ЎЗБЕКИСТОН АЛОҚА ВА АХБОРОТЛАШТИРИШ АГЕНТЛИГИ
ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

Қўлёзма ҳуқуқида
УДК 621.391

МУСАЕВ АНВАР ИСАКОВИЧ

УЗЛУКСИЗ ШИФРЛАШНИНГ КРИПТОБАРДОШЛИ АЛГОРИТМЛАРИ ВА УЛАРНИНГ САМАРАДОРЛИГИНИ БАҲОЛАШ

05.13.19 - Ахборотни ҳимоялаш усуллари ва тизимлари, ахборот хавфсизлиги

Техника фанлари номзоди
илмий даражасини олиш учун тақдим этилган диссертация
АВТОРЕФЕРАТИ

Тошкент -2011

Иш Тошкент ахборот технологиялари университетида бажарилган

Илмий раҳбар	физика-математика фанлари доктори **Акбаров Давлатали Егиталиевич**
Расмий оппонентлар:	техника фанлари доктори, профессор **Ганиев Салим Каримович**
	техника фанлари номзоди, доцент **Рахимжонов Зафар Ёкубович**
Етакчи ташкилот	UNICON.UZ Давлат унитар корхонаси - Фан-техника ва маркетинг тадқиқотлари маркази

Ҳимоя Тошкент ахборот технологиялари университети ҳузуридаги Д.001.25.01 ихтисослашган кенгашнинг 2011 йил «10» ноябр соат 9⁰⁰ да ўтадиган мажлисида бўлади. Манзил: 100084, Тошкент шаҳри, Амир Темур кўчаси, 108, тел.: 238-64-13, e-mail: tuit@tuit.uz.

Диссертация билан Тошкент ахборот технологиялари университетининг кутубхонасида танишиш мумкин.

Автореферат 2011 йил «7» октябр да тарқатилди.

Ихтисослашган кенгаш илмий котиби Ганиев А.А.

ДИССЕРТАЦИЯНИНГ УМУМИЙ ТАВСИФИ

Мавзунинг долзарблиги. Ахборот-коммуникация тизимларида локал ва корпоратив компьютер тармокларининг кўпайиши ва бу тармокларнинг глобал интернет тармоғига уланиши фойдаланувчилар ўртасида электрон маълумот алмашувининг кенг кўлланилишига олиб келди. Жамиятнинг ахборотга бўлган эхтиёжи ахборот-ресурс марказларининг ташкил этилиши ва очиқ интернет тармоғи орқали фаолият юритишига олиб келиши билан бир вақтда алмашинувчи маълумотларнинг узатилиши давомида кафолатли муҳофазасини таъминлаш масаласини келтириб чиқарди. Ахборот-коммуникация тизимларининг тўлиқ равишда рақамлилаштирилиши, маълумотни узатишда оптик толали воситалардан фойдаланилиши, вилоятлараро видеоконференция, IP-телефония ва бошқа тутилишсиз узатилишни талаб қилувчи катта миқдордаги ахборот оқимларининг очиқ алоқа каналларида узатилиш давомида муҳофазасини таъминлаш масаласи ўз навбатида юқори тезликда тутилишсиз ишловчи криптографик воситаларни талаб қилади. Бундай криптографик воситалар асосини аппарат ва аппарат-дастурий воситаларда қулай ҳамда самарали амалга оширилувчи криптобардошли узлуксиз шифрлаш алгоритмлари ташкил этади. Ахборот-коммуникация тизимларидан фойдаланувчи корхона, ташкилот ҳамда муассасалар ўз фаолияти учун зарур бўлган маълумотларининг узатилиши ва қабул қилиниши давомида кафолатли муҳофазани таъминлаш учун четда ишлаб чиқарилган аппарат ва аппарат-дастурий криптографик воситаларини қўлламоқдалар. Бу каби воситаларда амалга оширилган криптоалгоритмларнинг бардошлиги, ҳамда қурилмаларнинг аннотацияларида келтирилган самарадорлик ва криптобардошлик даражалари Сертификат кўрсаткичларига тўлиқ мослиги кафолатланмаган. Валюта ҳиссбига Республикага олиб киритиладиган аппарат-дастурий воситаларнинг қайтадан сертификатлаш масаласи узлуксиз шифрлаш алгоритмларининг самарадорлигини бахолаш талаблари ва амалий усулларини яратиш асосидагина тўлиқ ечилиши мумкин.

Ахборот-коммуникация тизимларида маълумотларни кафолатли муҳофазасини таъминловчи криптографик воситаларнинг маҳаллий шароитда яратилиши иқтисодий самарали бўлиши билан бир қаторда уларнинг доимий дастурий-техник кузатуви ҳамда такомиллаштирилиб бориши таъминланади. Самарали узлуксиз шифрлаш алгоритмлари шифрлашдан ташқари ахборот хавфсизлигини таъминлашнинг бошқа барча криптографик воситаларининг (блокли шифрлаш, асимметрик шифрлаш, электрон рақамли имзо, хэш-функция) таркибида сеанс калитларини ҳосил қилиш, дастлабки тасодифий қийматлар ҳосил қилиш генератори сифатида қўлланилиши билан ахборот хавфсизлиги тизими криптобардошлигининг юқори бўлишини таъминлайди. Диссертация иши, криптографик акслантиришлари мавжуд узлуксиз шифрлаш алгоритмлари акслантиришларидан фаркли, аппарат ва аппарат-дастурий қурилмалар

яратишда қулай ва самарали амалга ошириш имкониятини берувчи, криптобардошлиги етарли даражада юқори, асосий акслантиришлари криптобардошликни янада оширилишига ҳамда аппарат воситаларини кам харж эвазига такомиллаштириш ва модернизациялаш қулайлигини таъминловчи узлуксиз шифрлаш алгоритмларини яратиш, уларнинг криптобардошлиги ва самарадорлигини баҳолаш масалалари ечимларига бағишланган.

Муаммонинг ўрганилганлик даражаси. Компьютер тармоқлари ва электрон маълумот алмашинуви технологияларининг ривожланиши, молия, банк ишлари, савдо-сотиқ каби соҳаларда қўлланилиши ахборот муҳофазасининг криптографик усулларини умумжамият фаолиятининг турли соҳаларига кенг кириб боришига сабаб бўлди.

Крипография ва узлуксиз шифрлаш соҳасидаги манбалар сифатида Шнайер Б., Вернам Г., Рюппель Р.А., Керкхоффс А.О., Зигенталер Т., Шеннон К.Е., Кнут Д.Е., Харин Ю.С., Асосков А.В., Молдовян А.А. томонидан олиб борилган тадқиқотлар келтирилиши мумкин. Шифрлаш алгоритмлари асосида аппарат ва аппарат-дастурий воситаларни яратиш устида дунёнинг кўплаб етакчи илмий тадқиқот институтлари ва компаниялари («Crypto AG» Швейцария, «Анкад» Россия, «Global Crypto» АҚШ, «RSA Data Security» АҚШ ва бошқа.) томонидан инженерлик-тадқиқот ишлари олиб борилмоқда. Олиб борилган тадқиқотлар криптографик тизимнинг криптобардошлиги унинг таркибига кирувчи алгоритмнинг махфий сақланишига боғлиқ бўлмай, фақат махфий сақланувчи калитгагина боғлиқ қилиб яратиш кераклигини келтириб чиқарди ва исботлади. Нисбатан кичик узунликка эга бўлган, яъни кафолатланган криптобардошликни таъминловчи узунликка эга калит билан бир томонлама криптографик акслантиришлар асосида, етарли даражада катта узунликдаги псевдотасодифий сонлар кетма-кетлиги гаммасини ишлаб чиқарувчи генераторлар негизида тезкор узлуксиз шифрлаш алгоритмлари, бардошли калит ва бошқа тасодифий параметрлар ишлаб чиқиш алгоритмлари яратилди.

Бу соҳада Ўзбекистон Республикаси олимлари томонидан ҳам етарли даражада илмий-тадқиқот ишлари олиб борилмоқда ва бунга Хасанов П.Ф., Арипов М.М., Каримов М.М., Акбаров Д.Е., Ғаниев С.К., Исаев Р.И., Хасанов Х.П., Ахмедова О.П., Расулов О.Х. томонидан эришилган натижаларни келтириш мумкин. Олиб борилган тадқиқотдан олинган назарий ва амалий натижаларни замонавий иқтисодиётнинг турли соҳаларида қўллаш, ахборот хавсизлигини таъминловчи аппарат ва аппарат-дастурий воситалар таркибида фойдаланиш катта аҳамиятга эга.

Ахборот хавфсизлиги тизимининг воситаларида тасодифий кетма-кетлик генераторларидан ва тезкор ишловчи аппарат-дастурий воситалардан фойдаланиш учун псевдотасодифий сонлар кетма-кетлиги генераторларини кенг ўрганиш, узлуксиз шифрлаш алгоритмларининг криптобардошлик талаблари, гамма ишлаб чиқиш хусусиятлари ва самарадорлиги чуқур таҳлил

қилиниши ва етарли даражада ўрганилиши керак.

Диссертация ишининг илмий-тадқиқот ишлари режалари билан боғлиқлиги. Ўзбекистон Республикаси Президенти фармонларида ва Хукуматининг қарор ҳамда буйрукларида мамлакатни компьютерлаштириш, ахборотлаштириш, банк, савдо-сотиқ ва бошқа қатор соҳаларда электрон маълумотнинг муҳофазасини кафолатли таъминловчи шифрлаш алгоритмларини қўллашнинг қонуний меъёрий хужжатлари асослари ишлаб чиқилиб, бу соҳадаги илмий тадқиқот ишларни жадаллаштиришни тақазо этади. Ушбу диссертация иши ҳам Ўзбекистон Республикаси Президенти И.А. Каримовнинг 2007 йил 3 апрелдаги ПҚ-614–сон «Ўзбекистон Республикасида ахборотнинг криптографик ҳимоясини ташкил этиш чора-тадбирлари тўғрисидаги» қарори йўналишида олиб борилаётган илмий тадқиқот ишларидан ҳисобланади.

Тадқиқот мақсади. Ушбу номзодлик диссертациясида олиб борилган тадқиқотнинг мақсади маълумотларнинг муҳофазасини таъминловчи аппарат ва аппарат-дастурий криптографик воситаларда қулай ҳамда самарали қўлланувчи криптобардошли узлуксиз шифрлаш алгоритмларини яратиш, уларнинг самарадорлигини баҳолаш усулларини ва дастурий таъминотларини таклиф этиш.

Тадқиқот вазифалари. Тадқиқот мақсадини амалга ошириш учун диссертация ишини бажаришда қуйидаги вазифалар қўйилди:

- мавжуд узлуксиз шифрлаш алгоритмларини ва яратиш йўналишларини туркумлаш;
- аппарат ва аппарат-дастурий криптографик воситаларида самарали қўлланувчи криптобардошли акслантиришлардан фойдаланиб узлуксиз шифрлаш алгоритмларини яратиш ва жараён босқичларининг функционал схемасини тузиш;
- яратилган алгоритмларнинг самарадорлигини баҳолаш талабларини ва усулини ишлаб чиқиш;
- яратилган узлуксиз шифрлаш алгоритмлари ва акслантиришларининг дастурий таъминотларини объектга йўналтирилган дастурлаш тилида операцион тизим (кутубхонаси, library) функцияси ифодасида яратиш;
- криптобардошлик ва самарадорликни баҳолаш усулларининг дастурий таъминотларини ишлаб чиқиш;
- яратилган алгоритмларнинг криптобардошлиги ва самарадорлиги кўрсаткичлари хақида аниқ натижаларга эришиш.

Тадқиқот объекти ва предмети. Тадқиқотнинг объекти криптографик аппарат ва аппарат-дастурий воситаларда қўлланилувчи криптобардошли узлуксиз шифрлаш алгоритмлари.

Узлуксиз шифрлаш алгоритмлари ва таркибидаги акслантиришларнинг криптографик бардошлиги, самарадорлик даражаларини баҳолаш усуллари тадқиқотнинг предмети ҳисобланади.

Тадқиқот методлари. Ушбу диссертацияда ахборотни криптографик

ҳимоялаш тизимлари назарияси, эҳтимоллар назарияси, сонлар назарияси, математик мантиқ ва комбинаторика методларидан фойдаланилган.

Тадқиқот гипотезаси. Ахборот-коммуникация тизимларидаги маълумотларнинг муҳофазасини таъминловчи аппарат ва аппарат-дастурий криптографик воситаларда қулай ҳамда самарали қўлланувчи криптобардошли узлуксиз шифрлаш алгоритмларини яратиш, криптобардошлик ва самарадорликни баҳолаш усулларини криптографик алгоритмларига қўллаш масалалари ечимларига эришиш.

Ҳимояга олиб чиқилаётган асосий ҳолатлар:

- узлуксиз шифрлаш алгоритмларини унинг таркибидаги акслантиришлар хусусиятларига кўра туркумлаш;
- узлуксиз шифрлаш алгоритмларига қўйиладиган талаблар асосида умумий криптобардошлик ва самарадорликни баҳолаш усули;
- тўртта криптобардошли узлуксиз шифрлаш алгоритмлари ҳамда узлуксиз шифр асосида ихтиёрий узунликдаги хэш-қийматли хэш-функция алгоритми;
- узлуксиз шифрлаш алгоритмларининг операцион тизим кутубхонаси qulf.dll ва дастурий таъминоти;
- криптобардошлик ва самарадорлик талабларини текшириш усулларининг дастурий таъминоти;
- яратилган узлуксиз шифрлаш алгоритмларининг самарадорлик даражалари юқорилиги Хи-квадрат мезони, қатъий кўчки самарадорлиги мезони, Буль функцияларнинг чизиқсизлик даражасини аниқлаш, псевдотасодифий сонлар кетма-кетлиги ишлаб чиқиш тезлигини аниқлаш, статистик тақсимот усуллари ва криптотахлил усулларига бардошлиги бўйича олинган натижалар.

Илмий янгилиги қуйидагилардан иборат:

- мавжуд псевдотасодифий сонлар кетма-кетлиги генераторларининг такомиллаштирилган туркуми ишлаб чиқилди;
- узлуксиз шифрлаш алгоритмларининг криптобардошлиги ва самарадорлигини баҳолаш усули ишлаб чиқилди;
- тўртта криптобардошли узлуксиз шифрлаш алгоритмлари ҳамда узлуксиз шифрлашга алгоритмига асосланган хэш-функция алгоритми яратилди;
- алгоритмларнинг криптобардошлик ва самарадорлик даражасини баҳолаш усулининг дастурий таъминотлари ишлаб чиқилди.

Тадқиқот натижаларининг илмий ва амалий аҳамияти. Мавжуд ва яратилган узлуксиз шифрлаш алгоритмларнинг криптобардошлигини баҳолаш ва тизимли тадқиқлаш диссертациянинг илмий аҳамияти ҳисобланади.

Диссертация ишининг амалий аҳамияти - яратилган узлуксиз шифрлаш алгоритмлари ва дастурий таъминотларини Ўзбекистон шароитида ишлаб чиқиладиган ишончли ва тезкор ишловчи аппарат-дастурий

криптографик воситаларида, компьютердаги маълумотларнинг махфийлигини таъминлашда фойдаланиш мумкин.

Натижаларнинг жорий қилиниши. Диссертация доирасида яратилган дастурий таъминот, qulf.dll кутубхона дастури Ўзбекистон Республикаси ер ресурслари геодезия, картография ва давлат кадастри давлат қўмитасининг «Геодезия ва картография миллий маркази»да геодезия ўлчов ишлари, картографик растр материаллари, ер, бино, иншоотлар давлат кадастри бўйича олинган маълумотларни ҳимоялашга тадбиқ этилди. Ундан ташқари Ўзбекистон Республикаси Қуролли Кучлари Академиясида ўқув жараёнида қўлланилди.

Ишнинг синовдан ўтиши. Диссертация ишида олинган натижалар:

- халқаро миқиёсда ўтказилган « International conference on IT Promotion in Asia. In conjunction with international Summit on Information and Communication technologies. ETRI/TUIT/ITIRC» илмий конференциясида маъруза қилинган ва мутахасислар томонидан муҳокама қилинган (Тошкент, ТУИТ, 2009);
- Ўзбекистон алоқа ва ахборотлаштириш Агентлиги томонидан ўтказилган «Алоқа ва ахборотлаштириш соҳасида ахборот хавфсизлиги. Муаммо ва уларнинг ечимлари» республика семинарида маъруза қилинган ва мухокамадан ўтган (Тошкент, ЎзААА, 2010).

Натижаларнинг эълон қилинганлиги. Тадқиқот давомида олинган асосий натижалар 8 та илмий ишларда акс этган бўлиб, 4-таси илмий журналларда, 1-таси халқаро конференция тезислари тўпламида чоп этилган , 1-таси Патент идорасидан олинган муаллифлик гувохномаси, 2-таси семинар тезислари тўпламида CD-дискда тарқатилган.

Диссертациянинг тузилиши ва ҳажми. Диссертация кириш, тўртта бўлим, хулоса, 109 та номдаги фойдаланилган адабиётлар руйхати ва 11 та иловадан иборат. Диссертациянинг асосий хажми 120 бет матн, 9 та жадвал ва 14 та расмдан ташкил топган.

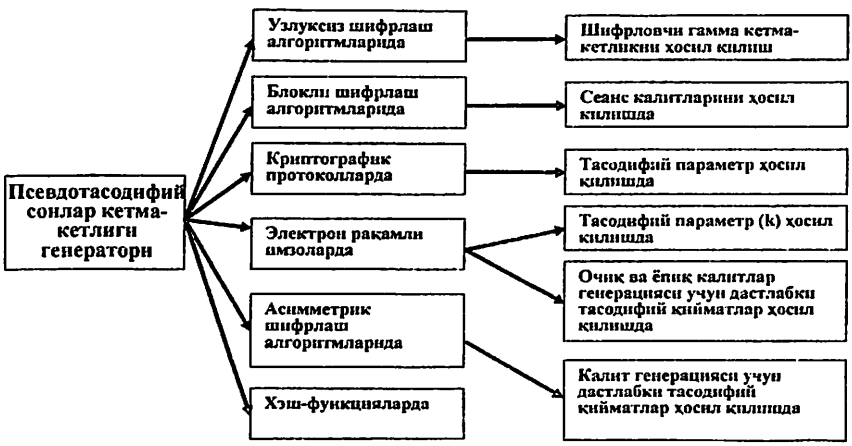
ДИССЕРТАЦИЯНИНГ АСОСИЙ МАЗМУНИ

Кириш қисмида диссертация иши мавзусининг долзарблиги, муаммонинг ўрганилганлик даражаси, тадқиқот объекти ва предмети, шунингдек, тадқиқотнинг мақсади ва вазифалари аниқланиб асослаб берилди. Илмий ишни бажаришда фойдаланилган тадқиқот методлари, тадқиқотнинг илмий янгилиги, тадқиқот натижаларининг илмий ва амалий аҳамияти, ҳимояга олиб чиқилаётган асосий ҳолатлар, тадқиқотнинг апробациядан ўтганлиги, натижаларнинг эълон қилинганлиги, диссертация ишининг тузилиши ва ҳажми тўғрисидаги ахборотлар баён этилган.

Диссертация ишининг **биринчи бўлимида** узлуксиз шифрлаш алгоритмлари, псевдотасодифий кетма-кетлик генераторлари тахлил қилиниб, улар асосида аппарат-дастурий воситаларда самарали қўлланувчи акслантиришлар ҳамда алгоритмларининг яратилиш ва қўлланилишининг

криптографик заруриятлари ёритилган. Узлуксиз шифрлаш алгоритмларини тизимли-назарий ёндашув, мураккабликка асосланган ёндашув ва комбинациялашга асосланган ёндашув йўналишида яратиш мумкин. Тизимли-назарий ёндашувда математик усуллардан фойдаланган ҳолда ечиш мураккаб бўлган математик муаммо алгоритмга асосий акслантириш қилиб олинади ва бу қийинчиликни амалий ечимлари изланади. Турли ҳил криптографик таҳлил усулларига бардошли бўлган алгоритм янги алгоритм сифатида таклиф қилинади. Мураккабликка асосланган ёндашувда мураккаб деб тан олинган катта сонларни туб кўпайтувчиларга ажратиш, дискрет логарифмлаш ва бошқа шу каби акслантиришлар асосида алгоритм яратилади. Бундай алгоритмларнинг криптобардошлиги даражаси юкорида келтирилган акслантиришларнинг мураккаблиги даражаси билан тенглаштирилади. Комбинациялаш йўналишида мавжуд бардошли алгоритмларнинг бир нечтасини биргаликда қўллаш асосида криптобардошлик оширилишига ҳаракат қилинади.

Узлуксиз шифрлаш алгоритмлари асосини псевдотасодифий кетма-кетликлар хосил қилувчи генераторлар ташкил қилади. Псевдотасодифий сонлар кетма-кетлиги генераторлари узлуксиз шифрлаш алгоритмларидан ташқари ахборот хавфсизлигининг бошқа воситаларида ҳам кенг фойдаланилади (1-расм).



1-расм. Пседотасодифий сонлар кетма-кетлиги генераторларининг қўлланиш соҳалари

Яратилган псевдотасодифий сонлар кетма-кетлиги генераторларининг хаммасини ҳам самарали ҳамда криптобардошли деб бўлмайди. Ушбу бўлимда уларни баҳолаш учун қуйидаги талаблардан иборат махсус

криптобардошлик ва самарадорликни баҳолаш усули ишлаб чиқилди:

- алгоритм акслантиришларининг соддалиги уларнинг криптографик таҳлилининг осон бўлишини таъминлаши керак;
- генератор асосидаги акслантиришларнинг умумий чизиқсизлик даражаси юқори бўлиши зарур;
- кириш параметридаги кичик ўзгаришнинг, ҳосил қилинган псевдотасодифий сонлар кетма-кетлиги элементларининг кескин ўзгаришига олиб келиши – қатъий кўчки самарадорлиги мезони юқори бўлиши керак;
- акслантиришлар умумий бир томонламалик хусусиятига эга бўлиши керак;
- ишлаб чиқилган псевдотасодифий кетма-кетлик блоклари текис статистик тақсимот кўрсаткичига эга бўлиши, яъни тасодифийлик даражаси юқори бўлиши керак;
- алгоритм таркибидаги псевдотасодифий кетма-кетлик ишлаб чиқарувчи генераторнинг акслантиришлари етарли даражадаги такрорланмас узун даврга эга бўлган кетма-кетлик ишлаб чиқишини таъминлаши зарур;
- алгоритмнинг псевдотасодифий кетма-кетлик ишлаб чиқариш ва шифрлаш тезлиги юқори бўлиши зарур;
- махфий калитни аниқлашда мумкин бўлган барча калитларни танлаб чиқиш имконияти йўқлиги;
- ҳосил қилинган кетма-кетлик ёки унинг бирор қисми бўйича калитни тиклаш имкони йўқлиги;
- ҳосил қилинган кетма-кетликнинг маълум қисмини билган ҳолда унинг қолган қисмини тиклаш имкони йўқлиги;
- дифференциал криптотаҳлил усулига бардошлиги;
- чизиқли криптотаҳлил усулига бардошлиги.

Бу ерда алгоритм қатъий кўчки самарадорлиги мезони кўрсаткичи деб бир битга $k`_1$ фарқ қилувчи ўхшаш кириш калитлари $K_1[k_1, k_2, \ldots, k_n]$ ва $K_2[k`_1, k_2, \ldots, k_n]$ орқали ҳосил қилинган $G_1[]$ ва $G_2[]$ псевдотасодифий кетма-кетликларнинг бир-биридан фарқ қилувчи мос тартибдаги битларининг миқдорига айтилади. Алгоритмнинг псевдотасодифий сонлар кетма-кетлиги ишлаб чиқиш тезлиги деб вақт бирлиги ичида ишлаб чиқилган псевдотасодифий битлар миқдорига айтилади. Бўлимда юқорида келтирилган талабларнинг таърифлари ва амалий фойдаланиш асослари келтирилган.

Иккинчи бўлимда криптографик акслантиришларнинг математик модели жегалкин кўпҳади деб аталувчи Буль функциялари орқали ифодаланиб уларнинг регулярлик, чизиқсизлик, корреляцион иммунитетлик, қатъий кўчки самарадорлиги мезони, тарқалиш каби хусусиятларини таҳлил қилиш усуллари ёритилди.

Шифрлаш алгоритмлари акслантиришларини умумий ҳолда

$$GF(2^n) = \{x = (x_1, x_2, \ldots, x_n) \in X : x_i \in \{0;1\}\} \qquad (1)$$

фазо элементларини бирор амал ёки амалларнинг чекли сондаги кетма-кетлиги орқали бошқа

$$GF(2^m) = \{y = (y_1, y_2, ..., y_m) \in Y : y_i \in \{0;1\}\} \quad (2)$$

фазо элеменларига алмаштириш деб қараш мумкин ва у Буль функция кўринишида қуйидагича ифодаланади:

$$Y = f(X) : GF(2^n) \rightarrow GF(2^m) \quad (3)$$

Буль функциялар орқали акслантиришларнинг чизиқсизлик даражаси қуйидагича аниқланади:

$$N(f) = 2^{n-1} - \frac{1}{2} \cdot \max_{\forall \alpha \in GF(2^n)} \left| U_\alpha^{\wedge}(f) \right| \quad (4)$$

Буль функциялардан фойдаланган ҳолда акслантиришларнинг чизиқсизлик, корреляцион иммуностлик, баланслашганлик, регулярлик кўрсаткичларини баҳолаш амалга оширилган.

Иккинчи бўлимда тизимли-назарий ёндашув асосида тўртта узлуксиз шифрлаш алгоритмлари яратилган бўлиб, уларнинг жараён босқичлари, кириш параметрлари, акслантиришлари ва блок-схемалари келтирилган.

Массив элементлари ўрнини алмаштиришга асосланган узлуксиз шифрлаш алгоритми асосини бир ўлчовли S-массив, икки ўлчовли ЗЖ-массиви ташкил этади.

Алгоритм таркибида (j+S[i]+K[j]) % 33 , R=ЗЖ(S[i]) – бир байтли S[i]-қийматни ЗЖ-массивидан ўтказиш орқали ярим байтли R-қийматга келтириш, S[j] <=> S[i] – S-массивнинг j-чи ва i-нчи элементлари ўрнини алмаштириш, v=L || R иккита ярим байтли (4 битли) қийматларни конкатенациясидан бир байтли V-қиймат ҳосил қилиш каби криптографик акслантиришлардан фойдаланилган.

Алгоритм жараёни босқичлари:

1. Бошланғич ҳолатда S-массив махсус сонлар билан кетма-кет тартибда тўлдирилиб чиқилади;

2. Сўнг K[ ] калит массив ёрдамида S-массивни аралаштириш амалга оширилади. Дастлабки ҳолатда i=0, j=0, j=(j+S[i]+K[i])mod33, S[i]⇔ S[j] ўрни алмаштирилади, i = (i+1) mod 33, бунда i=0 дан 33 гача ўзгаради.

3. Аралаштирилгандан сўнг ҳосил бўлган S-массив ёрдамида 2 байтли блок ҳосил қилиш амалга оширилади. i=(i+v+1)mod33, j=(j+S[i]+K[i%w]) mod33, S[i] ⇔ S[j] ўрни алмаштирилади.

4. Ҳосил қилинган S[i] ва S[j] 2 байтли блок зичлаш жадвали (ЗЖ) дан ўтказилади ва ҳосил бўлган натижа очиқ маълумотнинг 1 байтига ⊕ –XOR амали билан қўшилади. L=СЖ(S[i]) R=СЖ(S[j]), v= L||R z_n= S_v c_n=m_n ⊕ w_n. Бунда L, R –ярим байтли қиймат, c_n – шифрланган маълумот элементи, m_n – очиқ маълумот элементи, w_n – бир байтли гамма элементи.

5. Очиқ маълумот элементлари n-миқдорида алгоритмнинг 3-4 босқичлари такрорланади .

Иккинчи алгоритм **матрицали кенгайтириш ва зичлаш жадвали** акслантиришларига асосланган узлуксиз шифрлаш алгоритми бўлиб, асосини ўлчови 2^tx4 бўлган тўғри тўртбурчакли $A_{2^t x4}$ матрица ва зичлаш жадвалидан ташкил топган. Тўғри тўртбурчакли $A_{2^t x4}$ матрицанинг иккита устун элементлари пропорционал қилиб танланганлиги сабабли бу матрицага тескари бўлган матрица мавжуд эмас.

Алгоритм таркибидаги криптографик асосий акслантиришлар $A_{2^t x4}$ x $У_{j4x1}$ - 4 байтни 8 байтга кенгайтириш, w= ЗЖ(Z) – бир байтли Z-қийматни ЗЖ-массивидан ўтказиш орқали ярим байтли w қийматга келтириш кабилардан иборат бўлиб.

Алгоритм жараёни босқичлари:

1.К[ ] – 256 битли калит 4 байтли 8 та қисмга ажратилади.

2.Калитнинг ҳар бир 4 байтли қисмлари $A_{2^t x4}$ матрицага кўпайтирилиб 8 байтга кенгайтирилади.

3.Ҳар бир 8 байтли блок ЗЖ орқали 3 марта қайта зичлашлар натижасида 1 байтга келтирилиб очиқ маълумотнинг 1 байтига ⊕ XOR амали билан қўшилади.

4.Алгоритмда кўрсатилган қоида бўйича К[ ] калит массив байтлари аралаштирилиб, 1-3 босқичлар такрорланади.

Учинчи алгоритм **мантиқий функцияларга** асосланган узлуксиз шифрлаш алгоритми бўлиб, асосини тўртта 4 аргументли мантиқий функция ва ЗЖ ташкил этади. Алгоритм таркибида асосан F= f1(X,Y,Z,W) - байтлар устида мантиқий акслантириш амалини бажариш ва зичлаш акслантиришлари қўлланилган.

Алгоритм жараёни босқичлари:

К – 256 битли калит 4 байтли 8 та қисмга ажратилади;

2. Ҳар бир 4 байтли калитдан мантиқий акслантиришлар орқали 4 байтли блок ҳосил қилинади;

3. Ҳосил қилинган 4 байтли блок 2 марта ЗЖ орқали акслантирилиб, 1 байтли блок ҳосил қилинади;

4. Зичлаш натижасида олинган бир байтли блок очиқ маълумотнинг 1 байтига ⊕ –XOR амали билан қўшилади;

5.Алгоритмда кўрсатилган қонда бўйича К-калит байтлари аралаштирилиб, 1-4 босқичлар такрорланади.

Тўртинчи алгоритм **комбинациялашга асосланган** узлуксиз шифрлаш алгоритми кобинациялаш йўналиши асосида яратилган бўлиб таркибини 5 алгоритмнинг комбинацияси ташкил этади.

Умумий алгоритм жараёни босқичлари:

1. Комбинациялашган алгоритм таркибидаги 5 та генераторнинг ҳар бири учун алоҳида калит генерация қилинади. Калит генерацияси битта генератор орқали амалга оширилади.

2. Алгоритм учун танланган К[ ] (128-2048 биттача) калит массив ва битта генератордан 5 та 256 байтли гамма (1280 байт) ҳосил қилинади. Ҳар

бир алоҳида 256 байтли K_1, K_2, K_3, K_4, K_5 калитлар алгортм таркибидаги ҳар бир генератор учун алоҳида-алоҳида калитлар ҳисобланади.

3. Ҳар бир генераторнинг S-массивини алоҳида K_i калит билан аралаштириш босқичи амалга оширилади.

4. G_0 генератор ҳосил қилган гамма ҳосил қилиш босқичи амалга оширилади. Ҳосил қилинган бир байтли гамманинг охирги 2 бити қийматига караб генератор тартиби аниқланади.

5. Мос тартибдаги генератор гамма ҳосил қилиш жараёнида ҳосил қилинган гамма-байт чиқишга узатилиб очиқ маълумот билан ⊕–XOR амали билан қўшиш орқали шифрланган маълумот ҳосил қилинади.

6. Очиқ маълумот узунлиги миқдорида 4-5 босқичлар такрорланади.

Шунингдек тадқикот давомида узлуксиз шифрлаш алгоритмлари бир томонламалик талабига жавоб бериши, унинг ҳосил қилган гаммаларини билган ҳолда очиқ калитни топиш масаласининг мураккаблик даражасининг юқорилигига асосланган универсал хэш-функция алгоритми яратилди. Ҳозирги пайтда мавжуд фиксирланган хеш қийматли хэш-функциялар алгоритмлари маълумотнинг блоклари устида мураккаб итерацион жараёнлар орқали амалга оширилганлиги маълумотларни онлайн узатиш давомида хэш-қийматларини ҳисоблаш ёки имитовставка ҳосил қилишни қийинлаштириб ихтиёрий ЭРИ алгоритмлари таркибида қўллаш имкониятини чегаралайди. Бундай ҳолатларда таклиф этилган универсал хэш-функция алгоритмини қўллаш мақсадга мувофиқдир.

Яратилган тўртта узлуксиз шифрлаш алгоритмлари ахборот мухофазасига қўйиладиган талабларга кўра танлаб фойдаланиш мумкин.

3-бўлимда узлуксиз шифрлаш алгоритмларининг самарадорлигини баҳолаш асослари ёритилган. Яратилган ҳар қандай криптографик алгоритмларга қўйиладиган талаблардан бири бу алгоритм таркибидаги акслантиришларнинг мураккаб ифода ва ҳисоблашлардан ҳоли бўлишлигидан – соддалигидир. Акслантиришларнинг соддалиги ва криптографик хусусиятларнинг яққол таҳлил қилиниши алгоритмларнинг аппарат ва аппарат-дастурий воситаларда амалга ошириш қулайлигини таъминлайди. Таклиф этилган узлуксиз шифрлаш алгоритмлари таркибидаги акслантиришларнинг соддалиги уларнинг криптографик хусусиятларини тўла ва яққол таҳлил қилиш имконини беради. Узлуксиз шифрлаш алгоритмларининг криптографик самарадорлиги биринчи бўлимда келтирилган криптобардошлик ва самарадорликни баҳолаш талабларга кўра баҳоланди. Бу баҳолаш усули асосида ишлаб чиқилган algoritm_1234_tezlik.exe, anv_logic.exe, anv_xi_kvadrat.exe, matr_kengaytir.exe, qatiy_jadal_s_k.exe дастурий таъминотлар узлуксиз шифрлаш алгоритмларининг криптобардошлик ва самарадорлик кўрсаткичларини аниқ ҳисоблаш имконини беради.

Таклиф этилган узлуксиз шифрлаш алгоритмларида асосий амаллар сифатида ЗЖ(S_i) - бир байтли гаммани зичлаш жадвалидан ўтказиш,

матрицали кенгайтириш акслантириши, q= (j+S_i+K_i) mod256, mod 256 бўйича йиғинди хисоблаш акслантиришлари, мантикий функция акслантиришлари, a<<b, бир байтли «a» сонини «b» сонининг охирги 3 битига тенг бўлган кийматга циклик суриш, S_j <=> S_i - S-блокнинг S_j ва S_i элементлари ўрнини алмаштириш акслантиришлари қўлланилган.

a<<b циклик суриш акслантириши байтлар устида амалга оширилади. Ҳар бир b сонининг охирги 3 бити қиймати ҳар доим 0-7 оралиғида бўлганлиги сабабли($000_2=0_{10}$, $001_2=1_{10}$, $010_2=2_{10}$, $011_2=3_{10}$, $100_2=4_{10}$, $101_2=5_{10}$, $110_2=6_{10}$, $111_2=7_{10}$) бир байтли қийматни 8 хил ўзгартириши ёки 8 тагача ҳар хил қийматга эга бўлиши мумкин бўлган ҳолатга келтирилиши мумкин. Бу акслантириш алгоритм акслантиришларининг умумий қатъий кўчки самарадорлигини таъминлайди.

Матрицали кенгайтириш акслантириши 4 байтли маълумотни тўғри тўртбурчакли $A^{t}_{2^8\times4}$ матрицага кўпайтириш орқали амалга оширилади. Бу матрицанинг иккита устун элементлари пропорционал ва барча элементлари ҳар хил қилиб танланганлиги сабабли бу матрицага тескари бўлган матрица мавжуд эмаслиги бу акслантиришнинг бир томонламалигини таъминлайди. Матрицанинг устунлари сони 4 га тенг, қаторлар сони 4 га каррали бўлиб кириш 4 байтли қийматни неча маротаба кенгайтиришни белгилайди. Танланган матрицанинг ўлчами 4 устун ва 8 қаторга тенглиги кириш қиймат 4 байтни икки баробар кенгайтириш имконини беради. Статиктик хисоблаш натижасида хосил бўлган қийматларнинг такрорланмаслиги бу акслантиришнинг криптография нуқтаи назаридан самарадорлигини белгилайди.

ЗЖ(S_i) акслантириши бир байтли қийматни ярим байтли қийматга махсус ишлаб чиқилган жадвал асосида зичлаш акслантиришини амалга оширади. Жадвал кўриниши 16 та қатор ва 16 та устундан иборат бўлиб, умумий 256 та ярим байтли элементларнинг (қиймати 0-15 оралиғида бўлган сонларнинг) текис тақсимотидан ташкил топган. Ҳар бир кириш байтининг катта ярим байти қатор тартибини, кичик ярим байти қиймати эса устун тартибини белгилаб, улар кесишмасидаги элемент зичлаш натижаси хисобланади. Зичлаш жадвалини танлашда ҳам маълум мезонларга эътибор қилинган бўлиб, ҳар бир қаторда 0 дан 15 гача бўлган ярим байтли рақамлар бир мартадан иштирок этган. Кириш қийматининг икки баробар зичлаш натижасида кириш ва чиқиш ўртасида боғлиқлик олиб ташланиб, корреляцион мослик эхтимоллиги 1/2 эхтимолликка тенглашади. Бу эса акслантиришнинг бир томонламалигини таъминлайди.

Қатъий кўчки самарадорлиги мезони бир-бирига ўхшаш ва фақат бир битга фарқ қилувчи махфий калитлар орқали алоҳида ҳосил қилинган кетма-кетликларнинг фарқлари асосида хисобланди. Иккита бир хил калит билан ҳосил қилинган кетма-кетлик бир хил бўлади. Бу мезон иккита минимал фақат битта битга фарқ қилувчи калит орқали ҳосил қилинган кетма-кетликларнинг ўхшашлигини хисоблайди ва шу асосда хулоса қилинади.

Бу фарқларнинг ўртача 49-51% ташкил этиши қатъий кўчки

самарадорлиги мезони кўрсаткичи юқорилигини кўрсатди (1-жадвал). Хосил қилинган 8000 битли кетма-кетликларнинг ўзгарган битлар миқдори 3991 дан 4077 гача ташкил этиши ҳисобланди.

1-жадвал

Қатъий кўчки самарадорлигини ҳисоблаш натижаси

№	Алгоритм номи	Псевдотасодифий кетма-кетлик узунлиги (бит)	Ўзгарган битлар (бит)	Фонзлар хисобида
1	Массив элементлари ўрнини алмаштириш алгоритми	8000	3991	49,89 %
2	Матрицали кенгайтириш ва жадвалли зичлаш алгоритми	8000	4009	50,11 %
3	Мантиқий функцияларга асосланган алгоритми	8000	3941	49,26 %
4	Комбинациялашган алгоритм	8000	4077	50,96 %

Ҳосил қилинган псевдотасодифий кетма-кетликнинг тасодифийлик даражаси юқорилиги алгоритм ишлаб чиқарган кетма-кетлик гамма байтлари еталича узунликда файл сифатида ёзиб олиниб, Хи-квадрат мезонини қўллаш усулининг дастури асосида таҳлил қилинди. Хи-квадрат тақсимоти натижаси бошқа тақсимотлар учун етарлилик шартини таъминлаб, бошқа тақсимотларнинг ҳам қўлланиш асосини ташкил этади.

псевдотасодифий кетма-кетлик символлари деярли текис тақсимланган бўлса, етарли катта узунликдаги кетма-кетликни таҳлил қилишда символларининг ҳақиқий эҳтимоллиги ўртача эҳтимоллик қийматига якинлашиб бориши натижасида ҳисобланган Хи-квадрат мезони қиймати нолга якинлашиб боради. Бу қийматни ҳисоблаш учун кетма-кетлик таркибида маълум бир символнинг бор ёки йўқлиги ҳодиса деб олиниб, статистик ҳисоблаш амалга оширилди.

Статистик ҳисоб-китоб амалга оширилгандан сўнг ушбу формула асосида мезоннинг қиймати ҳисобланади:

$$V = \sum_{s=1}^{k} \frac{(Y_s - np_s)^2}{np_s} \qquad (5)$$

бунда, V-Хи-квадрат қиймати, Y_s – берилган кетма-кетликда s-символ учрашининг хақиқий эҳтимоллиги, n- s-символнинг учраган миқдори, p_s-символнинг учраши мумкин бўлган назарий эҳтимоллиги, s-символ индекси тартиби, k- берилган кетма кетликдаги хар-ҳил символлар миқдори.

Бу қиймат жадвалда берилган ораликлардаги қийматга мослигигига қараб тасодифийликка жавоб бериши тўғрисида хулоса қилинди. Ҳар-хил

олинган псевдотасодифий кетма-кетликлар таҳлили натижалари улар тасодифийлик даражаларини 85-100 % оралиғида бўлиши аниқланди.

Алгоритмларнинг гамма ҳосил қилиш тезлиги дастур асосида ҳисобланиб ўртача параметрли компьютерларда ўрта ва юқори тезликка эгалиги (7-90 Мбит/сек) аниқланди (2-жадвал). Бу алгоритмларни махсус процессорларда қўллаш тезликни бир-неча марта ошириш имконини беради. **Етарли даражадаги узунликда такрорланмас кетма-кетлик ишлаб чиқилишига** алгоритмларнинг таркибидаги массивларини қабул қилиши мумкин бўлган ҳолатлар $n!=(n/e)^n$ $sqrt(2\pi n)$ формула орқали ҳисобланиб, биринчи алгоритм учун $33!*256*256*256*2^{99} = 2^{1684}*256*256*256 = 2^{123}*2^{24}*2^{99} = 2^{246}$ га тенг, иккинчи алгоритм учун $2^{256}*2^8*2^3=2^{267}$, учинчи алгоритм учун $2^{256}*2^8*2^3=2^{267}$ ва тўртинчи алгоритм учун $(256!*256*256*256*2^{309})^5=2^{2020*5}= 2^{10100}$ бўлган такрорланмас давр узунлигига эгалиги ҳисобланди.

2-жадвал

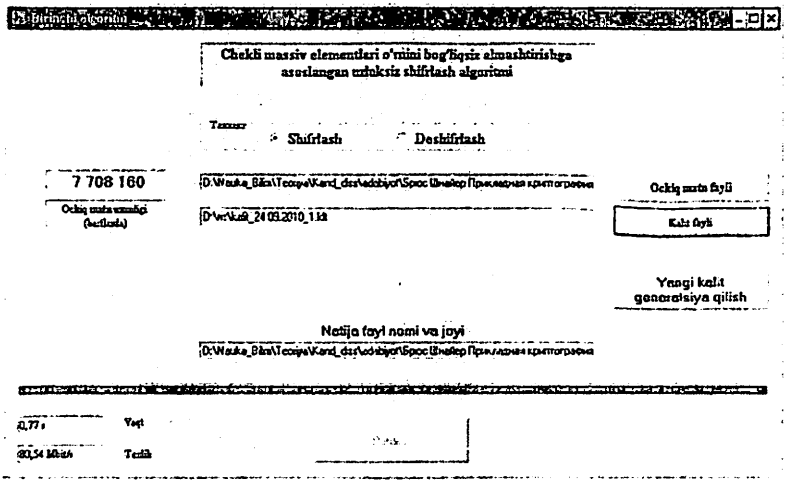
Узлуксиз шифрлаш алгоритмлари қиёсий кўрсаткичлари

	Алгоритм номи	Криптобардошлиги	Такрорланмас даври	Тезлиги
1.	Массив элементлари ўрнини алмаштириш	юқори, 2^{256}	2^{246}	Юқори, 107 Мб/с
2.	Матрицали кенгайтириш ва жадвалли зичлаш	юқори, 2^{256}	2^{267}	Ўрта, 7 Мб/с
3.	Мантиқий функцияли алгоритм	юқори, 2^{256}	2^{267}	Юқори, 24 Мб/с
4.	Комбинациялашган алгоритм	юқори, 2^{10100}	2^{10100}	Юқори, 90 Мб/с
5.	RC-4	юқори, 2^{1700}	2^{1693}	Юқори, 110 Мб/с
6.	SEAL, WAKE	ўрта, 2^{160}	2^{128}	Юқори, 50-60 Мб/с
7.	A-5, силжитиш регистрлари	кичик, 2^{64}	2^{64}	Юкори, 120 Мб/с
8.	RSA, BBS, Шамир	юқори, 2^{1024}	2^{1024}	кичик <1Мб/с
9.	ANSI X9.17, FIPS-186, YARROW-160	ўрта, 2^{128}	2^{160}	кичик, <1Мб/с

Тадқиқотнинг **4 бўлимда** амалий дастурий таъминотларни яратиш амалга оширилди. Дастурий таъминот яратиш воситаси сифатида MS Visual C# тили танланиб, шу асосда узлуксиз шифрлаш алгоритмлари ва улар таркибидаги акслантиришларнинг дастурий таъминотлари, уларнинг самарадорлигини ва криптобардошлигини баҳолаш дастурий таъминотлари

яратилди. Булар, algoritm_1.exe, algoritm_2.exe algoritm_3.exe algoritm_4.exe - узлуксиз шифрлаш алгоритмлари дастурлари, hesh_functsiya.dll - универсал хэш-функция кутубхона дастури, qulf.dll – акслантиришларнинг кутубхона дастури, algoritm_1234_tezlik.exe - тезликни аниқлаш, anv_logic.exe - Буль функциясини яратиш ва чизиқсизликка текшириш, anv_xi_kvadrat.exe - кетма-кетликларнинг тасодифийлик даражасини аниқлаш, matr_kengaytir.exe - матрицали кенгайтириш ва жадвалли зичлаш акслантиришининг статистик таксимотини аниқлаш, qatiy_jadal_s_k.exe – қатъий кўчки самарадорлигини аниқлаш дастурларидир.

Дастурларни яратиш давомида ҳар бир функция кодининг хатосиз ишлашини таъминлаш асосий ўринни эгаллайди. Дастурларни яратишда модулли дастурлаш усулидан фойдаланилган бўлиб алгоритм таркибида қўлланилган мантиқий функциялар ва жадвалли зичлаш каби 17 та криптографик акслантиришлар qulf.dll динамик кутубхона таркибига киритилган. Бу динамик кутубхона файлини ҳар қандай .NET дастурлар таркибида эркин қўллаш мумкин.



2-расм. Узлуксиз шифрлаш дастурининг кўриниши

Узлуксиз шифрлаш алгоритмлари дастурий таъминотларининг умумий кўринишига (2-расм) шифрлаш, дешифрлаш режимларини танлаш, очиқ файлни ва махфий калитни танлаш, сарфланган вақт кўрсаткичларини ҳисоблаш каби элементлардан ташкил топган. Бу дастурда компьютер файлларини узлуксиз шифрлаш алгоритмлари билан шифрлаб, уларнинг конфиденциаллигини таъминланади. Узлуксиз шифрлаш алгоритмлари дастурларидан фойдаланиш йўриқномаси диссертация иловасида тўлиқ келтирилган.

ХУЛОСА

Криптографик алгоритмларни қўллаш асосида ахборот-коммуникация тармоғида алмашинувчи рақамли маълумотларнинг муҳофазаситашкил қилиш бугунги кунда ахборот ҳавфсизлиги масалаларини ҳал қилишнинг асосий услубларидан биридир. Юқори тезликда маълумот алмашинувини талаб қилувчи ва тутилиш вақтига сезгир бўлиб, реал вақтда узатилишни талаб қилувчи овозли ва видео маълумотларнинг узатилиши давомида махфийликни узлуксиз шифрлаш орқали таъминлаш самаралидир. Ушбу тадқикот ишида олинган натижалар қуйидагилардан иборат.

1. Узлуксиз шифрлаш алгоритмларининг яратилиш йўналишлари туркумлари, алгоритмларга қўйиладиган талаблар асосида криптобардошликни баҳолаш усули ишлаб чиқилди ва бу усул дастурий ва аппарат-дастурий воситалар таркибида қўлланилган узлуксиз шифрлаш алгоритмларини аниқ баҳолаш имкониятини беради.

2. Матрицали кенгайтириш, жадвалли зичлаш ва мантиқий функцияли янги криптографик акслантиришлар ишлаб чиқилди ва бу акслантиришларни алгоритмлар таркибида асосий акслантиришлар сифатида фойдаланиш тавсия қилинади.

3. Ахборотларнинг махфийлигини таъминлаш, псевдотасодифий сонлар кетма-кетлиги ишлаб чиқиш ва аппарат-дастурий воситалар таркибида қўллаш учун қуйидаги узлуксиз шифрлаш алгоритмлари таклиф қилинди:

- массив элементлари ўрнини боғлиқсиз алмаштириш ва зичлаш жадвали ташкил этувчи узлуксиз шифрлаш алгоритми;
- матрицали кенгайтириш ва зичлаш жадвали асосидаги узлуксиз шифрлаш алгоритми;
- мантиқий функциялар асосидаги узлуксиз шифрлаш алгоритми;
- массив элементларини боғлиқсиз алмаштиришга асосланган генераторларни комбинациялаш асосида узлуксиз шифрлаш алгоритми.

4. Ахборотнинг тўлалигини таъминлаш ва ЭРИ таркибида қўлланилувчи узлуксиз шифрлаш алгоритмлари асосида яратилган универсал хэш-функция алгоритми таклиф этилди.

5. Алгоритмларнинг қатъий кўчки самарадорлиги мезони юқорилиги, чизиқсизлиги, бир томонламалиги, қисқа даврлари йўқлиги ва криптохужум турларига бардошлиги яратилган алгоритмларнинг умумий криптобардошлиги ва самарадорлиги юқорилигини тасдиқлади.

6. Яратилган узлуксиз шифрлаш алгоритмлари ҳосил қилган тасодифийлик даражалари юқори кетма-кетликлардан ахборот хавсизлиги воситалари учун бардошли калит ва бошқа тасодифий параметрлар ҳосил қилишда фойдаланиш тавсия қилинади.

7. Криптографик акслантиришларнинг кутубхона коди ва узлуксиз шифрлаш алгоритмларининг дастурий таъминоти компьютердаги файллар хавфсизлигини таъминлашда фойдаланилади.

ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ

1. Акбаров Д.Е., Мусаев А.И. Мавжуд узлуксиз шифрлаш алгоритмлари асосларини тадқиқи ва уларнинг туркумлари // Ахбороткоммуникациялар: Тармоклар -Технологиялар-Ечимлар. - Тошкент, 2009. - №1(9). - Б. 36-39.

2. Акбаров Д.Е., Мусаев А.И. Чекли майдонда матрицали кенгайтириш ва жадвалли зичлаш акслантиришларига асосланган узлуксиз шифрлаш алгоритми // Кимёвий технология:назорат ва бошқарув. - Тошкент, 2009. №3.-Б. 47-50.

3. Мусаев А.И. Криптобардошли алгоритмларни комбинациялашга асосланган узлуксиз шифрлаш алгоритми // ТАТУ хабарлари. - Тошкент, 2010. - №2. - Б.23-27.

4. Мусаев А.И. Узлуксиз шифрлаш алгоритмларидан универсал криптобардошли хэш-функция яратиш // ТАТУ хабарлари. - Тошкент, 2010. - №2. - Б. 36-38.

5. Мусаев А.И. «QULF.dll криптографик акслантиришларнинг динамик кутубхонаси» // Ўзбекистон Республикаси Давлат патент идораси. Гувохнома № DGU 02044. 26.08.2010 й.

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

7. Мусаев А.И. Узлуксиз шифрлаш алгоритмининг криптобардошлиги ва самарадорлигини баҳолаш // Алоқа ва ахборотлаштириш соҳасида ахборот хавфсизлиги. Респ.семинар тезислари материаллари. - Тошкент, 2010. - Б. 18-21.

8. Акбаров Д.Е., Камалов М.Э, Мусаев А.И. Янги ўрнига қўйиш шифрлаш алгоритми ҳамда унинг аппарат қурилмасини яратишнинг қулай ва самарали усули // Алоқа ва ахборотлаштириш соҳасида ахборот хавфсизлиги. Респ.семинар тезислари материаллари. - Тошкент, 2010. - Б. 31-32.

Техника фанлари номзоди илмий даражасига талабгор Мусаев Анвар Исаковичнинг 05.13.19 – «Ахборотларни ҳимоялаш усуллари ва тизимлари, ахборот хавфсизлиги» ихтисослиги бўйича «Узлуксиз шифрлашнинг криптобардошли алгоритмлари ва уларнинг самарадорлигини баҳолаш» мавзусидаги диссертациясининг

РЕЗЮМЕСИ

Таянч сўзлар: алгоритм, генератор, калит, псевдотасодифий, узлуксиз шифр, криптобардошлик, Буль функция, зичлаштириш жадвали, матрицали кенгайтириш.

Тадқиқот объектлари: узлуксиз шифрлаш алгоритмлари, криптобардошлик ва самарадорликни баҳолаш.

Ишнинг мақсади: узлуксиз шифрлаш алгоритмларини, криптобардошлик ва самарадорликни баҳолаш усулини яратиш ҳамда уларнинг дастурий таъминотларини ишлаб чиқиш.

Тадқиқот методлари: ахборотни криптографик ҳимоялаш тизимлари назарияси, эҳтимоллар назарияси, сонлар назарияси, математик мантиқ ва комбинаторика.

Олинган натижалар ва уларнинг янгилиги: псевдотасодифий кетма-кетлик генераторларининг туркуми ва уларни баҳолаш усули, таклиф этилган акслантиришлар асосида тўртта узлуксиз шифрлаш алгоритмлари яратилиб уларнинг криптобардошлик ва самарадорлик даражалари амалий баҳоланди.

Амалий аҳамияти: ишлаб чиқилган узлуксиз шифрлаш алгоритмлари ва псевдотасодифий кетма-кетлик генераторларини криптотизимлар таркибида ахборотнинг махфийлигини таъминлаш воситаси сифатида фойдаланиш тавсия қилинади.

Татбиқ этиш даражаси ва иқтисодий самарадорлиги: диссертация давомида олинган натижалар «Геодезия ва картография миллий маркази»да давлат кадастри ва ер ресурслари бўйича олинган маълумотларни ҳимоялашга тадбиқ этилди. Ундан ташқари Ўзбекистон Республикаси Қуролли Кучлари Академиясида ўқув жараёнида қўлланилди.

Қўлланиш (фойдаланиш) соҳаси: диссертация иши натижаларидан Республикамизнинг корхоналарида ахборот ва коммуникация тизимлари учун тезкор криптографик аппарат-дастурий воситалар яратишда, узлуксиз шифрлаш асосида яратилган барча аппарат-дастурий воситаларнинг криптобардошлик ва самарадорлигини баҳолашда фойдаланиш мумкин.

РЕЗЮМЕ

диссертации Мусаева Анвара Исаковича на тему «Криптостойкие алгоритмы поточного шифрования и оценка их эффективности» на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Ключевые слова: алгоритм, генератор, ключ, псевдослучайный, поточный шифр, криптостойкость, Булева функция, таблица сжатия, матричное расширение.

Объекты исследования: алгоритмы поточного шифрования, оценка криптостойкости и эффективности.

Цель работы: разработка алгоритмов поточного шифрования, метода оценки криптостойкости и эффективности, разработка программного обеспечения.

Методы исследования: теория систем криптографической защиты информации, теория вероятностей, теория чисел, математическая логика и комбинаторика.

Полученные результаты и их новизна: классификация генераторов псевдослучайных последовательностей и метод их оценки, на основе предложенных преобразований разработаны четыре алгоритма поточного шифрования, а также практически оценены их криптостойкость и эффективность.

Практическая значимость: разработанные алгоритмы поточного шифрования и генераторы псевдослучайных последовательностей рекомендуется использовать в составе криптосистем обеспечивающих конфиденциальности информации.

Степень внедрения и экономическая эффективность: результаты, полученные в диссертации внедрялись в «Национальный Центр картографии и геодезии» в целях защиты полученной информации государственного кадастра и земельных ресурсов, а также внедрены в учебный процесс Академии ВС РУ.

Область применения: результаты, полученные в диссертации могут быть использованы в предприятиях Республики по производству скоростных аппаратно-программных средств защиты информации в информационных и коммуникационных системах, в проведении оценки криптостойкости и эффективности аппаратно-программных средств основанных на алгоритмах поточного шифрования.

RESUME

Thesis of Musaev Anvar Isakovich on the scientific degree competition of the doctor of philosophy in technical sciences speciality 05.13.19 - «Information protecting methods and systems and information security» subject: «Cryptostrong algorithms of stream cipher and estimation of their efficiency»

Key words: algorithm, generator, key, pseudo-casual, stream cipher, crypto stability, Boolean function, table of compression, matrix expansion.

Subjects of the inquiry: algorithms of stream cipher, estimation crypto stability and efficiency.

Aim of the inquiry: development algorithms of stream cipher, methods estimation crypto stability and efficiency, development of the software.

Methods of inquiry: theory systems of cryptographic protection of information, theory of probability, theory of numbers, mathematical logic and combination theory.

The results achieved and their novelty: classification of generators of pseudo-casual sequences and a method them estimation, on the basis of the offered transformations developed four algorithms stream cipher, and also practically estimation them crypto stability and efficiency.

Practical value: developed algorithms of stream cipher can be used in cryptosystems for providing information confidentiality.

Degree of embed and economic effectivity: results gained in the dissertation, software is inculcated in the «National center of cartography and a geodesy» for protection of information state cadastre and land resource, used in educational process in Armed Forces Academy of Uzbekistan.

Sphere of usage: results gained in thesis, can be used in the enterprises and manufacturing in Republic high-speed hardware-software means for information safety in information and communication systems, estimation of crypto stability and efficiency hardware-software means based on algorithms stream cipher.

Босишга рухсат этилди 27.09.2011 й. Бичими 60x84 1/16.
Шартли босма табоғи 1. Нусхаси 100 дона. Буюртма № 284.

ТДТУ босмахонасида чоп этилди. Тошкент ш,
Талабалар кўчаси 54. тел: 246-63-84.