информации. - М., 2006. - №3(74). - С. 37-39.

60. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. - М.:ДМК, 2000. - 448 с.

61. Романец Ю.В., Тимофеев П.А. Защита информации в компьютерных системах и сетях. - М.: Радио и Связь, 2001. - 376 с.

62. Ростовцев А.Г. Алгебраические основы криптографии. - СПб.:Мир и Семья, 2000. - 296 с.

63. Ростовцев А.Г., Маховенко Е.Б. Введение в криптографию с открытым ключом. - СПб.: Мир и Семья, 2001. - 336 с.

64. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: Учебное пособие для вузов. - М.: Горячая линия-Телеком, 2005. - 229 с.

65. Рябко Б.Я., Фионов А.Н. Основы криптографии для специалистов в информационных технологиях. - М.:Научный мир, 2004. - 173 с.

66. Скляров Д.В. Исскуство защиты и взлома информации. - СПб.: БХВ-Петербург, 2004. - 288 с.

67. Снеддон Р., Вилански Э. Технология Kerberos для обеспечения безопасности MOSS 2007 // Windows IT Pro/RE. - М., 2008. - №5. - С.38-45.

68. Стахов А.П. «Золотая» криптография // Перспективные информационные технологии и интеллектуальные системы. 2006. № 4. - С.48-55.

69. Тужилин М.Э. Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. - № 3. - С.14-20.

70. Фергюсон Н., Шнайер Б., Практическая криптография. - М.: Вильямс, 2005. - 424 с.

71. Шалыто А.А. Методы аппаратной и программной реализации алгоритмов. - СПб.:Наука, 2001. - 777 с.

72. Хасанов П.Ф., Исаев Р.И., Назарова М.Х., Хасанов Х.П., Ахмедова О.П. Ахборотнинг криптографик муҳофазаси тарихи. Компьютер криптографияси даври // Алоқа дунёси. - Т., 2006, - №1(6). - Б. 59-74.

73. Акбаров Д. Е. Разработка алгоритма цифровой подписи на основе композиции существующих сложностей // Инфокоммуникации: Сети-Технологии-Решения.-3 (7)/2008. -с. 46-49.

74. Акбаров Д. Е. Об одном алгоритме шифрования данных с симметричным ключом. // Инфокоммуникации: Сети-Технологии-Решения. -4(8)/2008. -с. 25-36.

75. Акбаров Д. Е., Ахмедова О. П. Генерация стойких ключей для симметричных блочных алгоритмов шифрования. // Кимёвий технология, назорат ва бошқарув. -5/2008. –с. 29-32.

76. Акбаров Д. Е., Ахмадалив Ш.Ш., Хасанов П. Ф. Параметрли алгебра амалларидан фойдаланиб мавжуд ҳисоблаш мураккабликлари асосида янги асимметрик алгоритмлар яратиш усуллари //Инфокоммуникации: Сети-Технологии-Решения. -1(9)/2009. -с. 31-35.

77. Акбаров Д. Е., Мусаев А. И. Мавжуд узликсиз шифрлаш алгоритмлари асосларини тадқиқи ва уларнинг туркумлари //Инфокоммуникации: Сети-Технологии-Решения. -1(9)/2009. -с. 36-45.

78. Акбаров Д.Е., Камолов М.Э. Гаммалаштиришга асосланган самарали блоклаб шифрлаш алгоритми ва унинг аппарат қурилмасини яратишнинг функционал модели // ТАТУ хабарлари. Т., 2009. - №3. - Б.14-18.

79. Акбаров Д. Е., Собиров Ш.О. Скрытое использование параметра R эллиптической кривой, связанного случайно выбранной величиной, как параметр проверки подписи ЭЦП. //ФарПИ Илмий-техника журнали. -2009, №1.-с. 3-11.

80. Акбаров Д. Е., Мусаев А. И. Чекли майдонда матрицали кенгайтириш ва жадвалли сиқиш акслантиришларига асосланган узликсиз шифрлаш алгоритми //Кимёвий технология, назорат ва бошқарув. Илмий-техникавий журнал. -3/2009. - с. 47-50.

81. Акбаров Д.Е., Собиров Ш.О., Саидов М.И. О функциональной схеме приложения электронно-цифровой подписи в электронном документообороте // ФерГУ. Научный вестник. 2009 № 1. с. 3-9.

82. Акбаров Д.Е., Собиров Ш.О., Саидов М.И. Алгоритм ЭЦП со скрытым использованием параметра R эллиптической кривой, связанного

случайно выбранным параметром // ФерГУ. Научный вестник. -2009 № 2. -с. 3-11

83. Акбаров Д.Е., Собиров Ш.О. Маълумотларни шифрлашнинг симметрик калитли алгоритми яратиш // ФарПИ Илмий-техника журнали. -2009 № 2. -с. 3-6.

84. Акбаров Д.Е., Собиров Ш.О. Азизов Э.Ю. Шифрлаш алгоритм орқали эллиптик эгри чизиқ *R* параметрини ЭРИ текширишнинг яширин параметри сифатида ишлатиш // ФарПИ Илмий-техника журнали. -2009 № 3. -с. 3-7

85. Акбаров Д.Е., Собиров Ш.О. Алгоритм ЭЦП на эллиптической кривой в композиции сложностей вычисления дискретного логарифмирования и факторизации натуральных чисел на простые множители // Интернет журнал «Аспирант и соискатель» www.sputnikplus 2000 @ mail. ru. -2009 г. июнь.

86. Акбаров Д.Е., Собиров Ш.О., Азизов Э.Ю. Latent use of parameter R of the elliptic curve, as parameter ofcheck eds, with application of algorithm of enciphering It promotion in asia 2009, September 21-25, Tashkent University of IT) // Труды ммеждународной конференции. -с. 187-191.

87. Акбаров Д.Е., Тураев Б.Т. Электрон ҳужжатли маълумот алмашинуви муҳофазасида криптографик воситалар композицияси моделларидан фойдаланиш // ТАТУ хабарлари. Т., 2009. - №2. - Б.32-37.

88. Тураев Б.Т. Ахборот коммуникация тизимида маълумот алмашинуви муҳофазасида криптографик воситалар композицияси моделларидан фойдаланиш // Республиканский семинар: «Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения» Сборник тезисов и докладов Ташкент 29 октября 2010 год

89. Turaev B.T, Komolov M.E, Adenov B.E., Cryptographic protection of the information in information-telecommunication systems with application of composite models It promotion in asia 2009, September 21-25, Tashkent University of IT) // Труды ммеждународной конференции. -с. 192-195.

90. Тураев Б.Т., Ходжаев А.М. Компьютер тармокларида хужжатли маълумотларни кафолатли алмашинувини таъминлаш. // ********

91. Дейтель Г. Введение в операционные системы. Том 2. М.: Мир, 1987, с. 357-371.

92. Феллер В. Введение в теорию вероятностей и ее приложения. Том 2. М.: Мир, 1984.

93. Кнут Д. Искусство программирования для ЭВМ. Том 1. Основные алгоритмы. М.: Мир, 1976.

94. Гэри М. , Джонсон Д. Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.

95. Simmons G. J. «Authentication theory/coding theory, in Advances in Cryptology, Proceedings of CRYPTO 84, G. R. Blakley and D. Chaum, Eds. Lecture Notes in Computer Sciense, No. 196. New York, NY: Springer, 1985, pp. 411-431

96. Xiao G. Z., Massey J. L.A spectral characterization of correlation-immune functions. // IEEE Trans. Inform. Theory. 1988. - Pp. 569-571

97. Бабаш А. В., Шанкин Г. П. Криптография. –Москва: Лори Гелиос АРВ, 2002. –512 с.

98. Бабенко Л.К., Мишустина Е.А. Методическое пособие по изучению современных методов криптоанализа. - Таганрог, ТРТУ, 2003. - 66 с.

99. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. - М.: Горячая линия-Телеком, 2001. - 250 с.

100. Бутырский Л.С., Гольев Ю.И., Ларин Д.А., Никонов Н.В., Шанкин Г.П. Криптографическая деятельность в Швеции от викингов до Хагельмана // Защита информации. INSIDE.- М., 2007. - №3. - С. 88-96.

101. Новиков П.С. Элементы математической логики. - М. ИЛ, 1973.

102. Логачёв О. А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии. – М. Изд. МЦНМО, 2004. – 470 с.

103. Фомичев В. М. Дискретная математика и криптология. – Москва, “ДИАЛОГ-МИФИ”, 2003. – 400 с.

104. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии. – М., МЦНМО, 2003. – 328 с.

105. Столлингс В. Криптография и защита сетей: принципы и практика. – М. , Изд. дом «Вильямс», 2001. – 672 с.

106. Анохин М. И., Варновский Н. П., Сидельников В. М., Ященко В. В. Криптография в банковском деле. – М., Изд. МИФИ, 1997.

107. O‘z DSt 1106 : 2006. Государственный Стандарт Узбекистана. Информационная технология. Криптографическая защита информации. Функция хэширования. – Ташкент. Узбекское агентство стандартизации, метрологии и сертификации. 2006.

108. Shafi Goldwasser, Mihir Bellare. Lecture Notes on Cryptography. Cambridge, Massachusetts, August, 1999. – 268 p.

109. Menezes A., P. van Oorshot, Vanstone S. Handbook of Applied Cryptography. CRC Press, 1996. – 780 p.

110. ГОСТ Р 34.11 – 94. Государственный Стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования. – Москва. Издательство стандартов, 1994.

111. Federal Information Processing Standards Publication 180-2. Secure Hash Standard. 2002 August 1.

112. Federal Information Processing Standards Publication 198. The Keyed-Hash Message Authentication Code (HMAC). 2002 March 6.

113. Ященко В. В. и др. Введение в криптографию. – М., МЦНМО, 2000. – 288 с.

114. Чмора А. Современная прикладная криптография. – М., Гелиос АРВ, 2002. – 256 с.

115. Ростовцев А., Михайлова М. Методы криптоанализа классических шифров.

116. Акбаров Д. Е., Собиров Ш.О., Далиев Б., Бозоров Б. Вероятностно-статистические модели анализа текстов //ФарПИ Илмий-техника журнали. -2011, №1.-с. 41-46.

117. Акбаров Д. Е., Собиров Ш.О., … //ФарПИ Илмий-техника журнали. -2011, №2. -с. 41-46.

118. Акбаров Д. Е., Собиров Ш.О., … //ФарПИ Илмий-техника журнали. -2011, №4. -с. 41-46.

119. Акбаров Д.Е. , Ахмедова О.П., Хасанов Х.П. Криптографиянинг математик асослари. Дарслик. –Тошкент. Нашрёт, 2012. –200 с.

120. Шпак Ю.А. Программирование на языке С для микропроцессоров PIC и AVR. – Киев:МК-Пресс, 2006. -400 с.

121. Касымов С.С., Джураев О.Н. Проекты по разработке свободного программного обеспечения // ТАТУ хабарлари. - Т., 2009. - №2. -Б.7-10.

122. C# для профессионалов / Симон Робинсон, Олли Корнес Джей Глин, Бартон Харвей и др. В 2-х т. - М.:Лори, 2003. - 1616 с.

123. Microsoft Corporation, Разработка Windows-приложений на Microsoft Visual Basic .NET и Microsoft Visual C# .NET. Учебный курс MCAD/MCSD. - М.: Русская Редакция, 2003. - 512 с.

124. Агуров П.В. C# сборник рецептов. - СПб.: БХВ-Петербург, 2007. - 432 с.

125. Дейтел Х.М., Дейтел П.Дж. Как программировать на C++. - М.: Бином, 2003. - 115 с.

126. Лабор В.В. Создание приложений для Windows. - Минск:Харвест, 2003. - 384 с.

127. Либерти Д. Программирование на C#. - СПб.:Символ Плюс, 2003. - 680 с.

128. Петцольд Ч. Программирование для Microsoft Windows на C#. В 2-х т., -М.: Русская Редакция, 2002. - 576 с.

129. Просиз Д. Программирование для Microsoft .NET. - М.: Русская Редакция, 2003. - 704 с.

130. Рихтер Д. Программирование на платформе Microsoft .NET Framework. - М.: Русская Редакция, 2003. - 512 с.

131. Троелсен Э. C# и платформа .NET. Библиотека программиста. - СПб.: Питер, 2004. - 796 с.

132. Шилдт Г. Полный справочник по C#. - М.: Вильямс, 2004. - 752 с.

133. Andrew Rukhin, Juan Soto, James Nechvatal. A statistical test suite for random and pseudorandom number generators for cryptografic applications // NIST Special Publication. 800-22. 2001.

134. Camion P., Carlet C., Charpin P., Sendrier N. "On correlation-immune functions" // Lecture Notes in Computer Science. Advances in Crypology: Crypto '91 Proc., - Berlin, 1991. vol. 576. - Pp. 87-100.

135. Musaev A.I. Estimation cryptostability of the stream cipher algorithm // IT Promotion in Asia. Intern. conf. ETRI/TUIT/ITIRC. 2009. - P.p. 196-199.

136. Reinhard Wobst, Cryptography unlocked. Wiley, 2007. - 540 p.

138. Мусаев А. И. Мавжуд узликсиз шифрлаш алгоритмлари асосларини тадқиқ қилиш ва янги криптобардошли алгоритмлар яратиш // Мутахасислик: 05.13.19 –”Ахборотни химоялаш усуллари ва тизимлари, ахборот хавфсизлиги” ахборот хавфсизлиги йўналиши бўйича техника фанлари номзоди даражасидаги диссертация. –Тошкент.: ТАТУ, 2011.

139. Акбаров Д.Е., Мухтаров Ф. М., Сиддиқов А. Криптотаҳлил масалаларига тизимли ёндошув асослари ва уларни ечиш усуллари. –”Фарғона” нашрёти, 2014. –143 б.

ИЛОВА

des.pas

```
unit DES;
interface
Uses Windows, Classes, SysUtils, Math, Dialogs;
Type
  TBitString = Array of Boolean;
  PBitString = ^TBitString;
  TSplitKeyParts = record
    C:TBitString;
    D:TBitString;
    end;
  TSplitKey = Array[0..16]Of TSplitKeyParts;
  TConcatKey = Array[0..15]Of TBitString;
  TIPKeyParts = record
    L:TBitString;
    R:TBitString;
    end;
  TIPKey = Array[0..16]OF TIPKeyParts;
Const
DES_PC1:Array[0..55] Of Byte = (57,49,41,33,25,17,9,
                        1,58,50,42,34,26,18,
                        10,2,59,51,43,35,27,
                        19,11,3,60,52,44,36,
                        63,55,47,39,31,23,15,
                        7,62,54,46,38,30,22,
                        14,6,61,53,45,37,29,
                        21,13,5,28,20,12,4);
DES_PC2:Array[0..47] Of Byte = (14,17,11,24,1,5,
                        3,28,15,6,21,10,
                        23,19,12,4,26,8,
                        16,7,27,20,13,2,
                        41,52,31,37,47,55,
                        30,40,51,45,33,48,
                        44,49,39,56,34,53,
                        46,42,50,36,29,32);
DES_IP:Array[0..63] Of Byte = (58,50,42,34,26,18,10,2,
                       60,52,44,36,28,20,12,4,
```

```
                    62,54,46,38,30,22,14,6,
                    64,56,48,40,32,24,16,8,
                    57,49,41,33,25,17,9,1,
                    59,51,43,35,27,19,11,3,
                    61,53,45,37,29,21,13,5,
                    63,55,47,39,31,23,15,7);
DES_E:Array[0..47] Of Byte = (32,1,2,3,4,5,
                    4,5,6,7,8,9,
                    8,9,10,11,12,13,
                    12,13,14,15,16,17,
                    16,17,18,19,20,21,
                    20,21,22,23,24,25,
                    24,25,26,27,28,29,
                    28,29,30,31,32,1);
S_BOXES:Array[0..7,0..3,0..15]Of Byte = (
((14,04,13,01,02,15,11,08,03,10,06,12,05,09,00,07),
  (00,15,07,04,14,02,13,01,10,06,12,11,09,05,03,08),
  (04,01,14,08,13,06,02,11,15,12,09,07,03,10,05,00),
  (15,12,08,02,04,09,01,07,05,11,03,14,10,00,06,13)),
((15,01,08,14,06,11,03,04,09,07,02,13,12,00,05,10),
        (03,13,04,07,15,02,08,14,12,00,01,10,06,09,11,05),
        (00,14,07,11,10,04,13,01,05,08,12,06,09,03,02,15),
        (13,08,10,01,03,15,04,02,11,06,07,12,00,05,14,09)),
((10,00,09,14,06,03,15,05,01,13,12,07,11,04,02,08),
        (13,07,00,09,03,04,06,10,02,08,05,14,12,11,15,01),
        (13,06,04,09,08,15,03,00,11,01,02,12,05,10,14,07),
        (01,10,13,00,06,09,08,07,04,15,14,03,11,05,02,12)),
((07,13,14,03,00,06,09,10,01,02,08,05,11,12,04,15),
        (13,08,11,05,06,15,00,03,04,07,02,12,01,10,14,09),
        (10,06,09,00,12,11,07,13,15,01,03,14,05,02,08,04),
        (13,15,00,06,10,01,13,08,09,04,05,11,12,07,02,14)),
((02,12,04,01,07,10,11,06,08,05,03,15,13,00,14,09),
        (14,11,02,12,04,07,13,01,05,00,15,10,03,08,09,06),
        (04,02,01,11,10,13,07,08,15,09,12,05,06,03,00,14),
        (11,08,12,07,01,14,02,13,06,15,00,09,10,04,05,03)),
((12,01,10,15,09,02,06,08,00,13,03,04,14,07,05,11),
        (10,15,04,02,07,12,09,05,06,01,13,14,00,11,03,08),
        (09,14,15,05,02,08,12,03,07,00,04,10,01,13,11,06),
        (04,03,02,12,09,05,15,10,11,14,01,04,06,00,08,13)),
((04,11,02,14,15,00,08,13,03,12,09,07,05,10,06,01),
```

```
            (13,00,11,07,04,09,01,10,14,03,05,12,02,15,08,06),
            (01,04,11,13,12,03,07,14,10,15,06,08,00,05,09,02),
            (06,11,13,08,01,04,10,07,09,05,00,15,14,02,03,12)),
((13,02,08,04,06,15,11,01,10,09,03,14,05,00,12,07),
            (01,15,13,08,10,03,07,04,12,05,06,11,00,14,09,02),
            (07,11,04,01,09,12,14,02,00,06,10,13,15,03,05,08),
            (02,01,14,07,04,10,08,13,15,12,09,00,03,05,06,11))
);
DES_P:Array[0..31] Of Byte = (16,7,20,21,
                        29,12,28,17,
                        1,15,23,26,
                        5,18,31,10,
                        2,8,24,14,
                        32,27,3,9,
                        19,13,30,6,
                        22,11,4,25);
DES_REVERSE_IP:Array[0..63] Of Byte = (40,8,48,16,56,24,64,32,
        39,7,47,15,55,23,63,31,
        38,6,46,14,54,22,62,30,
        37,5,45,13,53,21,61,29,
        36,4,44,12,52,20,60,28,
        35,3,43,11,51,19,59,27,
        34,2,42,10,50,18,58,26,
        33,1,41,9,49,17,57,25);

DES_LSH:Array[0..15] Of Byte = (1,1,2,2,2,2,2,2,1,2,2,2,2,2,2,1);
Function BinToInt(S:TBitString):Integer;
Function IntToBin(N:Integer;Precision:Integer=8):TBitString;
Function BinToStr(Bits:TBitString):String;
Function StrToBin(S:String):TBitString;
Function AnsiStrToBin(S:String; Zeroes:Boolean=True):TBitString;
Function BinToAnsiStr(Bits:TBitString):String;
Procedure CopyBits(Var Dest:TBitString; Source:TBitString; NBits:Integer);
Function ConcatBits(Bits:Array Of TBitString):TBitString;
Function DESEncode(S,Key:String):TBitString;
Function DESDecode(S,Key:String):TBitString;
Function GetPermutedKey(Key:TBitString):TBitString;
Function GetPermutedKey2(Key:TBitString):TBitString;
Function GetSplitKey(Key:TBitString):TSplitKey;
Function GetConcatKey(Key:TSplitKey):TConcatKey;
```

```
Function GetIPKey(M:TBitString; ConcatKey:TConcatKey):TIPKey;
Function GetF(R,K:TBitString):TBitString;
Function GetSBox(Index:Integer; T:TBitString):TBitString;
Function GetReverseIP(RL:TBitString):TBitString;
Procedure ReverseSubKeys(Var Keys:TConcatKey);
implementation
Function ConcatBits(Bits:Array Of TBitString):TBitString;
Var
I,C:Integer;
Begin
SetLength(Result,0);
For C:=0 To Length(Bits)-1 Do
 Begin
 SetLength(Result,Length(Result)+Length(Bits[C]));
 For I:=0 To Length(Bits[C])-1 Do
  Result[Length(Result)-Length(Bits[C])+I]:=Bits[C][I];
 End;
End;
Procedure CopyBits(Var Dest:TBitString; Source:TBitString; NBits:Integer);
Var
I:Integer;
Begin
SetLength(Dest,NBits);
For I:=0 To NBits-1 Do
 Dest[I]:=Source[I];
End;
Function BinToInt(S: TBitString): Integer;
Var
L,I:Integer;
Begin
Result:=0;
L:=Length(S);
IF L=0 Then
 Raise EConvertError.Create('Specified bit string is zero length');
For I:=L-1 DownTo 0 Do
 Result:=Result+Ord(S[I])*Trunc(Power(2,L-I-1));
End;
Function IntToBin(N:Integer; Precision:Integer):TBitString;
Var
BitList:TList;
```

```
Bit:PBoolean;
Begin
SetLength(Result,0);
BitList:=TList.Create;
While N>0 Do
 Begin
 New(Bit);
 Bit^:=Boolean(N mod 2);
 BitList.Insert(0,Bit);
 N:=N div 2;
 End;
While BitList.Count<Precision Do
 Begin
 New(Bit);
 Bit^:=False;
 BitList.Insert(0,Bit);
 End;
For N:=0 To BitList.Count-1 Do
 Begin
 SetLength(Result,N+1);
 Bit:=BitList.Items[N];
 Result[N]:=Bit^;
 Dispose(Bit);
 End;
BitList.Free;
end;
Function AnsiStrToBin(S: String; Zeroes:Boolean):TBitString;
Var
Temp,B:TBitString;
L,I,J:Integer;
Begin
L:=0;
SetLength(Result,L);
SetLength(Temp,L);
SetLength(B,0);
For I:=1 To Length(S) Do
 Begin
 B:=IntToBin(Ord(S[I]));
 L:=L+Length(B);
 SetLength(Temp,L);
```

```
  For J:=0 To Length(B)-1 Do
    Temp[Length(Temp)-Length(B)+J]:=B[J];
  End;
Result:=Temp;
End;
Function BinToStr(Bits:TBitString):String;
Var
I,L:Integer;
Begin
Result:='';
L:=Length(Bits);
IF L=0 Then
  Raise EConvertError.Create('Specified bit string is zero length');
For I:=0 To L-1 Do
  IF Bits[I] Then Result:=Result+'1'
  Else Result:=Result+'0';
End;
Function StrToBin(S:String):TBitString;
Var
I:Integer;
Begin
SetLength(Result,0);
For I:=1 To Length(S) Do
  Begin
  IF (S[I]<>'1')And(S[I]<>'0') Then
    Raise EConvertError.Create(S+' is invalid binary string');
  SetLength(Result,I);
  Result[I-1]:=Boolean(StrToInt(S[I]));
  End;
End;
Function BinToAnsiStr(Bits:TBitString):String;
Var
I:Integer;
B:TBitString;
Begin
Result:='';
SetLength(B,8);
I:=0;
While I<=Length(Bits)-8 Do
  Begin
```

```
  CopyMemory(B,Ptr(Integer(Bits)+I),8);
  Result:=Result+Char(BinToInt(B));
  Inc(I,8);
  End;
End;
Function GetPermutedKey(Key:TBitString):TBitString;
Var
I:Integer;
Begin
SetLength(Result,Length(DES_PC1));
For I:=0 To Length(DES_PC1)-1 Do
  Result[I]:=Key[DES_PC1[I]-1];
End;
Function GetPermutedKey2(Key:TBitString):TBitString;
Var
I:Integer;
Begin
SetLength(Result,Length(DES_PC2));
For I:=0 To Length(DES_PC2)-1 Do
  Result[I]:=Key[DES_PC2[I]-1];
End;
Function GetSplitKey(Key:TBitString):TSplitKey;
  Function LeftShift(Key:TBitString; N:Integer):TBitString;
  Var
  I,J:Integer;
  Temp:TBitString;
  Begin
  SetLength(Result,28);
  SetLength(Temp,28);
  For I:=0 To 27 Do
    Temp[I]:=Key[I];
  For J:=1 To N Do
    Begin
    For I:=1 To 27 Do
      Result[I-1]:=Temp[I];
    Result[27]:=Temp[0];
    For I:=0 To 27 Do
      Temp[I]:=Result[I];
    End;
  End;
```

```
Var
I,J:Integer;
Begin
For J:=1 To 16 Do
 Begin
 SetLength(Result[J].C,28);
 SetLength(Result[J].D,28);
 End;
CopyBits(Result[0].C,Key,28);
CopyBits(Result[0].D,TBitString(Integer(Key)+28),28);
For I:=1 To 16 Do
 Begin
 Result[I].C:=LeftShift(Result[I-1].C,DES_LSH[I-1]);
 Result[I].D:=LeftShift(Result[I-1].D,DES_LSH[I-1]);
 End;
End;
Function GetConcatKey(Key:TSplitKey):TConcatKey;
Var
I:Integer;
Temp:TBitString;
Begin
For I:=0 To 15 Do
 Begin
 SetLength(Result[I],56);
 Temp:=ConcatBits([Key[I+1].C,Key[I+1].D]);
 Result[I]:=GetPermutedKey2(Temp);
 End;
End;
Function GetIPKey(M:TBitString; ConcatKey:TConcatKey):TIPKey;
Var
I,J:Integer;
IP, F:TBitString;
Begin
For I:=0 To 16 Do
 Begin
 SetLength(Result[I].L,32);
 SetLength(Result[I].R,32);
 End;
SetLength(IP,64);
For I:=0 To Length(DES_IP)-1 Do
```

```
  IP[I]:=M[DES_IP[I]-1];

For I:=0 To 31 Do
  Result[0].L[I]:=IP[I];
For I:=32 To 63 Do
  Result[0].R[I-32]:=IP[I];
For I:=1 To 16 Do
  Begin
  Result[I].L:=Result[I-1].R;
  F:=GetF(Result[I-1].R,ConcatKey[I-1]);
  For J:=0 To 31 Do
    Result[I].R[J]:=Result[I-1].L[J] XOR F[J];
  End;
End;
Function GetF(R,K:TBitString):TBitString;
Var
I,J:Integer;
S,E,KE,F,T:TBitString;
Begin
SetLength(E,48);
For I:=0 To 47 Do
  E[I]:=R[DES_E[I]-1];
SetLength(KE,48);
For I:=0 To 47 Do
  KE[I]:=K[I] XOR E[I];
SetLength(T,6);
SetLength(F,0);
SetLength(S,4);
I:=0;
While I<48 Do
  Begin
  For J:=0 To 6 Do
    T[J]:=KE[J+I];
  S:=GetSBox(I div 6,T);
  F:=ConcatBits([F,S]);
  I:=I+6;
  End;
SetLength(Result,32);
For I:=0 To 31 Do
  Result[I]:=F[DES_P[I]-1];
```

```
End;

Function GetSBox(Index:Integer; T:TBitString):TBitString;
Var
Val,Row,Col:Integer;
Temp:TBitString;
Begin
SetLength(Result,4);
SetLength(Temp,2);
Temp[0]:=T[0];
Temp[1]:=T[5];
Row:=BinToInt(Temp);
SetLength(Temp,4);
CopyBits(Temp,TBitString(@T[1]),4);
Col:=BinToInt(Temp);
Val:=S_BOXES[Index,Row,Col];
SetLength(Result,4);
Result:=IntToBin(Val,4);
End;
Function GetReverseIP(RL:TBitString):TBitString;
Var
I:Integer;
Begin
SetLength(Result,64);
For I:=0 To Length(DES_REVERSE_IP)-1 Do
  Result[I]:=RL[DES_REVERSE_IP[I]-1];
End;
Procedure ReverseSubKeys(Var Keys:TConcatKey);
Var
I,L:Integer;
T:TBitString;
Begin
SetLength(T,48);
L:=Length(Keys);
For I:=0 To (L-1)Div 2 Do
  Begin
  T:=Keys[I];
  Keys[I]:=Keys[(L-I)-1];
  Keys[(L-I)-1]:=T;
  End;
```

```
End;
Function DESEncode(S,Key:String):TBitString;
Var
I:Integer;
K:TBitString;
M:TBitString;
RL:TBitString;
Kplus:TBitString;
SplitKey:TSplitKey;
ConcatKey:TConcatKey;
IPKey:TIPKey;
Begin
K:=AnsiStrToBin(Key);
Kplus:=GetPermutedKey(K);
SplitKey:=GetSplitKey(Kplus);
ConcatKey:=GetConcatKey(SplitKey);
M:=AnsiStrToBin(S);
IPKey:=GetIPKey(M,ConcatKey);
SetLength(RL,64);
For I:=0 To 31 Do
 Begin
 RL[I]:=IPKey[16].R[I];
 RL[I+32]:=IPKey[16].L[I];
 End;
RL:=GetReverseIP(RL);
Result:=RL;
End;
Function DESDecode(S,Key:String):TBitString;
Var
I:Integer;
K:TBitString;
M:TBitString;
RL:TBitString;
Kplus:TBitString;
SplitKey:TSplitKey;
ConcatKey:TConcatKey;
IPKey:TIPKey;
Begin
K:=AnsiStrToBin(Key);
Kplus:=GetPermutedKey(K);
```

```
SplitKey:=GetSplitKey(Kplus);
ConcatKey:=GetConcatKey(SplitKey);
ReverseSubKeys(ConcatKey);
M:=AnsiStrToBin(S);
IPKey:=GetIPKey(M,ConcatKey);
SetLength(RL,64);
For I:=0 To 31 Do
 Begin
 RL[I]:=IPKey[16].R[I];
 RL[I+32]:=IPKey[16].L[I];
 End;
RL:=GetReverseIP(RL);
Result:=RL;
End;
end.
```

Форма қисми

```
unit Unit1;
interface
uses
 Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms,
 Dialogs, DES, StdCtrls;
type
 TForm1 = class(TForm)
   Label1: TLabel;
   Edit1: TEdit;
   Label2: TLabel;
   Memo1: TMemo;
   Button1: TButton;
   Label3: TLabel;
   Memo2: TMemo;
   Button2: TButton;
   Memo3: TMemo;
   Label4: TLabel;
   Memo4: TMemo;
   procedure Button1Click(Sender: TObject);
   procedure Button2Click(Sender: TObject);
   procedure Memo1Change(Sender: TObject);
   procedure FormCreate(Sender: TObject);
   procedure Edit1Change(Sender: TObject);
```

```
    procedure Memo2Change(Sender: TObject);
  private
    { Private declarations }
  public
    Data:TBitString;
  end;
var
  Form1: TForm1;
implementation
{$R *.dfm}
procedure TForm1.Button1Click(Sender: TObject);
Var
I:Integer;
S:String;
begin
IF ((Length(Memo1.Text)mod 8 <> 0) OR (Length(Edit1.Text)mod 8 <> 0)) Then
  Begin
  MessageBox(Handle,
  'Количество букв в сообщении должно быть кратоно 8 (перевод строки считается за 2 буквы)'+
  #10#13'Ключ должен состоять из 8 символов',
  Nil,MB_ICONSTOP);
  Exit;
  End;
SetLength(Data,0);
I:=1;
While I<=Length(Memo1.Text) Do
  Begin
  S:=Copy(Memo1.Text,I,8);
  Data:=ConcatBits([Data,DESEncode(S,Edit1.Text)]);
  I:=I+8;
  End;
Memo2.Text:=BinToAnsiStr(Data);
end;
procedure TForm1.Button2Click(Sender: TObject);
var
I:Integer;
begin
IF ((Length(Memo2.Text)mod 8 <> 0) OR (Length(Edit1.Text)mod 8 <> 0)) Then
  Begin
  MessageBox(Handle,
```

```
  'Количество букв в сообщении должно быть кратоно 8 (перевод строки считается за 2 буквы)'+
  #10#13'Ключ должен состоять из 8 символов',
  Nil,MB_ICONSTOP);
  Exit;
  End;
SetLength(Data,0);
I:=1;
While I<=Length(Memo2.Text) Do
  Begin
  Data:=ConcatBits([Data,DESDecode(Copy(Memo2.Text,I,8),Edit1.Text)]);
  I:=I+8;
  End;
Memo1.Text:=BinToAnsiStr(Data);
end;
procedure TForm1.Memo1Change(Sender: TObject);
begin
IF Memo1.Text<>'' Then
  Memo3.Text:=BinToStr(AnsiStrToBin(Memo1.Text))
Else Memo3.Clear;
Label2.Caption:='Message - ('+IntToStr(Length(Memo1.Text))+' characters)';
end;
procedure TForm1.FormCreate(Sender: TObject);
begin
Memo1.OnChange(Self);
Edit1.OnChange(Self);
end;
procedure TForm1.Edit1Change(Sender: TObject);
begin
Label4.Caption:=IntToStr(Length(Edit1.Text))+' characters';
end;
procedure TForm1.Memo2Change(Sender: TObject);
begin
IF Memo2.Text<>'' Then
  Memo4.Text:=BinToStr(AnsiStrToBin(Memo2.Text))
Else Memo4.Clear;
Label3.Caption:='Encoded message - ('+IntToStr(Length(Memo2.Text))+' characters)';
end;
end.
```