ЎЗБЕКИСТОН АЛОҚА ВА АХБОРОТЛАШТИРИШ АГЕНТЛИГИ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

Қўлёзма ҳуқуқида
УДК 621.391

Хасанов Хислат Пўлатович

ДИАМАТРИЦАЛАР АЛГЕБРАСИ ЭЛЕМЕНТЛАРИ АСОСИДА АХБОРОТЛАРНИ КРИПТОГРАФИК ҲИМОЯЛАШ УСУЛЛАРИ ВА АЛГОРИТМЛАРИ

05.13.19 – «Ахборотларни ҳимоялаш усуллари ва тизимлари, ахборот хавфсизлиги»

техника фанлари номзоди илмий даражасини
олиш учун тақдим этилган диссертация

АВТОРЕФЕРАТИ

Тошкент – 2010

Иш Тошкент ахборот технологиялари университетида ва Ўзбекистон алоқа ва ахборотлаштириш агентлиги «UNICON.UZ» Давлат унитар корхонаси - Фан-техника ва маркетинг тадқиқотлари марказида бажарилган

Илмий раҳбар техника фанлари доктори, профессор
Ғаниев Салим Каримович

Расмий оппонентлар: техника фанлари доктори, академик
Бекмуратов Тўлқин Файзиевич

и, доцент
бович

Етакчи ерситети

Ҳимоя ти ҳузуридаги
Д 001.25.01 ноябр
соат 12⁰⁰да
Манзил кўчаси, 108,
тел.: 238-64-1

Д ри
универс

А

...izm-otashparastlik diniga xos
...naxita)ga sig'inishi bo'lib, ibtidoiy o

RAMAZO

Turli urf-odatlar, marosim va irim
qo'shiqlar yaratilganki, bunga «Yo, ra
qochdi», «Badik», «Buka-bukavoy»,
kabilarni ko'rsatish mumkin. Shular
kalendaridagi ramazon oyidagi bola
kattalarning ham) hovlima-hovli yur
Sirdan qaraganda, «Yo, ramazon» di
o'xshasa-da, ularga xonadon egasiga
ning saxiy bo'lishi yoki baxilligi kab
«Yo, ramazon» qo'shiqlari ijro etilga
yengil yumor bilan ko'pchilik bo'lib
Bolalar uyma-uy yurib, borgan xon
bildirilgan qo'shiqlar ijro etishi bugung
«Yo ramazon» qo'shiqlari maxsus
da, o'ziga xos ohangga ega. Xalq ora
etuv-chilarga nisbatan «ramazonchilar
malar qo'llaniladi.

Ramazon qo'shiqlari o'zining ar

Ихт
ил

ДИССЕРТАЦИЯНИНГ УМУМИЙ ТАВСИФИ

Мавзунинг долзарблиги. Республикамизда сўнгги йилларда ахборот хавфсизлигини таъминлашга давлатимиз раҳбарияти томонидан катта аҳамият берилмоқда. Бунга қабул қилинган бир нечта қонун ва меъёрий ҳужжатлар, жумладан, «Электрон ҳужжат айланиши тўғрисида»ги, «Электрон рақамли имзо тўғрисида»ги қонунлар, Президентимизнинг 2007 йил 3 апрелда қабул қилган «Ўзбекистон Республикасида ахборотнинг криптографик ҳимоясини ташкил этиш чора-тадбирлари» тўғрисидаги қарори мисол бўлиши мумкин.

Ҳозирги кунга қадар ахборот хавфсизлигини таъминлашда энг ишончли воситалардан бири ахборотни криптографик ҳимоя қилиш воситалари ҳисобланади. Республикамизда бу йўналиш жадал суръатлар билан ривожланмоқда. Янгидан янги криптографик тизимлар, алгоритмлар, стандартлар ишлаб чиқилмоқда ва турли соҳаларга тадбиқ этилмоқда.

Криптографик воситаларни ишлаб чиқишда модуль арифметикасида алгебраик структуралардан кенг фойдаланилади. Булар ҳозирги кунга қадар дунёга кенг тарқалган барча криптоалгоритмлар асосида ётади. Маълумки, шифр ишлаб чиқишда дастлабки маълумотларнинг биргина элементи ўзгариши натижасида шифрматнинг барча элементлари тамомила ўзгариши жуда муҳимдир. Аммо, бу мақсадда матрицалар алгебрасидан фойдаланилганда, ҳар шифрлаш босқичида шифрматн матрицасининг фақат бир устун ёки сатр элементлари ўзгаради. Матрицавий алмаштиришлардан фойдаланишга асосланган шифрлар, масалан АҚШ стандарти AESда дастлабки маълумотлар блокининг байт сатҳидаги битта элементи ўзгарганда, биринчи босқичда аралаштириш *4* та элементнинг ўзгаришига олиб келади. Бу зарур криптобардошлиликни таъминлаш учун шифрлаш босқич(раунд)ларининг сонини кўпайтириб шифрлаш тезлигининг пасайишига олиб келади. Шу боисдан, матрицалар алгебрасини криптографик криптобардошлилик нуқтаи назаридан такомиллаштириш ва янги шифрлаш усуллари ва алгоритмларини ишлаб чиқиш долзарб муаммолар қаторига киради.

Шуни таъкидлаш лозимки, Ўзбекистон Республикаси Президенти И.А. Каримовнинг «Жаҳон молиявий иқтисодий инқирози. Ўзбекистон шароитида уни бартараф этишнинг йўллари ва чоралари» номли асарида Ўзбекистон учун инқирозни бартараф этиш ва жаҳон бозорида янги марраларга чиқишнинг ишончли йўлларидан бири инновацион технологияларни кенг жорий этиш эканлиги кўрсатиб ўтилган. Ҳозирги кунда ахборот хавфсизлигини таъминлашга қаратилган воситаларнинг аксарияти чет элдан сотиб олинади. Шунинг учун, ахборот хавфсизлигини таъминловчи воситаларни республикамизда ишлаб чиқаришни йўлга қўйиш, янги технологиялар ишлаб чиқиш, бунинг ҳисобига валютани иқтисод қилиш муҳим вазифалардан ҳисобланади.

Муаммонинг ўрганилганлик даражаси. Тадқиқот даврида ҳозирги кунда энг кўп қўлланиладиган, энг ишончли деб тан олинган ахборотнинг криптографик ҳимоялаш усулларига асосланган бир қанча шифрлаш алгоритмлари ва уларни ишлаб чиқишга асос бўлган алгебраик структура(АС)лар таҳлил қилиб чиқилди. Криптография соҳасидаги замонавий криптоалгоритмларнинг асосини ташкил этувчи бир қанча патентлар, илмий криптография асосчиси К. Шеннон ва криптография намояндалари О. Керхгофф, Ч. Беббиж, У. Фридман, Г. Вернам, Э. Хеберн, У. Диффи ва М. Хеллман, Р. Райвест, А. Шамир, Л. Адлеман, Т. Жамол, К. Шнорр, В. Миллер, Н. Коблиц, А. Менезец, Б. Шнайер, М. Молдовян, Н. Молдовян, Б. Изотов, А. Ростовцев ҳамда бошқа бир қанча олимларнинг ишлари тадқиқот давомида ўрганиб чиқилди. Ахборот хавфсизлигини таъминлаш йўналишида тадқиқот олиб бораётган ўзбек олимлари Ж.А. Абдуллаев, Т.Ф. Бекмуратов, М.М. Камилов, П.Ф. Хасанов, М.М. Арипов, С.К. Ғаниев, М.М. Каримов, Р.Х. Хамдамов, Д.Е. Акбаров, Р.И. Исаев, О.П. Ахмедова, М.Х. Назароваларнинг ишлари билан яқиндан танишиб чиқилди. Мавжуд шифрлаш алгоритмларининг қиёсий таҳлили ва криптографик миллий стандартлар ишлаб чиқиш бўйича хорижий давлатлар, шу жумладан, Россия Федерацияси, Белоруссия, Украина, Корея каби давлатларнинг тажрибаси шуни кўрсатадики, улар миллий стандарт лойиҳасини ишлаб чиқишда прототип танлашда АҚШ стандартларини асос сифатида олиб, унинг камчиликларини бартараф этувчи амаллар комбинациясидан фойдаланган ҳолда, юқори криптобардошлиликка эга бўлган ўз стандартларини яратганлар. Криптографлар амалиётида шифрлаш алгоритмларини ишлаб чиқишда асосий ўзгартиришлар сифатида *XOR*, ўрнига қўйиш, жой алмаштириш, кенгайтмали-зичламали жой алмаштириш, суриш ва матрицавий кўпайтириш амалларига асосланган акслантиришлар ҳамда модуль арифметикасининг бир томонлама функцияларидан фойдаланиш одат тусига кирган.

Мавжуд АСлар ҳозирги ахборотни криптографик ҳимоялаш алгоритмларининг бардошлилигини етарли даражада таъминлашга қодир. Аммо, криптографик тизимларнинг бардошлилигини янада ошириш мақсадида мавжуд АСларни такомиллаштириш ва янги АСлар ишлаб чиқиш бўйича изланишлар олиб бориш ҳамиша долзарб масала бўлиб қолади.

Шуни эътиборга олган ҳолда мазкур тадқиқот ишида диаматрицалар алгебраси ахборотнинг криптографик ҳимоялаш масалаларини самарали ечиш учун такомиллаштирилди ва унинг асосида махсус тузилмали диаматрицавий ва устунлар алгебраик структуралари ишлаб чиқилди. Ишлаб чиқилган алгебраик структуралар ахборотни криптографик ҳимоялашнинг янги усулини ва шифрлаш алгоритмларини яратишга асос қилиб олинди.

Диссертация ишининг илмий-тадқиқот ишлари режалари билан боғлиқлиги. Ушбу диссертация иши Ўзбекистон алоқа ва ахборотлаштириш агентлиги илмий-тадқиқот ишлари режалари доирасида Фан-техника ва

маркетинг тадқиқотлари марказининг ахборот хавфсизлиги ва криптология йўналиши бўйича С-30 - «Маълумотларни шифрлашнинг мураккаб модулли алгоритми ва дастурини ишлаб чиқиш» ва С-36 - «Ахборотни криптографик муҳофазалаш тизими бардошлилигини баҳолашнинг замонавий усулларини тадқиқ этиш. Криптографик модулларга оид хавфсизлик талабларини ишлаб чиқиш» мавзуларида олиб борилган илмий-тадқиқот ишларига мувофиқ бажарилган.

Тадқиқот мақсади. Тадқиқотни олиб боришдан асосий мақсад, диаматрицалар алгебрасини ахборотнинг криптографик ҳимоялаш масалалари учун такомиллаштириш асосида мавжуд шифрлаш алгоритмларига нисбатан криптобардошлилиги юқори бўлган ахборотни криптографик ҳимоялаш алгоритмларини ва уларни ишлаб чиқиш усулини таклиф этишдан иборат.

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

- ҳозирги кунда энг кўп қўлланиладиган, энг ишончли деб тан олинган ахборотни криптографик ҳимоялашнинг мавжуд алгоритмлари, жумладан шифрлаш алгоритмларини ва уларда фойдаланилган алгебраик амалларни таҳлил этиш;
- диаматрицалар алгебрасини ахборотнинг криптографик ҳимоялаш масалалари учун такомиллаштириш;
- ахборотни криптографик ҳимоялаш учун ишлаб чиқилган диаматрицавий устунлар алгебраик структурасини ишлаб чиқиш ва унинг хоссаларини аниқлаш;
- диаматрицалар алгебраси элементлари асосида янги криптобардошли симметрик криптоалгоритмлар, шу жумладан махфий калит алмашув алгоритмини ишлаб чиқиш;
- ишлаб чиқилган ахборотларни шифрлашнинг янги алгоритмларида дастлабки матнни тиклаш мураккаблигини баҳолаш;
- ишлаб чиқилган янги шифрлаш алгоритмлари асосида электрон ҳужжат айланиш тизими дастурий мажмуаларини ишлаб чиқиш.

Тадқиқот объекти ва предмети. Тадқиқот объекти сифатида ахборотни криптографик ҳимоялаш алгоритмлари, алгебраик структуралар, симметрик криптотизимлар ишлаб чиқиш усуллари ва алгоритмлари хизмат қилади.

Тадқиқот предмети сифатида диаматрицалар алгебраси ва шифрлаш алгоритмлари хизмат қилади.

Тадқиқот методлари. Диссертация ишида информатика асослари, ахборот-коммуникация технологиялари ва ахборотни криптографик ҳимоялаш тизимлари назариясидан, модуль арифметикаси ҳамда алгебраик структуралар асосларидан фойдаланилган.

Тадқиқот гипотезаси. Диаматрицалар алгебраси элементларини ахборотни криптографик ҳимоялаш масалалари учун такомиллаштириш янги

бир томонлама функциялар ишлаб чиқишга ва шифрлаш алгоритмларини ишлаб чиқишга янгича ёндашувларга йўл очади.

Ҳимояга олиб чиқилаётган асосий ҳолатлар:

- ахборотни криптографик ҳимоялаш масалаларини ечиш учун такомиллаштирилган диаматрицалар алгебраик структураси;
- янги амаллар асосида ишлаб чиқилган ҳамда ахборотни криптографик ҳимоялаш масалаларини ечишга йўналтирилган устунлар алгебраик структураси ва унинг хоссалари;
- диаматрицалар ва устунлар алгебраик структуралари асосида ахборотларни криптографик ҳимоялаш усули;
- ахборотларни ҳимоялашнинг янги усули асосида ишлаб чиқилган криптобардошли симметрик криптоалгоритмлар;
- ахборотларни криптографик ҳимоялаш усули асосида криптобардошлилиги юқори махфий калит алмашув алгоритми ва ҳимояланган электрон ҳужжат айланиш тизими.

Илмий янгилиги қуйидагилардан иборат:

- ахборотни криптографик ҳимоялаш масалаларини ечиш учун такомиллаштирилган диаматрицалар алгебраик структураси ишлаб чиқилган;
- ахборотни криптографик ҳимоялаш масалаларини ҳал этишга йўналтирилган устунлар алгебраик структураси ишлаб чиқилган ва унинг криптографик хоссаларини аниқланган;
- диаматрицалар ва устунлар алгебраик структуралари асосида ахборотларни криптографик ҳимоялаш усули ва янги криптобардошли симметрик криптоалгоритмлар ишлаб чиқилган;
- ахборотларни криптографик ҳимоялаш усули асосида криптобардошлилиги юқори махфий калит алмашув алгоритми ва ҳимояланган электрон ҳужжат айланиш тизими ишлаб чиқилган.

Тадқиқот натижаларининг илмий ва амалий аҳамияти. Ишлаб чиқилган алгебраик структуралар янги шифрлаш алгоритмларини ишлаб чиқишда, криптография йўналишида илмий тадқиқотлар олиб боришда ҳамда ўқув муассаларида криптография фанидан таълим беришда қўлланилиши мумкинлиги билан илмий аҳамиятга эгадир.

Тадқиқот иши патижаларидан республикамизнинг ахборот ва коммуникация тизимларида ахборотларни ҳимоялаш вазифасини ҳал қилишда, маълумотларни шифрлаш алгоритми бўйича давлат стандартини ишлаб чиқишда, ҳимояланган электрон ҳужжат айланиш, ҳимояланган электрон хат алмашув, файлларни ҳимоялаш тизимлари ишлаб чиқишда фойдаланилганлиги тадқиқотнинг амалий аҳамиятидан далолат беради.

Натижаларнинг жорий қилиниши. Тадқиқот ишининг натижаларидан O'z DSt 1105:2009 «Ахборот технологияси. Ахборотларнинг криптографик муҳофазаси. Маълумотларни шифрлаш алгоритми» давлат стандарти амалиётга жорий этилган. Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2010 йил 22 июлдаги "Республикада қоғозни тежаш ва ундан

оқилона фойдаланишга доир чора-тадбирлар тўғрисида"ги 155-сон қарорига мувофиқ, Вазирлар Маҳкамаси билан давлат ва хўжалик бошқаруви органлари, маҳаллий ижро этувчи ҳокимият органлари ўртасида «E-Xat» ҳимояланган ягона корпоратив электрон почтани ва «E-Hujjat» тизимини жорий этиш ва улардан белгиланган тартибда фойдаланиш кўзда тутилган.

Ҳозирги кунда «E-Hujjat» ҳимояланган электрон ҳужжат айланиш тизими Ўзбекистон алоқа ва ахборотлаштириш агентлиги тизимидаги бир қанча корхоналарда жумладан – «UNICON.UZ» ДУК - Фан-техника ва маркетинг тадқиқотлари маркази, Ўзимпексалоқа корхонаси, Давлат алоқа инспекцияси ва бошқаларда мувафаққиятли ишлаб турибди.

Ишнинг синовдан ўтиши. Диссертация ишидаги асосий ҳолатлар қуйидаги халқаро илмий-амалий конференциялар, республика ва халқаро семинарларида маъруза қилинган ва муҳокамадан ўтган.

- «Алоқа ва ахборотлаштириш соҳасида ахборот хавфсизлиги» республика семинарларлари (Тошкент ш. 2003 й., 2005 й., 2006 й.);
- «Алоқа ва ахборот технологияларининг ҳозирги ҳолати ва ривожланиш истиқболлари» халқаро илмий-техник конференцияси (Тошкент ш. 11-12 май 2005 й.);
- PKI-Forum-2005 ва PKI-Forum-2008 халқаро илмий-амалий конференцияларида (Санкт-Петербург ш. 2005 й., 2008 й.);
- «Инфокоммуникацияларнинг бизнес бошқарувини ривожлантиришдаги роли» республика семинари (Тошкент ш., 2008 й.);
- «Банк-молия соҳасида ахборот технологияларининг қўлланилиши» республика семинари (Тошкент ш., 2009 й.).

Натижаларнинг эълон қилинганлиги. Диссертациянинг асосий моҳияти ва мазмуни 20 та илмий ишларда акс этган. Шулардан 1 таси электрон дарслик, 2 таси патент, 9 таси журнал мақолалари, қолганлари илмий тўпламларда чоп этилган, 1 таси CD-дискда тарқатилган.

Диссертациянинг тузилиши ва ҳажми. Диссертация иши кириш қисми, 4 та бўлим, хулоса, 112 та номдаги фойдаланилган адабиётлар рўйхати ва 6 та иловадан иборат. Диссертация ишининг асосий қисми 124 варақ машина матнида ёритиб берилган ва 8 та расм ва 3 та жадвалдан иборат.

Ушбу диссертация ишини тайёрлашда услубий маслаҳатлар берган Ўзбекистонда хизмат кўрсатган фан арбоби академик Ж.А. Абдуллаевга ҳамда ўз тажрибалари ва илмий маслаҳатларини аямай кўмак берган илмий раҳбарим техника фанлари доктори, профессор С.К. Ғаниевга ўз миннатдорчилигимни билдираман.

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** ҳозирги кунда энг кўп қўлланиладиган, энг ишончли деб тан олинган ахборотни криптографик ҳимоялашнинг мавжуд алгоритмлари, жумладан шифрлаш алгоритмларининг қиёсий таҳлили ва уларда фойдаланилган алгебраик амаллар ёритиб берилган.

Ахборотларни криптографик ҳимоялашнинг мавжуд усулларини тадқиқ этиш натижасида симметрик шифрлаш усули Клод Шеннонниг фундаментал тамойиллари асосида шифрларнинг зарур криптобардошлилигини таъминлаш учун хизмат қилувчи амаллардан фойдаланишга, носимметрик усулни ишлаб чиқишда эса махфий йўлли бир томонлама осон ҳисобланадиган функциялар асосий роль ўйнаши кўрсатиб берилди.

Шифрлаш алгоритмлари бир-биридан асосан, архитектураси, алгебраик амаллар мажмуи ва модуль тури билан фарқланади. Миллий стандартлар орасида фақат АҚШ стандарти AESда полиномли модулдан, қолган алгоритмларда туб ва/ёки мураккаб модуль арифметикаси амалларидан фойдаланилади.

Криптографик миллий стандартлар ишлаб чиқиш бўйича хорижий давлатлар, масалан Россия Федерацияси ва Корея тажрибаси шуни кўрсатадики, улар миллий стандарт лойиҳасини ишлаб чиқишда прототип танлашда АҚШ стандартларини асос сифатида олиб, унинг камчиликларини бартараф этувчи амаллар комбинациясидан фойдаланган ҳолда, ўз стандартларини яратганлар.

Мавжуд маълумотларни шифрлаш алгоритмларини қиёсий таҳлил этиш ва уларни ишлаб чиқишга асос бўлган алгебраик амалларни тадқиқ этиш натижаси шуни кўрсатадики, фақат AESда матрицавий кўпайтма амалларидан фойдаланилади. Унда қўлланилган 4-тартибли матрицанинг битта элементи ўзгариши натижавий матрицада фақат тўртта элементининг ўзгаришига олиб келади. AES ҳозирги кунда криптобардошлик нуқтаи назаридан анча кучли бўлсада, янги алгебраик амаллар асосида уни янада такомиллаштириш имкони мавжуд. Алгоритмни такомиллаштиришдан асосий мақсад шифрлаш алгоритмининг криптобардошлилигини янада мустаҳкамлашдан ва бир хил криптобардошлик даражаси бўлганда ундан

тезроқ ишлай оладиган алгоритм яратишдан иборат. Шунинг учун мазкур номзодлик диссертацияси ишида AESни янги алгоритм ишлаб чиқиш учун прототип сифатида асос қилиб олиш мақсадга мувофиқ деб топилди.

Иккинчи бўлимда такомиллашган диаматрицалар алгебраси, устунлар алгебраик структураси, киритилган алгебраик амалларнинг хос ҳамда устунлар функциясининг хоссалари келтирилган. Ахборотни криптографик ҳимоялаш масалаларини ечиш учун мўлжалланган содда ва махсус тузилмали такомиллашган диаматрицалар устида бажариладиган асосий амалларни амалга ошириш алгоритмлари ёритилган.

Маълумки, диаматрицалар алгебраси 1974 йилда т.ф.д., проф. П.Ф. Хасанов томонидан чизиқли электромагнит ва электр занжирлари ҳамда тизимлари анализи ва синтези масалаларини самарали ечиш учун ишлаб чиқилган эди. Бунинг сабаби, чизиқли занжирнинг модели диаматрицалар алгебрасида бевосита акс этишидадир. Диаматрицалар алгебрасида чизиқли тенгламалар тизимини акс эттириш назарда тутилган бўлиб, диаматрицани матрицага кўпайтириш амалидан фойдаланилган эди. Лекин, криптографик масалалар учун диаматрицалар устида амаллар модуль арифметикасида бажарилиши ва натижа диаматрица шаклида бўлиши қулайдир. Шу мақсадда квадрат матрицалар устида киритилган d_l-алмаштиришни бажариш такомиллашган диаматрицалар алгебрасини шакллантиришга олиб келди.

Таъриф. $\check{D}$ – чекли, яъни, n та элементдан иборат бутун сонлар майдони устида аниқланган квадрат диаматрицалар чекли тўплами, $\Omega = \{+, ®_l, d_l, {}^{t1}, {}^{t2}, {}^{\backslash -1}, {}^{\backslash -1}, E\}$ – $\check{D}$ устида аниқланган алгебраик амаллар тўплами бўлса, $(\check{D}; \Omega)$ – жуфтлик диаматрицалар алгебраик структураси (диаматрицалар алгебраси) деб аталади; бу ерда ўзаро мос тарзда + – қўшиш, $®_l$ – кўпайтириш, $®_l \in \{®_1, ®_2\}$, d_l – алмаштириш, ^{t1}, ^{t2} – транспонирлаш, ${}^{\backslash -1}$, ${}^{\backslash -1}$ – тескарилаш амалларининг, E – бирлик элементининг рамзларидир.

Қуйида модуль n бўйича mxm-тартибли d_l – матрицалар устида кўпайтириш ифодалари келтирилган.

$$c[u,u] \equiv a[u,u]*\Sigma^{m-1}{}_{i=0}\, b[i,u] - \Sigma^{m-1}{}_{i=0,\, i\neq u}\, a[i,i]*\, b[i,u] \ (mod\ n), \qquad (1)$$

$$c[c,u]_{c\neq u} \equiv a[c,u]*\Sigma^{m-1}{}_{i=0}\, b[i,u] + b[c,u]*\Sigma^{m-1}{}_{i=0}\, a[i,u] - \Sigma^{m-1}{}_{i=0;\ i\neq c,u}\, a[c,i]*\, b[i,u] \ (mod\ n). \qquad (2)$$

Бу ерда: mxm тартибли d_l - матрицалар d_lA, d_lB, d_lC учун c-сатр ва u-устунда жойлашган элементлар мос тарзда $a[c,u]$, $b[c,u]$, $c[c,u]$, $0 \le c$, $u < m$.

Диаматрицавий кўпайтириш амали матрицавий кўпайтириш амалига нисбатан мукаммал шифрлар ишлаб чиқиш муаммоси нуқтаи назаридан қулай эканлигини илмий криптология асосчиси Клод Шеннонниг, мукаммал шифр ишлаб чиқишда ишлатиладиган алмаштиришлар яхши аралашиш ва кенг ёйилишга олиб келиши лозимлиги ҳақидаги тавсиялари кўпроқ мос келиши диссертация иловаларида келтирилган мисолларда ўз аксини топган.

Шифрлаш алгоритмларини ишлаб чиқишда махсус тузилмали диаматрицалардан фойдаланиш диаматрицалар учун унга мос матрицанинг детерминанти диаматрица элементлари бўйича содда формула орқали

ҳисобланиши, бу ўз навбатида шифрлаш ва шифрни очишда муҳим бўлган матрицаларни тескарилаш амалларини соддалаштириб бериши билан аҳамиятга молик. Шу билан бир қаторда, махсус тузилмали диаматрицанинг тескариланиш шартларини аниқлаш жараёни соддалашади. Бу эса, берилган ҳар қандай махфий шифрлаш калити асосида, мураккаб модуль бўйича тескариланиши шарт бўлган диаматрицани шакллантириш имконини яратади. Махсус тузилмали диаматрицани тескарилаш алгоритми диссертация ишида келтирилган.

Махсус тузилмали диаматрицанинг хусусий ҳоли бўлган содда тузилмали диаматрицаларга диссертация ишида алоҳида эътибор берилди.

Таъриф. Агар берилган *mxm* тартибли махсус тузилмали диаматрицанинг барча диагонал элементлари бирга тенг ва ҳар бир сатрда шу сатр учун махсус тузилмали диаматрицанинг нодиагонал элементлари бир-бирига тенг бўлса, ундай диаматрица содда тузилмали диаматрица деб аталади.

Содда тузилмали диаматрицада диагонал элемент информатив бўлмагани сабабли, у ахборот узатишда ва уни ифода этишда қатнашмайди, бироқ, ахборотга ишлов бериш жараёнларида фаол иштирок этади. Шуни ҳисобга олган ҳолда, *mxm* тартибли содда тузилмали диаматрица *dA* ни *m* элементли даматрицавий устун (қисқача, устун) $\underline{A}$ билан ифодаланса, унинг транспонирланган шакли сатр кўринишини олади:

$$\underline{A}^{t} = [a_0\, a_1\, a_2 .. \, a_{m-2}\, a_{m-1}]^{t}. \qquad (3)$$

Устунлар алгебраик структураси қуйидагича таърифланади:

Таъриф. $\hat{C}_n$ – чекли, яъни, *n* та элементдан иборат бутун сонлар тўплами устида аниқланган *m* элементли устунлар тўплами $\hat{C}_n(mx1)$, $\dot{w} = \{\circledR_3, \underline{0}, {}^{t}, {}^{-1}\}$ – $\hat{C}_n(mx1)$ устида аниқланган алгебраик амаллар тўплами бўлса, $(\hat{C}_n(mx1); \dot{w})$ – жуфтлик устунлар алгебраик структураси деб аталади; бу ерда $m>1$, $\underline{0}$ – бирлик элементи, ўзаро мос тарзда устунлар группасининг $\circledR_3$ – кўпайтириш, ^{t} – транспонирлаш, $^{-1}$ – тескарилаш амаллари рамзлари.

Устунлар устида кўпайтириш амали матрица-устунни скаляр сонга кўпайтириш амалига нисбатан мукаммал шифрлар ишлаб чиқиш муаммоси нуқтаи назаридан қулай бўлиб, яхши аралашиш ва кенг ёйилишга олиб келиши лозимлиги ҳақидаги тавсияларга жавоб беради. Кириш устунини доимий устунга кўпайтиришга асосланган шифралмаштиришларда киришда *1* та элемент ўзгариши чиқишда матрица-устунни скалярга кўпайтмаси чиқишидагига нисбатан *(m-1)*та кўп элементлар ўзгаришига олиб келиши алмаштириш босқичлари сонини камайтириш имконини беради.

Берилган устун $\underline{A}$ учун тескари устун $\underline{A}^{-1}$ билан белгиланади ва $\underline{A}^{-1}$ устун $\underline{A}$ нинг устун параметри *R* модуль *n* билан ўзаро туб бўлсагина мавжуд бўлади. Устун $\underline{A}$ учун тескари устун $\underline{A}^{-1}$ ҳосил қилиш тартиботи диссертацияда келтирилган.

Дискрет даражага оширишда худди анъанавий дискрет даражага ошириш жараёни каби даража кўрсаткичи *e* ни *2* нинг даража кийматларини

ўз ичига олган ва унга тенг бўлган йиғинди кўринишига келтирилиб, рекурсив тарзда ҳисоблашлар орқали амалга оширилади.

Масалан, *1* нинг *e=37* - даражаси қуйидагича ҳисобланади:

$1^{\backslash 37}=1^{\backslash 32+4+1}\equiv(((((1^{\backslash 2})^{\backslash 2})^{\backslash 2})^{\backslash 2})^{\backslash 2}\circledR_3(1^{\backslash 2})^{\backslash 2})\circledR_3 1 (mod\ n)$, бу ерда $1^{\backslash 2}\equiv 1+R(mod\ n)$.

Шуни таъкидлаш лозимки, устунни дискрет даражага ошириш функцияси бир томонлама функция бўлиб, у носимметрик криптотизимлар ишлаб чиқишда ҳам аҳамиятга молик.

Мультипликатив группанинг барча аксиомалари *устунлар алгебраик структурасини* ҳам қаноатлантиради.

Матрицалар алгебрасида матрица-устун тушунчаси мавжуд, бироқ, матрицавий устунлараро кўпайтириш амали мавжуд эмас. Диаматрицавий алгебрада эса диаматрицавий устунлараро кўпайтириш амали устунлар алгебраик структураси ва группасининг криптографик масалаларни ҳал этишга йўналтирилган асосий амалларидан биридир. Шу боис қуйида келтирилган устун функциясининг хоссалари ўз тамойили бўйича янги хоссалардир.

Таъриф. Модуль арифметикасида устунни даражага ошириш функцияси устун функцияси деб аталади.

1-хосса. Агар z $\varphi(n)$ билан ўзаро туб сон бўлса, унда $\underline{A}^{\backslash z+d}\equiv\underline{A}^{\backslash z}\circledR_3\underline{A}^{\backslash d}(mod\ n)$, $\underline{A}^{\backslash z}\equiv\underline{A}^{\backslash z}\circledR_3\underline{0}\ (mod\ n)$, $\underline{A}^{\backslash z}\equiv\underline{A}^{*}\ 1^{\backslash z}\ (mod\ n)$, бу ерда $\underline{A}\in\hat{C}_n(mx1)$, $\varphi(n)$ – Эйлер пи-функцияси, z, $d\in\{1,2,..., \varphi(n)-1\}$, $\circledR_3$ – модуль n бўйича устунлар устида кўпайтириш амалининг рамзи, $\underline{0}$ – бирлик элементи.

2-хосса. Агар $\underline{A}\in\hat{C}_n(mx1)$ бўлса, унда $\underline{A}^{\backslash zd}\equiv(\underline{A}^{\backslash z})^{\backslash d}\equiv(\underline{A}^{\backslash d})^{\backslash z}(mod\ n)$, бу ерда, z, $d\in\{1,2,..., \varphi(n)-1\}$.

3-хосса. $\underline{A}^{\backslash \varphi(n)+1}\equiv\underline{A}\ (mod\ n)$, $\underline{A}^{\backslash 0}=\underline{0}$, $\underline{A}^{\backslash 1}=\underline{A}$, бу ерда $\varphi(n)$ – Эйлер пи-функцияси.

4-хосса. Агар d, e $\varphi(n)$ билан ўзаро туб бўлиб, $\varphi(n)$ модули бўйича ўзаро тескари жуфтлик бўлса, унда $(\underline{A}^{\backslash d})^{\backslash e}\equiv\underline{A}\ (mod\ n)$, бу ерда $\underline{A}\in\hat{C}_n(mx1)$.

5-хосса. $\underline{A}^{\backslash x+1}\equiv\underline{A}*\Sigma^{i=x}_{i=0}R^i(mod\ n)$, бу ерда R – устун параметри, $\underline{A}^{\backslash x+1}$ – $\underline{A}$ нинг устун параметри R билан $(x+1)$ – даражаси қиймати, R^x – R нинг x-даражаси қиймати, $\Sigma^{i=x}_{i=0}R^i$ – Rнинг 0 дан x гача даражаларининг йиғиндиси.

6-хосса. Агар $a^{\backslash x}\equiv s\ (mod\ n)$ ва $aR^{-1}\equiv b\ (mod\ n)$ бўлса, унда

$R^{-1}a^{\backslash x}\equiv b^{\backslash\backslash x}(mod\ n)$, $a^{\backslash x}\equiv a^{\backslash\backslash\backslash x}(mod\ n)$,

бу ерда $^{\backslash}$ - устунлар группасида устун параметри $R=a+1$ билан даражага ошириш рамзи, $^{\backslash\backslash}$ - параметрли алгебрада $R>1$ параметр билан даражага ошириш рамзи, $^{\backslash\backslash\backslash}$ - параметрли алгебрада $R=1$ параметр билан даражага ошириш рамзи, a, b, s,R, $x\in\hat{C}_n(1x1)$.

7-хосса. $R_1^{-1}*(R_2^{-1}*a)^{\backslash x}(mod\ n)\equiv(R_1^{-1}*R_2^{-1}*a)^{\backslash\backslash x}\ (mod\ n)$, бу ерда R_1, R_2 – параметрлар, $(R_2^{-1}*a)^{\backslash x}$ – $(R_2^{-1}*a)$ нинг параметр R_2 $(mod\ n)$ билан x-даражаси қиймати, $(R_1^{-1}*R_2^{-1}*a)^{\backslash\backslash x}$ – $(R_1^{-1}*R_2^{-1}*a)$ нинг параметр $R_1*R_2\equiv$

R_1*R_2 *(mod n)* билан *x*-даражаси қиймати, R_1^{-1}, R_2^{-1} – мос тарзда R_1, R_2 нинг модуль *n* бўйича тескари қийматлари.

Юқорида келтирилган хоссалар учун $n \in \{p, p_1*p_2\}$.

Учинчи бўлимда симметрик криптографик ҳимоялаш алгоритмларини диаматрицавий алгебраик структуралар асосида яратиш усули, симметрик шифрлаш алгоритмининг асосий массивлари, диаматрицалар алгебралари амаллари асосида оддий ва функционал алмаштиришлар баён этилган. Шифрнинг псевдокоди ва алмаштиришлари ҳамда шифрлаш алгоритми алмаштиришлари бардошлилигининг баҳоси келтирилган.

Диаматрицалар ва устунлар алгебраик структуралари асосида маълумотларни криптографик ҳимоялаш усули нафақат мавжуд симметрик криптотизимларни алгебраик амаллар аналогиясидан фойдаланиб улардан кам бўлмаган криптобардошлиликка эга бўлган уларга ўхшаш криптотизимлар ишлаб чиқиш, балки махфий параметрлардан турлича фойдаланиш асосида мавжуд симметрик криптотизимларга нисбатан юқори криптобардошлиликка эга бўлган криптотизимлар ишлаб чиқиш имкониятини беради.

Мазкур усул криптотизимлар алгоритмларида анъанавий алгебраик структураларда ўрнатилган амаллар ва элементлар рамзлари сатри

+	x	$^{-1}$	$\sqrt{}^e$	*E*	*	$^{-1}$	$\sqrt{}^e$	*1*

ўрнига мос тарзда диаматрицалар ва устунлар группаси устида аниқланган амаллар ва бирлик элементлар рамзлари сатри

+	$®_2$	$^{-dI}$	^{de}	*E*	$®_3$	$^{-1}$	$^{\backslash e}$	*0*

билан алмаштириб, усулни синовдан ўтказишдан иборат.

Бу ерда иккала сатрда ҳам $\sqrt{}^e$ ни $^{\backslash e}$ га алмаштиришда бутун сонли даража кўрсатгичлари бир хил. Бинобарин, усулга биноан прототипда фойдаланилган даража кўрсатгичларига оид таққосламалар ўзгаришсиз қолади. Анъанавий даражага ошириш функциясида даража асоси чекли майдонда ҳосил қилувчи-генератор элемент (бошланғич илдиз) бўлса, уни устунлар чекли тўпламининг генератор элементи билан алмаштириш зарур.

Ишлаб чиқилган блокли симметрик шифрлаш алгоритмида *256* битга каррали узунликка эга бўлган маълумотлар учун мўлжалланган. Унда шифрлаш калити билан бир қаторда функциональ калитдан ҳамда диаматрица ва устун кўринишдаги блоклардан, улар устида амалга оширилган алмаштиришлардан фойдаланилганлиги шифрлаш алгоритмини мавжуд криптотизимлардан асосий фарқли томонларини белгилайди.

Шифрлаш криптографик модулига киритиладиган калит *256* ёки *512* бит қабул килинади.

Биринчи ҳолатда, шифрлаш криптографик модулига *256* битли калит киритилади. Бу калит тўлалигича шифрлаш калити k сифатида олинади, дастлабки сеанснинг k_f функционал калити эса, шифрлаш калитининг хэш-функцияси қиймати сифатида ҳисоблаб топилади.

Иккинчи ҳолатда, шифрлаш криптографик модулига *512* битли калит киритилади. Бу калитнинг *256* битли биринчи ярми, шифрлаш калити k сифатида олинади, унинг *256* битли иккинчи ярми биринчи сеанснинг функционал калити k_f сифатида олинади.

Юқорида кўриб ўтилган ҳолатларда жорий сеанс учун янгиланган функционал калит k_f бундан олдинги сеансда фойдаланилган функционал калит k_{f-1} нинг хэш-функцияси сифатида ҳисоблаб топилади. Хэшлаш калити сифатида қоидага кўра шифрлаш калитидан фойдаланилади, хэшлаш функциясини ҳисоблаш дастури эса маълумотларни шифрлаш алгоритми (МША)нинг дастур (ёки аппарат) таъминотига қўшиб қўйилади. Функционал калитни янгилаш даври фойдаланилаётган шифрдан фойдаланиш режими ва дастлабки маълумотларнинг махфийлик даражасини ҳисобга олган ҳолда МШАдан фойдаланадиган баённома билан белгиланади.

МША стандартидан халқаро стандартларда қабул қилинган барча блокли шифр режимларида фойдаланиш мумкин.

Шифрлаш жараёнида шифрлаш сеанси калити массиви K_s ва сеанс давомида шифрлаш босқичи калити массиви K_e дан фойдаланилади. Булар шифрлаш калити k ва функционал калит k_f асосида шакллантирилади. Шифрлаш калити k ни генерациялаш жараёнида у ва унинг иштирокида янгиланадиган функционал калитлар тўплами ҳамда улар асосида шакллантириладиган k_{se} албатта тасодифийлик мезонлари (масалан, Хи-квадрат) бўйича синовлардан ўтказилиши шарт.

Шифрда *8* та оддий шифралмаштиришлардан фойдаланилган. Улардан мавжуд шифрлаш алгоритмларида ўхшаши бўлмаганлари қуйида келтирилган.

а) *Aralash()* – оддий шифралмаштириш бўлиб, дастлабки матнни шифрматнга ва тескари йўналишда алмаштириш учун *икки вариантдан бирида* амалга оширилади; *биринчи вариантда* мазкур шифралмаштириш кириши *Holat* массивининг диаматрицавий қисмлари ҳамда K_1 ва K_2 массивлари бўлиб, чиқиши *Holat* массивидир; *иккинчи вариантда* эса шифралмаштириш кириши *8x4* тартибли *Holat* массиви ва K_{sh} ёки K_{dsh} бўлиб, чиқиши *Holat* массивидир;

b) *ShaklSeansKalitBayt()* – сеанс учун калит шакллантириш бўлиб, *икки вариантдан бирида* амалга оширилади; дастлабки матнни шифрматнга ва тескари йўналишда алмаштиришда *BaytAlmash()* ва *ShaklBosqichKalit()* шифралмаштиришларини бажариш учун фойдаланилади; мазкур шифралмаштириш кириши шифрлаш калити k ва функционал калит k_f бўлиб, чиқиши байт сатҳида чизиқли массивлар B_{sA} *[256]* ва B_{sAD} *[256]*;

c) *ShaklSeansKalit()* – сеанс учун калит шакллантириш бўлиб, дастлабки матнни шифрматнга ва тескари йўналишда алмаштиришда *Aralash()* шифралмаштиришини бажариш учун фойдаланилади; мазкур шифралмаштириш кириши байтли элементлардан таркиб топган чизиқли массив K_{sl}=*[32]* бўлиб, чиқиши *биринчи вариантда* махсус тузилмали диаматрицалардан ташкил топган (K_{1t}, K_2) ёки (K_1, K_{2t}) массивлар жуфтликларидир, *иккинчи вариантда* эса *8x4* тартибли K_{sh} ёки K_{dsh} массивидир;

d) *ShaklBosqichKalit()* – сеанс давомида сеанс-босқич калитидан босқич калитини шакллантириш бўлиб, *икки вариантдан бирида* амалга оширилади; дастлабки матнни шифрматнга ва тескари йўналишда алмаштиришда *Qo'shBosqichKalit()* алмаштиришини бажариш учун фойдаланилади; мазкур алмаштириш кириши чизиқли сеанс-босқич калити массиви k_{se}, чиқиши байт сатҳида берилган икки ўлчамли K_e*[8,4]* массивидир.

Диссертацияда электрон код китоби *(Elektron kod kitobi) m=Ekk* ва шифр блокларнинг илашиши *(ShifrBloklarning ilashishi) m=ShBil* режимларига тегишли псевдокод келтирилган.

Дастлабки матнни тиклаш мақсадида криптотаҳлилчи томонидан шифрлаш псевдокодининг тескари тариботини амалга ошириш учун шифрда фойдаланилган *(ShaklBosqichKalit, ShaklSeansKalit, ShaklSeansKalitBayt*дан бошқа) алмаштиришларнинг мураккаблик даражаси алмаштиришларнинг биринчи вариантида 2^{1144}, алмаштиришларнинг иккинчи вариантида 2^{2624} амал билан белгиланади. Албатта, бундай ҳужум усулидан фойдаланиш мақсад ва мантиққа тўғри келмайди. Бундан кўра агар шифрлаш калити *256* бит бўлса, мураккаблик даражаси 2^{256} бўлган шифрлаш калитига, агар шифрлаш калити *512* бит бўлса, мураккаблик даражаси 2^{512} бўлган шифрлаш ва функционал калитга ҳужум қилиш осонроқ туюлади. Бироқ яқин ўн йилликларда ҳисоблаш ресурслари бундай имкониятга эга бўлади деб башорат қилишга ҳали вақт етилмаган.

Аммо МШАга ҳужум қилиш учун функционал калит k_f *1÷100* сеансдан кейин янгиланиб турилиши туфайли муваффақиятли *криптотаҳлил ҳужум учун* зарур очиқ матнлар сони ниҳоятда оз бўлиши МШАга криптологияда энг эффектив ҳисобланган дифференциал, чизиқли ва дифференциал-чизиқли усуллар ёрдамида қилинадиган ҳужумлар самарасини йўққа чиқаради.

Диссертацияда маълумотларни шифрлаш алгоритмининг AESдан криптобардошликка таъсирчан фарқли томонлари эътиборга олиниб, қуйидаги жадвалда МША ва AES алгоритмларининг қиёсий таҳлили келтирилган.

Жадвал

МША ва AES алгоритмларининг қиёсий таҳлили

Кўрсаткич	МША	AES
Блок узунлиги, бит	*256*	*128*
Шифрлаш калити узунлиги, бит	*256, 512*	*128, 192, 256*
Функционал калит узунлиги, бит	*256*	-
Функционал калитнинг янгиланиш тартиби	*Сеанслар сони бўйича*	-
Функционал калитни янгилаш функцияси	*Хэш-функция*	-
Раунд калити ўзгаришининг боғлиқлиги	*Функционал калитга*	*Шифрлаш калитига*
Аралаштириш ўзгартиришида ишлатиладиган матрица тури	*Махфий; функционал калитга боғлиқ*	*Ошкора, доимий*
Байтлаб алмаштиришда фойдаланиладиган жадвал	*Махфий; функционал калит ва раундга боғлиқ*	*Ошкора, доимий*
Алмаштиришлар тўплами (шифрлаш ва шифрни очиш учун)	*Битта*	*Иккита*
Псевдокод (шифрлаш ва шифрни очиш учун)	*Битта*	*Иккита*
Алмаштиришларнинг мураккаблик даражаси	*1-вариантда - 2^{363} 2-вариантда - 2^{832}*	*2^{256}*
Шифрни бузиб очиш (секундига $4,2*10^{12}$ суперкомпьютер)	*$>3,9*10^{63}$ mips-йил*	*$< 3,9*10^{63}$ mips-йил*
Мураккаблик даражаси	*2^{2624}*	*2^{1624}*
Шифрлаш тезлиги	*56 Мбит/сек*	*75 Мбит/сек*

Диссертацияда муаллиф томонидан ишлаб чиқилган маълумотларни шифрлаш тизимидан фойдаланиш учун мўлжалланган маълумот алмашиш протоколлари келтирилган бўлиб, улар маълум протоколлардан функционал калитни ҳисоблаш қадами ва уни даврий тарзда янгилаб турилиши билан фарқланади.

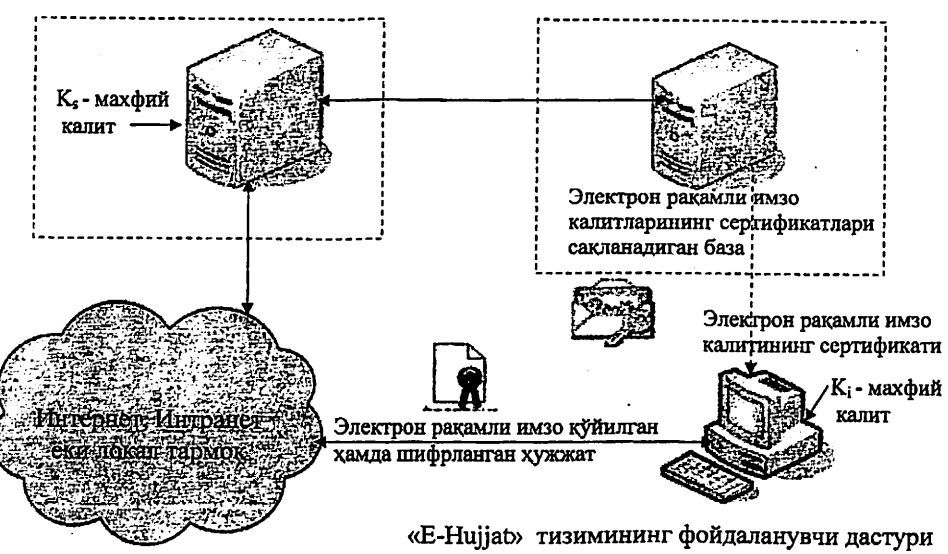
Тўртинчи бўлимда ҳозирги кунда республикамизда қўлланилиб келинаётган электрон ҳужжат айланиш тизимларининг қиёсий таҳлили, муаллиф иштирокида ишлаб чиқилган «E-Hujjat» тизимининг имкониятлари,

самарадорлиги, унда фойдаланилган махфий калит алмашув алгоритми ва аутентификация тизимининг ишлаш жараёни келтирилган.

Ҳозирги кунда республикамизда ишлаб турган тизимларнинг 10 га яқин тури мавжуд бўлиб, уларнинг асосий камчилиги электрон ҳужжатга юридик мақом бериш имконининг йўқлиги, ахборот хавфсизлиги масаласининг тўлиқ ечилмаганлиги ва кўпгина тизимларнинг фойдаланувчилар ишлатиши жараёнининг мураккаблиги ҳисобланади. Бу тизимлар ичида «Гермес» тизимида ва муаллиф томонидан таклиф этилган «E-Hujjat» тизимида ҳужжатга юридик мақом бериш имкони мавжуд. «E-Hujjat» давлат ва тижорат корхоналарида электрон ҳужжат айланиш тизимини юритиш учун мўлжалланган.

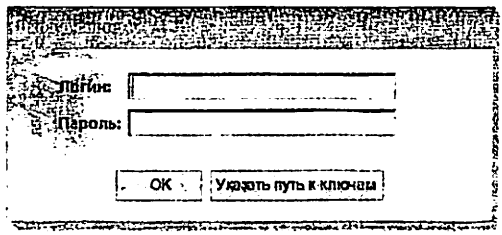
Муаллиф томонидан ишлаб чиқилган алгоритм асосида яратилган «E-Hujjat» электрон ҳужжат айланиш тизими сервер қисмидан ва фойдаланувчининг дастурий криптографик модулидан иборат бўлиб унинг инфратузилмаси қуйидаги 1-расмда келтирилган.

«E-Hujjat» тизимида муаллиф томонидан Диффи-Хеллман усулига ёндашув асосида такомиллаштирилган махфий калит алмашув алгоритмидан фойдаланилган.



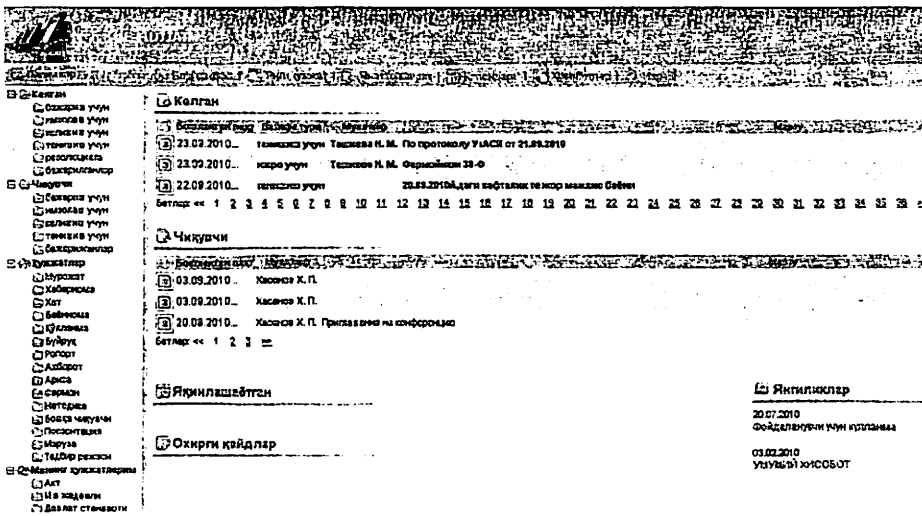
1-расм. «E-Hujjat» электрон ҳужжат айланиш тизимининг инфратузилмаси

Диссертация ишида маълумотларни шифрлаш алгоритмидан фойдаланувчини аутентификация қилиш жараёнида фойдаланиш бўйича маълумотлар келтирилган. Ушбу фойдаланувчиларни аутентификация қилиш жараёни дунёда кучли деб тан олинган Kerberos аутентификация тизимига ўхшаш бўлиб, тизимни ахборотнинг криптографик ҳимоя қилишда муаллиф томонидан ишлаб чиқилган алгоритмларнинг қўлланилганлиги билан фарқланади. «E-Hujjat» электрон ҳужжат айланиш тизимининг аутентификациялаш жараёнида логин ва парол тўғрисидаги маълумотдан ташқари, 2-расмда келтирилганидек, махфий калит сақланадиган жой ҳам кўрсатилади.



2-расм. «E-Hujjat» электрон ҳужжат айланиш тизимининг аутентификациялаш майдони

«E-Hujjat» электрон ҳужжат айланиш тизимининг умумий кўриниши 3-расмда келтирилган.



3-расм. «E-Hujjat» электрон ҳужжат айланиш тизимининг умумий кўриниши

Умуман олганда электрон ҳужжат айланиш тизимининг корхоналарда тўғри жорий қилиниши нафақат иқтисодий самара беribгина қолмай, иш юритиш ишларини такомиллаштиради. Ходимларнинг вазифаларни ўз вақтида бажариш назоратини кучайтирганлиги туфайли, уларнинг ишга бўлган муносабатини ижобий томонга ўзгартиради.

«E-Hujjat» тизими жаҳон бозоридаги мавжуд электрон ҳужжат айланиши тизимлари билан нафақат ўзининг арзонлиги билан балки функционал имкониятлари билан ҳам рақобатлаша олади ҳамда уни чет элдан кириб келаётган тизимларнинг ўрнига қўллаш катта миқдорда валютани тежаш имконини ҳам беради.

ХУЛОСА

Ушбу диссертацияда шу кунга қадар дунёда кенг тарқалган ва энг пухта деб тан олинган ахборотларни криптографик ҳимоялаш тизимлари, уларни ишлаб чиқишга асос бўлган алгебраик структуралар қисқача ёритиб берилди, қўшимча махфийлик киритишга имкон берувчи янги алгебраик структуралар ишлаб чиқишга асосий эътибор қаратилди. Натижада, такомиллашган диаматрицалар ва устунлар алгебраик структуралари, улар асосида маълумотларни криптографик ҳимоялашнинг янги усули ва алгоритмлари ишлаб чиқилди. Тадқиқот ишида олинган натижалар қуйидагилардан иборат.

1. Мавжуд шифрлаш алгоритмларининг қиёсий таҳлили ва криптографик миллий стандартлар ишлаб чиқиш бўйича хорижий давлатлар, тажрибаси шуни кўрсатадики, Ўзбекистон Республикасида криптографик давлат стандартларини ишлаб чиқиш учун прототип сифатида шифрларга қўйиладиган барча талабларга жавоб берувчи AESни асос қилиб олиш мақсадга мувофиқ.

2. Диссертация ишида диаматрицалар алгебрасини ахборотнинг криптографик ҳимоялаш масалалари учун такомиллаштириш асосида такомиллашган диаматрицалар ва устунлар алгебраик структуралари ишлаб чиқилди ҳамда улар асосида бажариладиган асосий амаллар ёритиб берилди.

3. Ишлаб чиқилган маълумотларни шифрлаш алгоритми учун шифрларга қўйиладиган барча талабларга жавоб берувчи AESни прототип сифатида олинган ҳолда такомиллашган диаматрицалар алгебрасининг криптобардошлиликни оширишга қаратилган хоссаларидан фойдаланилиш йўллари *таклиф этилди.*

4. Диссертация ишида шу нарса аниқландики, шифрлар ишлаб чиқишда анъанавий матрица-устунларга нисбатан диаматрицавий устунлардан фойдаланиш ва анъанавий матрицалар алгебраси ўрнига ёки биргаликда такомиллашган диаматрицалар алгебрасидан фойдаланиш мақсадга мувофиқдир. Бу фикрга шифралмаштиришларда киришда битта

элемент ўзгариши чиқишда матрицавий кўпайтма чиқишидагига нисбатан *1,5-1,75* марта кўп элементлар ўзгаришига олиб келиши асос бўлади. Бу хоссалар шифрлаш босқичлари сонини камайтиришга ва криптобардошлиликни оширишга хизмат қилиши *аниқланди.*

5. Диаматрицалар ва устунлар алгебраик структуралари асосида ишлаб чиқилган *маълумотларни криптографик ҳимоялаш усули* алгебраик амаллар аналогиясидан фойдаланиб нафақат криптобардошлиги етарлича юқори бўлган симметрик, балки носимметрик . криптотизимларни яратиш имкониятини бериши *аниқланди.* Ишлаб чиқилган маълумотларни шифрлаш ва махфий калитларни очиқ канал орқали алмашиш алгоритмлари бунга етарлича далил бўла олади.

6. Муаллиф томонидан ишлаб чиқилган маълумотларни шифрлаш алгоритми прототип AESдан фарқли равишда мавжуд симметрик шифрлаш криптотизимларга нисбатан самарали ҳисобланган дифференциал ва чизиқли таҳлил усулларидан фойдаланиш имкониятини йўққа чиқариб, шифр криптобардошлилигини оширишга хизмат қилади.

7. Муаллиф томонидан ишлаб чиқилган алгебраик структуралар ахборотни криптографик ҳимоялашда фойдаланиладиган мавжуд алгебраик структуралар билан бир қаторда ўзининг муносиб ўрнига эга. Олиб борилган тадқиқотлар натижасида Ўзбекистон давлат стандартининг такомиллашган янги русумига асос қилиб олинган маълумотларни шифрлаш алгоритми, «E-Hujjat» ҳимояланган электрон ҳужжат айланиш тизими ишлаб чиқилди.

8. Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2010 йил 22 июлдаги "Республикада қоғозни тежаш ва ундан оқилона фойдаланишга доир чора-тадбирлар тўғрисида"ги 155-сон қарорига мувофиқ, Вазирлар Маҳкамаси билан давлат ва хўжалик бошқаруви органлари, маҳаллий ижро этувчи ҳокимият органлари ўртасида «E-Xat» ҳимояланган ягона корпоратив электрон почтани ва «E-Hujjat» тизимини жорий этиш ва улардан белгиланган тартибда фойдаланиш кўзда тутилган. Ҳозирги кунда улардан давлат ва нотижорат корхоналарида фойдаланилмоқда.

9. Яратилган алгоритмлар асосида ишлаб чиқилган биргина «E-Hujjat» тизимининг ўзигина чет элдан валюта ҳисобига кириб келаётган тизимларнинг сонини камайтириш ҳамда уларга нисбатан 3-5 баравар арзонлиги эвазига республикамиз иқтисодиётига миллионлаб доллар фойда келтиради. «E-Hujjat» электрон ҳужжат айланиш тизимини жорий қилишнинг иқтисодий самарадорлиги назарий ҳисоб-китоблари шуни кўрсатадики, қиймати 80 минг сўм бўлган тизим танланганда, бу тизим жорий қилинган йилнинг ўзидаёқ мусбат иқтисодий самара бериши мумкин.

ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ

1. Хасанов П.Ф., Исаев Р.И., Батиров М.А., Волкович О.Г., Хасанов Х.П. Internet, Intranet va Axborot himoyasi. Электрон дарслик // CD. Тошкент, 2000, http://elamak.freenet.uz.

2. Хасанов Х.П. Критерии оценки безопасности информационных технологий // Информационная безопасность в сфере связи и информатизации: Матер. респ. сем. 3 декабря 2003. – Ташкент, 2003. – 71-76 б.

3. Хасанов Х.П. Махсус ва содда тузилмали диаматрицалар // Информатика ва энергетика муаммолари. – Тошкент, 2005, №4-5. – 71-76 б.

4. Хасанов Х.П. Такомиллаштирилган диаматрицалар алгебраси // Infocom.uz. – Тошкент, 2005, №9. – 68-70 б.

5. Хасанов П.Ф., Исаев Р.И., Хасанов Х.П., Мазгаров Б.А., Ахмедова О.П. О проектах государственного стандарта Республики Узбекистан на Алгоритм шифрования данных и Функцию хэширования // Информационная безопасность в сфере связи и информатизации: Тезисы докл. респ. сем. 24 ноября 2005 г. – Ташкент. – С. 77-80.

6. Хасанов Х.П. Диаматрицалар алгебралари асосида симметрик ва носимметрик криптотизимлар ишлаб чиқиш усуллари ва алгоритмлари // Состояние и перспективы развития связи и информационных технологий Узбекистана: Доклады и тезисы междунар.конференции 11-12 мая 2005 г. Ташкент, 2005. – С. 50-51.

7. Исаев Р.И. Хасанов Х.П. О нормативно-правовых актах по использованию электронной цифровой подписи в Республике Узбекистан // Актуальные проблемы создания системы удостоверяющих центров России. Аспекты международного сотрудничества в области ЭЦП: Тез. докл. международной научно–практической конференции PKI-Forum-2005. – Санкт-Петербург, 2005.

8. Хасанов П.Ф., Исаев Р.И., Хасанов Х.П., Назарова М.Х., Ахмедова О.П. Ахборотнинг криптографик муҳофазаси тарихи (Дастлабки ва формал криптография даври) // Aloqa dunyosi. – Тошкент, 2005. – №1 (4) – 32-37 б.

9. Хасанов П.Ф., Исаев Р.И., Хасанов Х.П., Назарова М.Х., Ахмедова О.П. Ахборотнинг криптографик муҳофазаси тарихи (Илмий криптография даври) // Aloqa dunyosi. – Тошкент, 2005, №2 (5). – 47-53 б.

10. Ўзбекистон Давлат патент идораси томонидан берилган IAP 03070-сон патенти. Рақамли имзо шакллантириш ва аутентификациялаш усули / Хасанов П.Ф., Хасанов Х.П., Хасанов Ш.П., Хасанов С.П., Хасанов З.П., Ахмедова О.П. // Расмий ахборотнома. – 2006. -№3.

11. Хасанов П.Ф., Исаев Р.И., Назарова М.Х., Хасанов Х.П., Ахмедова О.П. Ахборотнинг криптографик муҳофазаси тарихи (Компьютер криптографияси даври) // Aloqa dunyosi. – Тошкент, 2006, №1 (6). – 59-74 б.

12. Хасанов Х.П. Диаматрица устунлар ва параметрлар алгебраси // Кибернетика масалалари. – Тошкент, 2006, №173. – 93-100 б.

13. Хасанов Х.П. Актуальность развития инфраструктуры открытых ключей в Республике Узбекистан // CD «Алоқа ва ахборотлаштириш соҳасида ахборот хавфсизлиги. Муаммолар ва уларни ҳал этиш йўллари» республика семинари. – Тошкент, 2006.

14. Хасанов П.Ф., Исаев Р.И., Хасанов Х.П. Ахмедова О.П. О государственном стандарте Узбекистан на алгоритм шифрования данных // Aloqa dunyosi. – Т.: №1, 2007. – 57-71 б.

15. Ўзбекистон Давлат патент идораси томонидан берилган IAP 03416-сон патенти. Диаэкспоненциал криптографик коммуникация, аутентификация ва махфий калитлар генерацияси системасини яратиш усули / Хасанов П.Ф., Исаев Р.И., Хасанов Х.П., Назарова М.Х. Ахмедова О.П. // Расмий ахборотнома. – 2007. -№7.

16. Хасанов П.Ф., Исаев Р.И., Хасанов Х.П. Ахмедова О.П. Такомиллаштирилган хэшлаш функцияси // Ахборотқоммуникациялар: Тармоқлар – Технологиялар – Ечимлар. – Т.: №3, 2007. – 70-77 б.

17. Хасанов П.Ф., Хасанов Х.П., Ахмедова О.П., Давлатов А.Б. Параметрлар алгебраси асосида такомиллаштирилган хэшлаш функциясининг асосий амаллари ва функциялари // Ахборотқоммуникациялар: Тармоқлар – Технологиялар – Ечимлар. – Т.: №4, 2008. – 36-41 б.

18. Хасанов Х.П. Криптографические системы на основе односторонних функций диапреобразования // Шестая ежегодная международная научно-практическая конференция PKI-Forum-2008: Программа конференции и тезисы выступлений – Санкт-Петербург, 2008. – С. 29-34.

19. Хасанов Х.П. Проблемы обеспечения информационной безопасности в сфере ИКТ // Инфокоммуникацияларнинг бизнес бошқарувини ривожлантиришдаги роли - тезис материаллари тўплами: - Т. «Академия», 2008. – 204-206 б.

20. Хасанов Х.П. Диаматрица-устунлар алгебраси асосида шифрлаш алгоритми ишлаб чиқиш // Банк-молия соҳасида ахборот технологияларининг қўлланилиши - тезис материаллари тўплами: - Т. «Академия», 2009. – 164-167 б.

Ҳаммуаллифликдаги IAP 03070-сон патентида параметрли кўпайтириш амали ифодаси, IAP 03416-сон патентида калит алмашиш тизимини яратиш усули, Электрон дарсликда эса RSA тизимининг ахборотларни алмашув протоколи баёни, бошқа мақола ва маърузаларда эса криптографиянинг ривожланиши даврларига оид маълумотлар таҳлили, симметрик криптотизимларнинг қиёсий таҳлилига ва таснифига оид маълумотлар, стандартларнинг математик таъминоти баёни, тадқиқотнинг умумий вазифаларига оид маълумотлар муаллифга тегишлидир.

Техника фанлари номзоди илмий даражасига талабгор Хасанов Хислат Пўлатовичнинг 05.13.19 – «Ахборотларни ҳимоялаш усуллари ва тизимлари, ахборот хавфсизлиги» ихтисослиги бўйича «Диаматрицалар алгебраси элементлари асосида ахборотларни криптографик ҳимоялаш усуллари ва алгоритмлари» мавзусидаги диссертациясининг

РЕЗЮМЕСИ

Таянч (энг муҳим) сўзлар: алгоритм, симметрик криптотизим, калит, шифр, бардошлилик, параметр, усул, алгебраик структура, бир томонлама функция.

Тадқиқот объектлари: алгебраик структуралар, симметрик криптотизимлар ишлаб чиқиш усуллари ва алгоритмлари.

Ишнинг мақсади: диаматрица алгебраси элементлари асосида шифр ишлаб чиқиш усуллари ва алгоритмларини ишлаб чиқиш.

Тадқиқот методлари: информатика асослари, ахборот-коммуникация технологиялари, криптографик тизимлар ва матрица ҳамда диаматрицалар алгебралари усуллари.

Олинган натижалар ва уларнинг янгилиги: Ушбу диссертацияда қўшимча махфийлик киритишга имкон берувчи янги алгебраик структуралар ишлаб чиқишга асосий эътибор қаратилди. Натижада, диаматрицалар ва устунлар алгебраик структуралари, улар асосида маълумотларни шифрлаш алгоритмлари ишлаб чиқишнинг янги усули ва алгоритмлари ишлаб чиқилди.

Амалий аҳамияти: ишлаб чиқилган криптоалгоритмлар мавжуд криптотизимларга нисбатан бардошлилиги юқори бўлган криптотизимлар ишлаб чиқишда ва ўқув муассасаларида ахборот хавфсизлиги бўйича кадрлар тайёрлаш жараёнида қўлланилиши мумкинлиги билан аҳамиятга эга.

Татбиқ этиш даражаси ва иқтисодий самарадорлиги: диссертация давомида олинган натижалардан ахборотнинг криптографик муҳофазаси бўйича Ўзбекистон давлат стандартлари ишлаб чиқишда, «E-Hujjat» ҳимояланган электрон ҳужжат айланиш тизими ва ЎзААА ФТМТМ ахборот хавфсизлиги ва криптология йўналиши бўйича илмий ҳисоботларда фойдаланилган.

Қўлланиш (фойдаланиш) соҳаси: диссертация иши натижаларидан республикамизнинг ахборот ва коммуникация тизимларида ва ўқув муассасаларида фойдаланиш мумкин.

РЕЗЮМЕ

диссертации Хасанова Хислата Пулатовича на тему «Методы и алгоритмы криптографической защиты информации на основе элементов алгебры диаматриц» на соискание ученой степени кандидата технических наук по специальности 05. 13. 19 – «Методы и системы защиты информации, информационная безопасность»

Ключевые слова: алгоритм, симметричная криптосистема, ключ, шифр, стойкость, параметр, метод, алгебраическая структура, односторонняя функция.

Объекты исследования: алгебраические структуры, методы разработки симметричных криптосистем и алгоритмы шифрования.

Цель работы: разработка методов и алгоритмов создания стойких симметричных криптосистем на основе элементов алгебры диаматриц.

Методы исследования: основы информатики, информационно-коммуникационные технологии, криптографические системы и методы алгебры матриц и диаматриц.

Полученные результаты и их новизна: В диссертации основное внимание уделено разработке новых алгебраических структур с дополнительным секретом. В результате разработаны алгебраические структуры диаматриц и столбцов, а также новые методы и алгоритмы шифрования данных.

Практическая значимость: разработанные криптоалгоритмы могут быть использованы в процессах разработки криптосистем, обладающих по сравнению с известными повышенной стойкостью, а также в процессах подготовки кадров в учебных заведениях по информационной безопасности.

Степень внедрения и экономическая эффективность: результаты, полученные в диссертации, использованы в процессе разработки государственного стандарта Узбекистана по криптографической защите информации, в системе защищенной электронной документообороте «E-Hujjat» и в научных отчетах по направлениям информационной безопасности и криптологии ЦНТМИ УзАСИ.

Область применения: результаты, полученные в диссертации, могут быть использованы в информационных и коммуникационных системах республики и в процессах обучения в высших учебных заведениях.

RESUME

Thesis of Hasanov Xislat Polatovich's on the scientific degree competition of the doctor of sciences (philosophy) in 05.13.19 speciality «Information protecting methods and systems and information security» subject: «Cryptographic protection methods and algorithms on base elements of diamatrix algebra»

Key words: algorithm, symmetric cryptosystem, key, cipher, resistance, parameter, method, algebraic structure, one-way function.

Subjects of the inquire: algebraic structure, symmetric cryptosystem developing method and ciphering algorithm.

Aim of the inquire: developing methods and algorithms of creating resistant symmetric cryptosystems on base elements of diamatrix algebra.

Methods of inquire: base of informatics, information and communication technologies, cryptographic systems and matrix and diamatrix algebra methods.

The results achieved and their novelty:

In thesis main attention to developing new algebraic structures with additional secret is given. Consequently algebraic structure of diamatrix and rows and also new data encryption methods and algorithms were developed.

Practical value: developed crypto algorithms can be used in cryptosystems developing process, which have higher resistance in comparison with known and in education process by information security in institutes of education.

Degree of embed and economic effectivity: results gained in thesis used in developing process of government standards of Uzbekistan in cryptographic protection of information, in the system of secure electronic document management «E-Hujjat» and in scientific reports by information security and cryptology in SEMRC of UzACI.

Shphere of usage: results gained in thesis can be used in information and communication systems of Republic of Uzbekistan and in education process in institutes of higher education.

Босишга рухсат этилди 11.10.2010 й. Бичими 60x84 1/16.
Шартли босма табоғи 1. Нусхаси 100 дона. Буюртма № 430.

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