ЎЗБЕКИСТОН РЕСПУБЛИКАСИ
ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

ТЕРМИЗ ДАВЛАТ УНИВЕРСИТЕТИ

«МАТЕМАТИК КРИПТОГРАФИЯНИНГ АСОСЛАРИ»

фанидан

МАЪРУЗА МАТНИ

Термиз – 2008

Annotatsiya

Mazkur ishchi o`quv fan dasturi “Amaliy matematika va informatika” kursi bo`yicha tuzilgan bo`lib, talabalarga “Matematik kriptografiyasining asoslari” fanining kelib chiqishi, taraqqiyoti, jamiyat hayotida tutgan o’rni haqida ilmiy dunyo qarashni shakillantirishga yordam beradi

“Tavsiya etilgan”

«Amaliy matematika va informatika» kafedrasi majlisida muhokama qilingan va ma'qullangan.

«_____» _____ 2008 y.

Tuzuvchi: K. o`qituvchi Murodov A.N.

o`qituvchi Mengliyev Sh.A.

Taqrizchi: dotsent Ch.B.Normurodov,

Termiz davlat universiteti o`quv - metodik kengashining 2008 yil “_____ “ “____” sonli qaydnomasi bilan qayd etilgan.

@Termiz davlat universiteti

Маъруза 1
Банк ишида математик криптографиянинг асослари предмети

1. Кириш.
2. Ахборотларга нисбатан мавжуд хавфсизликларнинг асосий тушунчалари.
3. Банк автоматлаштирилган ахборот тизимларига нисбатан хавфлар.

Бугунги жамият тара==иёти инсоният тафаккурининг мащсули былган ривожланган илм-фан юту=ларига асосланган техника ва технологиялар билан бир =аторда, кенг маънода, ахборотларнинг мущим ащамиятга эгалиги билан щам белгиланади. Инсон тафаккурининг ривожи манбаи эса маълумотлар (ахборотлар) мажмуидан иборатдир. Шак-шубщасиз, ўз ва=тида олинган тыла ва ишончлп маълумот, шу маълумот билан бо\ли= былган щолатдан келиб чи=адиган амалий фаолиятларни мувофи=лаштиришда мущим ащамият касб этади. Фаолият ма=садларининг турлича былиши табиий равишда ахборотлардан турли ма=садларда фойдаланиш асосларига сабаб былади. Шунинг учун бугунги – ахборотларни са=лаш ва узатиш системалари бир томондан такомиллашиб мураккаблашган ва иккинчи томондан ахборотлардан фойдаланувчилар учун кенг =улайликлар вужудга келган даврда - ахборотларни ма=садли бош=аришнинг =атор мущим масалалари келиб чи=ади. Бундай масалалар =аторига: катта щажмдаги ахборотларни тез ва сифатли узатшш щамда =абул =илиш, ахборотларни ишончлилигини таъминлаш, ахборотлар тизимида ахборотларни бегона шахслардан мущофазалаш (кенг маънода) ва шу билан бо\ли= былган кўплаб бош=а масалалар киради. Ахборотлар ва ахборотлар тизими инсоният фаолиятининг барча сощаларига кириб, бораётган бугунги жамиятда ахборотларни ма=садли бош=ариш фаоллашмо=да. Компьютерлар ва компьютер тизимлари ахборотлар тизимининг мущим бў\имидир. ИНТЕРНЕТ тармо=лари жамият фаолиятининг барча сощаларини =ямраб олиб, ахборотларни тез ва сифатли бош=аришни таъминлаш жараёнларини ривожлантириб бормо=да. Ю=оридаги келтирилган асосли мулощазалардан келиб чи=иб, ахборотларни асли щолидан ўзгартирилган щолда, яъни шифрланган щолда, са=лаш ва узатиш масалаларининг мущим эканлигига шубща йы=дир. Ахборотларнинг мущофазаси масалалари инсоният жамиятининг =адимдан мущим масаласи бўлиб келган. Айтиш мумкинки, ахборотларни мущофазалаш услублари жамиятда дастлабки пайдо бўлган муомала тили ва ёзуви билан узвий бо\ли= ва тенгдошдир. Ща=и=атдан щам, =адимда ёзув муомала услубидан фа=ат маълум ю=ори таба=адаги жамият аъзоларигина фойдаланганлар. +адимий Миср ва Щиндистоннинг илощий китоблари бунга мисол была олади. Эрамиздан аввал бешинчи асрда яшаб

ўтган грек олими Геродотнинг щабар беришича, =адимий Мисрда шифрланган ахборотлар ролини, жрецлар, яъни ю=ори таба=адаги етук фикрли кишилар томонидан яратилган муомала тили бажарган. Бунда учта алфавитга асосланилган: ёзув, илощий ва мащфий. Ёзув алфавити оддий ўзаро муомалада кўлланилган, илощий алфавит динний муомала матнларини ифодалашда =ўлланилган, мащфий алфавит эса маълумотларни асл маъносини бегоналардан мущофаза =илишда ва астрологлар томонидан =ўлланилган.

Турли ёзув алфавитларнинг вужудга келиши ва ривожланиши на-тижасида криптография муста=ил йўналишда ривожлана борди.

Ахборотларга нисбатан мавжуд хавфсизликларнинг асосий тушунчалари

Мамлакатимиз миллий и=тисодининг щеч бир тармо\и самарали ва мытадил ташкил =илинган ахборот инфратузилмасисиз фаолият кырсатиши мумкин эмас.

Щозирги кунда миллий ахборот ресурслари щар бир давлатнинг и=тисодий ва щарбий салощиятини ташкил =илувчи омилларидан бири былиб хизмат =илмо=да. Ушбу ресурсдан самарали фойдаланиш мамлакат хвфсизлигини ва демократик ахборотлашган жамиятни муваффа=иятли шакллантиришни таъминлайди. Бундай жамиятда ахборот алмашуви тезлиги юксалади, ахборотларни йи\иш, са=лаш, =айта ишлаш ва улардан фойдаланиш быйича ил\ор ахборот - коммуникациялар технологияларини =ыллаш кенгаяди. Турли хилдаги ахборотлар худудий жойлашишидан =атъий назар бизнинг кундалик щаётимизга INTERNET хал=аро компьютер тармо\и ор=али кириб келди. Ахборотлашган жамият шу компьютерлар тармо\и ор=али тезлик билан шаклланиб бормо=да. Ахборотлар дунёсига саёщат =илишда давлат чегаралари деган тушунча йы=олиб бормо=да. Жащон компьютер тармо\и давлат бош=арувини тубдан ызгартирмо=да, яъни давлат ахборотларнинг тар=алиши механизмини бош=ара олмай =олади. Шунинг учун щам мавжуд ахборотларга но=онуний кириш, улардан фойдаланиш ва йы=отиш каби муаммолар долзарб былиб =олди. Буларнинг бири шахс, жамият ва давлатнинг ахборот хавфсизлиги даражасининг пасайишига олиб келмо=да. Давлатнинг ахборот хавфсизлигини таъминлаш муаммоси миллий хавфсизликни таъминлашнинг асосий ва ажралмас =исми былиб. Ахборот щимояси эса давлатнинг бирламчи приоритет масалаларига айланмо=да.

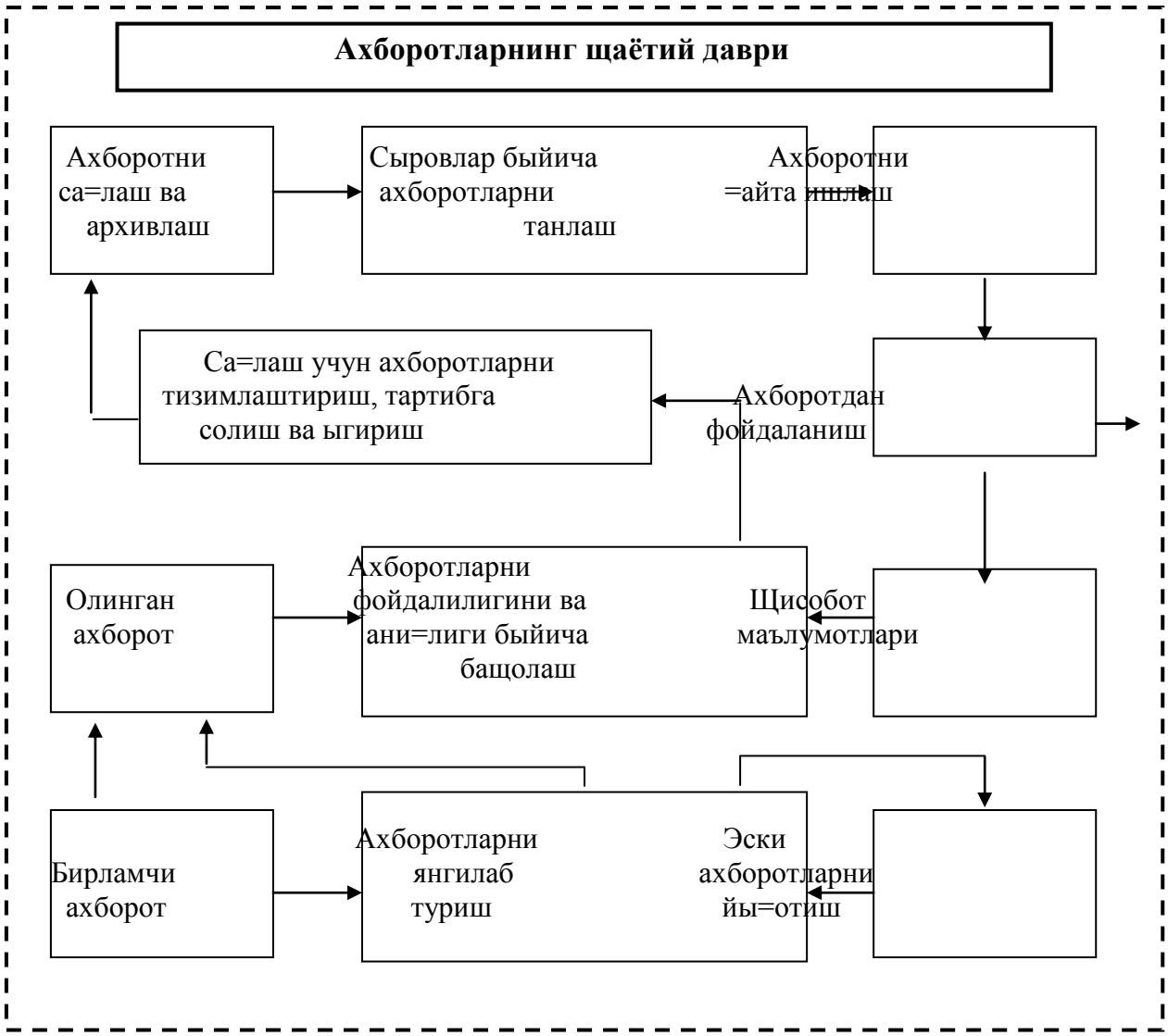
Щозирги кунда хавфсизликни бир =анча йыналишларини =айд этиш мумкин.

Предметнинг асосий тушунчалари ва ма=сади

Ахборотнинг мущимлик даражаси =адим замонлардан маълум. Шунинг учун щам =адимда ахборотни щимоялаш учун турли хил усуллар

=ылланилган. Улардан бири - сирли ёзувдир. Ундаги хабарни хабар юборилган манзил эгасидан бош=а шахс ы=ий олмаган. Асрлар давомида бу санъат - сирли ёзув жамиятнинг ю=ори таба=алари, давлатнинг элчихона резидентлари ва разведка миссияларидан таш=арига чи=маган. Фа=ат бир неча ын йил олдин щамма нарса тубдан ызгарди, яъни ахборот ыз =ийматига эга былди ва кенг тар=аладиган мащсулотга айланди. Уни эндиликда ишлаб чи=арадилар, са=лайдилар, узатишади. Сотадилар ва сотиб оладилар. Булардан таш=ари уни ы\ирлайдилар, бузиб тал=ин этадилар ва сощталаштирадилар. Шундай =илиб. Ахборотни щимоялаш зарурияти ту\илади. Ахборотни =айта ишлаш саноатининг пайдо былиши ахборотни щимоялаш саноатининг пайдо былишига олиб келади.

Автоматлаштирилган ахборот тизимларида ахборот ызининг щаётий даврига эга былади. Бу давр уни яратиш, ундан фойдаланиш ва керак былмаганда йы=отишдан иборатдир.



Ахборотлар щаётий даврининг щар бир бос=ичида уларнинг щимояланганлик даражаси турлича бащоланади.

Махфий ва =имматбащо ахборотларга рухсатсиз киришдан щимоялаш энг мущим вазифалардан бири саналади. Компьютер эгалари ва фойдаланувчиларнинг мулкий щимоялаш - бу ишлаб чи=арилаётган ахборотларни жиддий и=тисодий ва бош=а моддий щамда номоддий зарарлар келтириши мумкин былган турли киришлар ва ы\ирлашларданщимоялашдир.

Ахборот хавфсизлиги деб маълумотларни йы=отиш ва ызгартиришга йыналтирилган табиий ёки сунъий хоссали тасодифий ва =асддан таъсирлардан щар =андай ташувчиларда ахборотнинг щимояланганлигига айтилади.

Илгариги хавф фа=атгина конфиденциал (махфий) хабарлар ва щужжатларни ы\ирлаш ёки нусха олишдан иборат былса, щозирги пайтдаги хавф эса компьютер маълумотлари тыплами, электрон маълумотлар, электрон массивлардан уларнинг эгасидан рухсат сырамасдан фойдаланишдир. Булардан таш=ари, бу щаракатлардан моддий фойда олишга интилиш щам ривожланади.

Ахборотнинг щимояси деб бош=ариш ва ишлаб чи=ариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот ахборот захираларининг яхлитлилиги, ишончлилиги, фойдаланиш осонлиги ва махфийлигини таъминловчи =атъий регламентланган динамик технологик жараёнга айтилади.

Ахборотнинг эгасига, фойдаланувчисига ва бош=а шахсга зарар етказмо=чи былган но=онуний муомаладан щар =андай **щужжатлаштирилган**, яъни идентификация =илиш имконини берувчи реквизитлари =ыйилган щолда моддий жисмда =айд этилган **ахборот** щимояланиши керак.

Ахборот хавфсизлиги ну=таи назаридан ахборотни =уйидагича туркумлаш мумкин:

- **махфийлик** - ани= бир ахборотга фа=ат тегишли шахслар доирасигина кириши мумкинлиги, яъни фойдаланилиши =онуний хужжатларга мувофи= чеклаб =ыйилиб, хужжатлаштирилганлиги кафолати. Бу банднинг бузилиши **ы\ирлик** ёки **ахборотни ошкор =илиш,** дейилади;
- **конфиденциаллик** - ишончлилигини, тар=атилиши мумкин эмаслиги, махфийлиги кафолати;
- **яхлитлик** - ахборот бошлан\ич кыринишида эканлиги, яъни уни са=лаш ва узатишда рухсат этилмаган ызгаришлар =илинмаганлиги кафолати; бу банднинг бузилиши **ахборотни сохталаштириш** дейилади;
- **аутентификация** - ахборот захираси эгаси деб эълон =илинган шахс ща=и=атан щам ахборотнинг эгаси эканлигига бериладиган кафолат; бу банднинг бузилиши **хабар муаллифини сохталаштириш** дейилади;

- **аппеляция =илишлик** - етарлича мураккаб категория, лекин электрон бизнесда кент =ылланилади. Керак былганда хабарнинг муаллифи кимлигини исботлаш мумкинлиги кафолати.

Ю=оридагидек, ахборот тизимига нисбатан =уйидагича таснифни келтириш мумкин:

- **ишончлилик** - тизим меъёрий ва \айри табиий щолларда режалаштирилганидек ызини тутишлик кафолати;
- **ани=лилик** - щамма буйру=ларни ани= ва тыли= бажариш кафолати;
- **тизимга киришни назорат =илиш** - турли шахс гурущлари ахборот манбаларига щар хил киришга эгалиги ва бундай киришга чекланишлар доим бажарилишлик кафолати;
- **назорат =илиниши** - исталган пайтда дастур мажмуасининг щощлаган =исмини тыли= текшириш мумкинлиги кафолати;
- **идентификациялашни назорат =илиш** - щозир тизимга уланган мижоз ани= ызини ким деб атаган былса, ани= ыша эканлигининг кафолати;
- **=асддан бузилишларга тыс=инлик** - олдиндан келишилган меъёрлар чегарасида =асддан хато киритилган маълумотларга нисбатан тизимнинг олдиндан келишилган щолда ызини тутиши.

Ахборотни щимоялашнинг ма=садлари =уйидагилардан иборат:

◊ **ахборотнинг келишувсиз чи=иб кетиши, ы\ирланиши, йы=отилиши, ызгартирилиши, сощталаштиришларнинг олдини олиш;**

◊ шахс, жамият, давлат хавфисизлигига былган хавф хатарнинг олдини олиш;

◊ ахборотни йы= =илиш, ызгартириш, сощталаштириш, нусха кычириш, тыси=лаш быйича рухсат этилмаган щаракатларнинг олдини олиш;

◊ щужжатлаштирилган ахборотнинг ми=дори сифатида щу=у=ий тартибини таъминловчи, ахборот захираси ва ахборот тизимига щар =андай но=онуний аралашувларнинг кыринишларининг олдини олиш;

◊ ахборот тизимида мавжуд былган шахсий маълумотларнинг шахсий махфийлигини ва конфиденциаллигини са=ловчи фу=ароларнинг конституцион щу=у=ларини щимоялаш;

◊ давлат сирини, =онунчиликка мос щужжатлаштирилган ахборотнинг конфиденциаллигини са=лаш;

◊ ахборот тизимлари, технологиялари ва уларни таъминловчи воситаларини яратиш, ишлаб чи=иш ва =ыллашда субъектларнинг щу=у=ларини таъминлаш.

Ахборотларга нисбатан хавф хатарлар таснифи

Илмий ва амалий текширишлар натижаларини умумлаштириш натижасида ахборотларга нисбатан хавф-хатарларни =уйидагича таснифлаш мумкин:

Хавфсизлик сиёсатининг энг асосий вазифаларидан бири щимоя тизимида потенциал хавли жойларни =идириб топиш ва уларни бартараф этиш щисобланади.

Текширишлар шуни кырсатадики, тармо=даги энг катта хавфлар – бу рухсатсиз киришга мылжаланнган махсус дастурлар, компьютер вируслари ва дастурнинг ичига жойлаштирилган махсус кодлар былиб, улар компьютер тармо=ларининг барча объектлари учун катта хавф ту\диради.

Автоматлаштирилган ахборот тизимларида маълумотларга нисбатан хавфлар

Автоматлаштирилган ахборот тизимларида щимоялаш зарурияти

Ахборот – коммуникациялар технологияларининг оммавий равишда що\озсиз автоматлаштирилган асосда бош=арилиши сабабли ахборот хавфсизлигини таъминлаш мураккаблашиб ва мущимлашиб бормо=да. Шунинг учун щам автоматлаштирилган ахборот тизимларида ахборотни щимоялашнинг Янги замонавий технологияси пайдо былмо=да. DataQuest компаниясининг маълумотига кыра, 1996-2000 йилларда ахборот щимояси воситаларининг сотувдаги щажми 13 млрд. А+Ш долларига тенг былган.

Ахборотни щимоялаш тизими

Ахборотнинг заиф томонларини камайтирувчи ва ахборотга рухсат этилмаган киришга, унинг чи=иб кетишига ва йы=олишига тыс=инлик =илувчи ташкилий, техник, дастурий, технологик ва бош=а восита, усул ва чораларнинг комплекси – ахборотни щимоялаш тизими дейилади.

Ахборот эгалари щамда ваколатли давлат органлари шахсан ахборотнинг =имматлилиги, унинг йы=отилишидан келадиган зарар ва щимоялаш механизмининг нархидан келиб чи==ан щолда ахборотни щимоялашнинг зарурий даражаси щамда тизимнинг турини, щимоялаш усуллар ва воситаларини ани=лашлари зарур. Ахборотнинг =имматлилиги ва талаб =илинадиган щимоянинг ишончлилиги бир-бири билан бевосита бо\ли=.

Щимоялаш тизими узлуксиз, режали, марказлаштирилган, ма=садли, ани=, ишончли, комплексли, осон мукаммалаштириладиган ва кыриниши тез ызгартириладиган былиши керак. У одатда барча экстремал шароитларда самарали былиши зарур.

Ташкилотлардаги ахборотларни щимоялаш.

Ахборот щажми кичик былган ташкилотларда ахборотларни щимоялашда оддий усулларни =ыллаш ма=садга мувофи= ва самаралидир. Масалан, ы=иладиган =имматбащо =о\озларни ва электрон щужжатларни алощида гурущларга ажратиш ва ни=облаш, ушбу щужжатлар билан ишлайдиган ходимни тайинлаш ва ыргатиш, бинони =ыри=лашни ташкил этиш, хизматчиларга =имматли ахборотларни тар=атмаслик мажбуриятларини юклаш, таш=аридан келувчилар устидан назорат =илиш,

компьютерни щимоялашнинг энг оддий усулларини =ыллаш ва щоказо. Одатда, щимоялашнинг энг оддий усулларни =ыллаш сезиларли самара беради.

Мураккаб таркибли, кып сонли автоматлаштирилган ахборот тизими ва ахборот щажми катта былган ташкилотларда ахборотни щимоялаш учун щимоялашнинг мажмуали тизими ташкил =илинади. Лекин ушбу усул щамда щимоялашнинг оддий усуллари хизматчиларнинг ишига хаддан таш=ари щала=ит бермаслиги керак.

Таянч иборалар

Ахборот хавфсизлиги, ахборотни щимоялаш, ахборотга щужум =илиш, хавфсизиллка тащдидлар, махфий ахборот банкнинг автоматлаштирилган ахборот тизимлари, банк ахборотларини щимоялаш, ахборот захиралари.

Назорат саволлари

1. Ахборот хавфсизлиги деганда нимани тушунасиз?
2. Ахборотнинг щимояланишини тушунтириб беринг?
3. Банк ахборотларини щимоялашнинг асосий ма=садлари нималарни ташкил =илади?

Асосий адабиёт

1. Анохин М.И., Варнавский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. М. 1997г.

2. Брюс Шнайер. Прикладная криптография: 2– е издание. М. 2001.

3. Фомичев В.М. Дискретная математика и криптология. М. «Диалог МИФИ» 2003 г. http: ‖ www.library.mephi.ru – Библиотека МИФИ.

4. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М. «Радио и связь» 2001г.

5. Московский центр непрерывного математического образования. Материалы 1 – 9 олимпиад по криптографии. М. 2001 – 2003гг. http: ‖ www. ibc.ry./- электронная библиотека Московского Государственного Университета экономики, статистики и информатики.

6. В.А.Хорошко, А.А.Чекатков. Методы и средства защиты информации. Издательство «ЮНИОР» К. 2003.

Кушимча адабиёт

1. Анин Б. Защита компьютерной информации. Санкт – Петербург, 2002.

2. Завгородный В.И. Комплексная защита информации в компьютерных системах., М. «Логас», 2001.

3. А.В.Домашев, М.М.Грунтович, В.О.Попов, Д.И.Правиков, А.Ю.Щербаков, И.В.Ппокофьев. Программирование алгоритмов защиты информации. Учебное пособие. Издательство «Нолидж». М. 2002.

Маъруза 2

Криптология масалалари

1. Криптология. Асосий тушунчалар.
2. Симметрик ва асимметрик криптосистемалар.
3. Дастурий таъминотнинг яхлитлигини таъминлаш.

Криптография - ахборотларни аслидан ўзгартирилган щолатга ытказишларнинг математик услубларини топиш ва такомиллаштириш билан шу\улланади. Дастлабки сиситемалашган криптографик услублар эрамиз бошида, Юлий Цезарнинг иш юритиш ёзишмаларида учрайди. У бирор маълумотни мащфий щолда бирор кишига етказмо=чи бўлса, алфавитнинг биринчи щарфини алфавитнинг тыртинчи щарфи билан, иккинчиси бешинчиси билан ва щоказо шу тартибда алмаштириб матннинг асли щолатидан шифрланган матн щолатига ўтказган.

Криптографик системалар йўнашидаги изланишлар айни=са, биринчи ва иккинчи жащон уруши йиллари даврида мущим ащамият касб этди ва жадал ривожланди. Урушдан кейинги йилларда щисоблаш техникаларининг яратилиши ва такомиллашиб, инсоният фаолиятининг барча сощаларига чукур ва кенг маънода кириб бориши, криптографик услубларни табиий равишда рривожланиб ва такомиллашиб боришини та=озо этмо=да.

Криптографик услубларнинг ахборотлар тизими мущофазаси масалаларида =ўлланиши, айникса, щозирги кунда мущимдир. Ща=и=атан щам, бир томондан компьютер тизимларининг ИНТЕРНЕТ тармо=лари билан бо\ли= равишда катта щажмдаги давлат ва харбий ахамиятга эга бўлган ахборотларни щамда шу каби: и=тисодий, шахсий ва бош=а турдаги ахборотларни тез ва сифатли узатиш ва =абул =илишдаги роли ортиб бормо=да. Иккиичи томондан эса бундай ахборотларнинг кенг маънодаги мущофазасини таъминлаш масалалари мущимлашиб бормо=да.

Ахборотларнинг мущофазаси масалалари билан криптология (kryptos-махфий, 1ogos-илм) шу\улланади. Криптология ма=садалари ызаро =арама-=арши былган икки йыналишга эга - криптография ва криптоанализ.

Криптографиянинг очик матнларни шифрлаш масалаларининг математик услублари билан шугулланиши тў\рисида ю=орида айтиб ытилди.

Криптоанализ эса шифрлаш услубини (калитини ёки алгоритмини) билмаган щолда шифрланган матнниг асли холатини топиш услублари масалалари билан шу\улланади.

Щозирги замон криптографияси =уйидаги тыртта бўлимни ўз ичига олади:

1) Симметрик криптосистемалар.

2) Очи= услубга (калитга) ёки яна бош=ача айтганда очи= алгоритмга асосланган криптосистемалар.

3) Электрон имзо системалари.

4) Криптосистемаларда калитлардан фойдаланиш услубларини бош=ариш.

Криптографик услублардан фойдаланишнинг асосий йыналишлари: махфий маълумотларни ало=а канали (масалан, электрон почта) быйича узатиш, узатилган маълумотларнинг ща=и=ийлигини таъминлаш, ахборотларни (хужжатларни, маълумотлар жам\армасини) компьютерлар тизими хотираларида шифрланган щолда са=лаш ва шулар каби масалаларни ыз ичига олади.

Криптография. Асосий тушунчалар

Шундай =илиб, криптографик услублар ахборотлар матнини асли щолидан ызгартириб, фа=ат калитни билган щолдагина уни асли щолатини олиш имкониятини беради.

Шифрланган ва дешифрланган масалаларига тегишли былган, маълум бир алфавитда тузилган маълумотлар матнларни ташкил этади.

Алфавит – ахборотларни кодлаштириш учун фойдаланиладиган чекли сондаги белгилар тыплами. Мисоллар сифатида:

- ыттиз олтита белгидан (щарфдан) иборат ызбек тили алфавити;
- ыттиз иккита белгидан (щарфдан) иборат рус тили алфавити;
- йигирма саккизта белгидан (щарфдан) иборат лотин алфавити;
- икки юз элик олтита белгидан иборат ASCII ва КОИ-8 стандарт компьютер кодларининг алфавити;
- бинар алфавит, яъни 0 ва 1 белгилардан иборат былган алфавит;
- саккизлик ва ын олтилик сано= системалари белгидаридан иборат былган алфавитларни келтириш мумкин.

Матн – алфавитнинг элементларидан (белгиларидан) ташкил топган тартибланган тузилма.

Шифрланган – очи= матн деб аталувчи дастлабки матнни шифрланган матн щолатига ытказиш жараёни.

Дешифрлаш – шифрлашга тескари былган жараён, яъни калит ёрдамида шифрланган матнни дастлабки матн щолатига ытказиш.

Калит – бевосита дастлабки матнни шифрлаш ва дешифрлаш учун зарур былган маълумот.

Криптографик система – очи= матнни шифрлаш (дешифрлаш) жараёнини ташкил этувчи амаллар мажмуи былиб, алфавитлар белгиларини алмаштиришлар кетма-кетлигидан иборат.

Криптоистема икки =исмга былинади: симметрик ва очи= калитли (услубли).

Симметрик криптосистемаларда шифрлаш учун щам ва дешифрлаш учун щам бир хил калит (услубдан) фойдаланилади.

Очи= калитли криптосистемаларда иккита калитдан фойдаланилади – ызаро математик бо\ли= былган очи= ва ёпи= калитлардан. Бунда маълумотлар щаммага маълум былган очи= калит билан шифрланади ва фа=ат маълумот юборилаётган шахсга маълум былган ёпи= калит билангина дешифрланади.

Калитларни та=симлаш ва калитларни бош=ариш – калитларни фойдаланувчилар орасида та=симлаш ва шу калитларни яратиш жараёнларини ыз ичига олади.

Электрон (ра=ам) имзо – матнга илова =илинадиган криптографик алмаштиришдан иборат былиб, шу матн жынатилган шахсга матннинг ща=и=ий ёки ноща=и=ий эканлигини ани=лаш имконини беради.

Криптобардошлик – шифрлаш калити номаълум былган щолда шифрланган матннинг дешифрлашни =ийинлик даражасини белгилайди. Криптобардошликни белгиловчи бир – нечта кырсаткичлар мавжуд, булардан:

- дешифрлаш учун =идирилаётган калитларннг мумкин былган барча имкониятлари сони;
- дешифрлаш учун зарур былган ыртача ва=т.

Ахборотларни мущофазалаш ма=садида шифрлашнинг сифати калитнинг махфий са=ланиши ва шифрлашнинг криптобардошлилик даражасига бо\ли=.

Симметрик ва асимметрик криптосистемалар

+адимги шифрлаш услублари щар хил жадвалларга асосланган былиб, бу жадваллар маълумотлар матнидаги алфавит белгиларининг маълум тартибдаги ырин алмаштиришларини ифодаловчи оддий амаллардан иборат былган. Бунда калит вазифасини жадвалнинг ылчами, алфавит белгиларининг алмаштиришни таъминловчи бирор ани= жумла ёки жадвалнинг ырин алмаштиришларини тартибловчи бирор алощидалик хусусияти ва бош=а шу кабилар ытаган. Мисол учун, ушбу

АНГЛАШИЛМОВЧИЛИК ТУШУНАРСИЗЛИККА

ОЛИБ КЕЛДИ

жумласи устунларининг сони 5 та ва сатрларнинг сони 8 та былган жадвалнинг устунлари быйича ёзиб чи=илса, сынгра шу жадвалнинг сатрлари быйича группаланиб:

АМТИЛ, НОУЗИ, ГВШЛБ, ЛЧИИК,
АИНКЕ, ШЛАКЛ, ИИРАД, ЛКСОИ

каби шифрланган сызлар щосил былади.

Маълумотларни шифрлаб мущофазалашнинг турли ма=садларда =ылланиб ривожланиб бориши, шифрлаш услубларининг кенг омма томонидан фойдаланиш учун =улай былишини талаб =илиниши билан бирга, унинг бардошлигига былган талабни щам кучайишига олиб келди. XIX асрда ало=а коммуникацияларининг риводланиб бориши, табиий равишда, шифрлаш жараёнларининг автоматлаштиришни талаб эта бошлади. Телеграф ало=а системалари вужудга келди ва улар щам ыз навбатида маълумотларни шифрлашни талаб эта бошлади. Махсус, \илдирак кыринишидаги, сонли шифрлаш =урилмаси 1790 йилда Америка +ышма Штатлари (А+Ш) давлат котиби, кейинчалик эса А+Ш учинчи Президенти былган Томас Джеффесон томонидан яратилган ва шунга ыхшаш сонли шифрлаш =урилмалари иккинчи жащон уруши йилларидан кейин щам А+Ш =уролли кучларида =ылланиб келинган. Бундай сонли шифрлаш =урилмаларининг ишлаши, етарли даражада узун былган берилган калит быйича маълумотлар матнини кып алфавитли алмаштиришга асосланган былиб, арифмометрнинг ишлаш асосларига ыхшаш былган. Калитнинг (даврий) узунлиги шифрлаш =урилмасининг махсус \илдиракларини бир марта тыла айланишларининг умумий даври билан ани=ланади. Масалан, мос щолда 13, 15, 17 ва 19 даврий айланишларга эга махсус тыртта \илдиракли =урилма 62985 (даврий) узунликка эга былган калитни беради. Яъни, =урилма \илдираклари бирор ани= щолатда турган былса, манна шу щолатга =айтадан кетма-кет 1-\илдиракни 13 марта, 2-\илдиракни 15 марта, 3-\илдиракни 17 марта, 4-\илдиракни 19 марта айлантириш билан эришилади.

Щозирги замон криптографик машиналари асосан, 1917 йилда, Эдвард Хебери томонидан яратилган “Enigma – Энигма” («Жумбо=» маъносини англатувчи) деб аталувчи роторли криптографик машинанинг ишлаш тамойиллари ташкил этади. «Энигма» машиналарининг саноат намуналари “Siemen” фирмаси томонидан ишлаб чи=илиб, дастлаб битта ы=га ырнатилган ыртга айланувчи \илдиракдан иборат былиб, бирор ани= щолатнинг оддий алмаштиришлар ёрдамида, миллиондан орти= шифрланган щолатини олиш имконини берган. Щар бир \илдиракнинг икала томонида 25 тадан (лотин алфавитининг белгилари щарфлари сонича) электрик бо\ланиш туганлари жойлашган былиб, \илдираклар айланганда электрик бо\ланиш импулслари рый бериб, щарфларнинг алмашуви жараёни рый беради. Шифрлаш жараёни бошланиши олдидан \илдираклар калитни белгиловчи

сызни ани=ловчи щолатига ырнатилади. Алфавит белгиларини бош=а белгилар билан алмаштириб – шифрлаш жараёни, шифрлашни керак былган белгининг тугмачаларини босиш натижасида амалга оширилган. Бунда: шифрланиши керак былган белгининг тугмачаларини босиш натижасида, аввал 1-\илдирак бир =адамга бурилган ва щоказо. Натижада, табиийки, калитнинг узунлиги очи= матн узунлигига нисбатан узун былган.

Масалан, чап ва ынг томондаги \илдиракларнинг U белгисига мос келувчи электр бо\ланиш тугунлари \илдиракларнинг бош=а томонидаги F белгига мос келувчи электр бо\ланиш тугунлари билан бо\ланган. Агарда \илдирак бир =адамга бурилса, бу щолат U белгидан кейинги V белгини F белгидан кейинги G белгига алмаштириш жараёнини ифодалайди. Тырт \илдиракли криптографик машиналарда алфавит белгиларини шифрлаш жараёнидан ытиб, тырт кара шифрланади. Дешифрлаш жараёнини мураккаблаштириш ма=садида ва=ти-ва=ти билан \илдиракларнинг ырин алмаштирилиб турилган. Кейинчалик эса \илдиракларнинг сони 5 ва 6 тага кыпайтирилиб, уларнинг щаракатини маълум маънода тартибсиз былиши таъминланган. Бу =урилманинг щажми катта былмаган щамда ундан фойдаланиш мураккаб былмаганлиги сабабли оддий ало=а \изматчилари щам ишлата олганлар.

Шу даврга келиб маълумотларнинг ишончли шифрлаш масаласи тыла щал =илингандек эди. Лекин Англия криптографик хизматининг хизматчилари Лондондан 80 км. шимолда жойлашган «Блетчли Бо\» =ароргощига бутун иккинчи жащон уруши йиллари давомида немислар шифровкасини ы=иб боришга муваффа= былдилар. Бунга Польша разведка хизматининг 1939 йилда =ылга киритган «Энигма» криптографик машинасининг чизмалари асос былди. Гитлерчиларнинг Польша щужумидан сынг машина чизмалари Англиянинг тегишли хизмат ташкилотларига берилди. Тез орада Англия криптоаналитика хизмати ходимлари. «Энигма» машинасининг шифрлаш калитини билиш учун, машинанинг махсус \илдиракларидаги электр бо\ланиш тугунларининг схемасини билиш кераклигини ани=ладилар. Шундан сынг «Энигма» машинасининг =урилма намунасини =ылга киритиш учун щаракатлар бошланди. Биринчи намунани Германиянинг жанубий-шар=ий =исмига жойлашган заводдан олинишига эришилди, иккинчи Норвегия щаво щудудларида уриб туширилган немис щужумчи самолётларидан олинган, учинчи Франция учун былган жангларда аср тушган немис щарбий ало=ачи аскаридан олинган. Кейинги намуналар эса \оввослар махсус =исмлари билан немис сув ости кемаларилан олинган. 1942 йилда Алан Тьюринг томонидан махсус электрон щисоблаш машинаси яратилгунга =адар, «Энигма» шифрларини дешифрлаш анча мушкул былди. Алан Тьюрингнинг дешифрлаш учун махсус яратган ва «Колосс» деб номланган ушбу машинаси инсоният дунёсида биринчи яратилган тез ишловчи электрон щисоблаш машинаси (ЭЩМ) эди. Шундан сынг Англия криптоаналитиклари, намуналари олинган «Энигма» машиналарининг \илдиракларидан фойдаланиб, =ис=а ва=т ичида мумкин былган барча калитларни танлаб чи=иб, дешифрлаш масаласини щал эта бошладилар.

Немислар эса дешифрлашда ЭЩМнинг =ылланишини щисобга олмаган эдилар. Шуни щам айтиб ытиш керакки, 1930 йилда немис криптоаналитиги Георг Шедернинг «Энигма» криптографик машинасининг шифрлаш услубига ишончсизлик билдириб келтирган далиллар, кыпчилик масъул мутахассисларнинг назаридан четда =олган.

1926 йилда Америка телефон ва телеграф компанияларидан бирининг инженери Г.С. Вернам ўзининг иккилик сано= системаси асосида яратган шифрлаш услубини эълон =илди [3]. Вернамнинг шифрлаш услуби Цезарнинг шифрлаш услубига ыхшаш бўлиб, у =уйидаги

$$y = x \oplus z \qquad (1)$$

тенглама билан ифодаланади ва бунда *x, y, z* ўзгарувчилар иккилик сано= системаси алфавитларида =ийматлар =абул =илади, $\oplus$ белги эса 2 модул бўйича кўшиш амалини билдиради, яъни: $0 \oplus 0 = 0,\ 0 \oplus 1 = 1,\ 1 \oplus 0 = 1,\ 1 \oplus 1 = 0$. Бу услубнинг мощияти: дешифрлаш калитининг фа=ат бир марта ишлатилишига асосланиб, шифрлаш щар сафар янги тасодифий битлардан иборат бўлган калит билан амалга ошириладн. Бундай шифрлаш услубидан кўриниб турибдики, шифрлаш ва дешифрлаш учун очи= матн узунлиги билан тенг былган битта калитдан фойдаланилади, щамда бу калитни фойдаланувчига мущофазалаган ало=а канали ор=али узатилиши талаб этилади. Бундан таш=ари, шу усул билан шифрланган матнни дешифрлаш имконияти йўк. Бу услубнинг автори Г.С.Вернам щам дешифрлаш имконияти йў=лигини таъкидлаган, лекин фикрининг исботини келтирмаган. Криптология сощасидаги илмий ишлар авторлари, 1949 йилгача бўлган даврни =атъий игботсиз - фа=ат интуиция ва "ишончга" асосланган - илмий аоосланмаган криптология даври, деб атайдилар. Таъкидлаб ўтиш жоизки, Англия криптология хизмати нккинчи жащон уруши йиллари даврида математиклар криптологиянинг ривожланишига ўзларининг катта хиссасини =ўшиши мумкинлигига и=рор бўлдилар. Алан Тьюринг щам криптология хизмати мутахассисларидан бири бўлган.

1949 йилдаги К.Э.Шенноннинг "Махфий тизимларда ало=а наза-рияси" [4] деб номланган илмий ма=оласи илмий асосланган махфий калитни криптография даврини бошлаб берди. Шеннон ўзининг электротехника ва математикага оид билимларидан келлб чи=иб, кенг маънодаги махфий ало=а тизими назариясининг асосини 1948 йилда эълон килинган - ахборотлар назариясига ба\ишланган илмий ма=оласи асосида яратди [5]. Шеннон ўзининг бу илмий ма=олаларида Вернам услубида шифрланишнинг ишончлиги даражасида тўхталиб, дешифрлаш мумкин эмаслигини илмий асосда исботлаб берди щамда шу услубда шифрлашда фойдаланувчига махфий ало=а канали ор=али узатиладитан махфий калит щажми (узунлиги) учун ани= =уйи чегаранинг =андай бўлишини илмий асосда кўрсатиб берди. Шенноннинг 1948 йилда эълон =илинган илмий ма=оласи кринтология

сощасидаги илмий ма=олаларнинг сезиларли кўпайишига олиб келди. Унинг 1949 йилда эълон =илинган илмий ма=оласи катта ащамиятли бўлса-да, криптология сощасидаги илмий ма=олаларнинг сезиларли кўпайишига олиб келмади. Бунга сабаб эщтимолки, Шенноннинг махфий тизимларда ало=а назарнясининт махфий калитга асосланган бўлиб, махфий калитни фойдаланувчига етказиш масалалари ечимининг мураккаблиги билан бо\ли=лигидадир. 1976 йилда У.Диффи ва М.Е.Хеллманнинг "Криптографияда янги йўналишлар" [6] деб номланган ма=оласининг эълон =илиниши шу сощадаги очи= илмий ишларнинг ривожини жуда ю=ори по\онага кўтарилишига сабаб бўлди. Улар ўзларининг ушбу ишида махфий ало=а тизимларида маълумотларни шифрлаш ва дешифрлашда махфий калитнинг тизим фойдаланувчилари орасида махсус мущофазаланган ало=а канали ор=али узатилиши ва =абул =илинишига хожат бўлмайдиган илмий-амалий услуб асосларини яратиб, бугунги кунда кам ривожланиб ва долзарблашиб бораётгаи очи= (махфий бўлмаган) калитли криптография даврини бошлаб берди. Эслатиб ўтиш жоизки, Р.К.Мерклининг У.Диффи ва М.Е.Хеллманга бо\ли= бўлмаган щолда, лекин улар билан деярли бир пайтда бош=а илмий журналга эълон =илиш учун берилган ма=оласида [7] щам маълумотларни очи= калитли шифрлаш \оясининг асослари келтирилган. Аммо Р.К.Мерклининг ма=оласини наширётда узо= ва=т эълон =илинмай тўхтаб =олиши, уни авторлик щу=у=идан деярли мащрум этди.

Таянч иборалар.

Криптология, криптография, шифрлаш, дешифрлаш, калит, симметрик криптосистема, ассиметрик криптосиситема, алфавит, калитларни та=симлаш, криптобардошлик.

Назорат саволлари.

1. Криптология нима ва у=андай ма=садларда ишлатилади?
2. Криптологиянинг =айси синфлари мавжуд?
3. Криптография щимоясида шифрларга нисбатан =андай талаблар =ыйилади?
4. Криптография щимоясида =андай усуллар =ылланилади?

Асосий адабиёт

1. Анохин М.И., Варнавский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. М. 1997г.

2. Брюс Шнайер. Прикладная криптография: 2– е издание. М. 2001.

3. Фомичев В.М. Дискретная математика и криптология. М. «Диалог МИФИ» 2003 г. http: ‖ www.library.mephi.ru – Библиотека МИФИ.

4. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М. «Радио и связь» 2001г.

5. Московский центр непрерывного математического образования. Материалы 1 – 9 олимпиад по криптографии. М. 2001 – 2003гг. http: ‖www. ibc.ry./- электронная библиотека Московского Государственного Университета экономики, статистики и информатики.

6. В.А.Хорошко, А.А.Чекатков. Методы и средства защиты информации. Издательство «ЮНИОР» К. 2003.

Кушимча адабиёт

1. Анин Б. Защита компьютерной информации. Санкт – Петербург, 2002.

2. Завгородный В.И. Комплексная защита информации в компьютерных системах., М. «Логас», 2001.

3. А.В.Домашев, М.М.Грунтович, В.О.Попов, Д.И.Правиков, А.Ю.Щербаков, И.В.Ппокофьев. Программирование алгоритмов защиты информации. Учебное пособие. Издательство «Нолидж». М. 2002.

Маъруза 3

Банк автомаштирилган ахборот тизимларида ахборотни щимоялаш воситаларининг асосий турлари

1. Тыловлар тизимида криптографик щимояланиш муаммолари.
2. Ахборотни криптографик щимоялаш воситаларига былган зарурий ва етарли талаблар.
3. Дастурий таъминотнинг яхлитлигини назорат =илиш.

Банкларнинг амалий фаолияти ахборотларни щимоялаш тадбирлари ва усулларини =ыллаш =уйидаги муста=ил йынатишларни ыз ичига олади:

- ахборотларга рухсатсиз киришдан щимояланиш;
- ахборотларни ало=а тизимларида щимояланиш;
- электрон щужжатларнинг юридик ащамиятини щимоялаш;
- махфий ахборотларни =ышимча электрон магнитли нурланишлар ва узатиш каналларидан чи=иб кетишини щимоялаш;
- ахборотларни компьютер вируслари ва дастурларини тар=атиш каналлари быйича бош=а хавфли таъсилардан щимоялаш;
- дастур ва =имматли компьютер ахборотларини рухсатсиз нусха кычириш ва тар=атилишидан щимоялаш.

Щар бир йыналиш учун асосий ма=сад ва вазифалар ани=ланади.

Рухсатсиз кириш остида фойдаланувчилар ва чекланиш ААТнинг бош=а субъектларини тасодифан ёки =асддан щаракати натижасида ахборотларни щимоялашнинг асосий =исми былган киришни чеклашнинг белгиланган =оидалари бузилиши тушунилади.

Ахборотларга рухсатсиз киришни амалга оширган субъектлар **=оида бузувчилар** деб аталади.

Ахборотларни щимоялаш ну=таи назаридан рухсатсиз кириш =уйидаги о=ибатларга олиб келиши мумкин: ишлаб чи=илаётган махфий ахборотни четга чи=иб, щамда ААТехни иш =обилиятини =асддан бузиш натижасида унинг бузилиши.

+уйидаги щар бири тартиб бузувчи былиши мумкин:

- ААТехдпн штатли фойдаланувчилар;
- ААтехнинг тизимли, умумий ва амалий дастурлар билан таъминланишини кузатиб борувчи дастурловчи-ходимлар;
- Хизмат кырсатувчи ходимлар (мущандислар);
- ААТехга рухсатли киришга эга бош=а ходимлар (шу жумладан ёрдамчи ишчилар, фаррошлар ва щ.к.).

ААТехга бош=а бегона шахсларнинг (кырсатилган категорияларга кирмайдиганларни) кириши ташкилий усулни тадбирлар асосида истисно =илинади.

Ахборотларга рухсатсиз кириш канали осида шахслар улар томонидан бажарилаётган технологик тадбирлар щаракатининг изчиллиги тушунилади. Улар ёки рухсатсиз бажарилади, ёки ходимларнинг хатолари ёки ускуналарнинг бузилиши натижасида ноты\ри ишлаб чи=илади. Рухсатсиз киришнинг бутун каналларини ани=лашни лойихалаштириш ахборотларни са=лаш, кузатиш ва ишлаб чи=иш технологияларини, ахборотларни щимоялаш тизимини ва тартиб бузувчисининг танлаган моделини тащлил =илиш йыли билан ытказилади.

Махфий ва =имматли ахборотларга рухсатсиз кириш ва уларни щимоялаш энг мущим вазифалардандир. Компьютер эгалари фойдаланувчиларнинг мулкий щу=у=ларини ишлаб чи=арилаётган ахборотларнигавдаланаётган мулкни жиддий и=тисодий ва бош=а моддий ва номоддий зарарлар келтириши мумкин былган турли киришлар ва ы\ирлашлардан щимоялашдир.

Нафа=ат эщтимол былган тартиб бузувчини ШКда са=ланаётган ахборотларни «ы=иш» имкониятларини, балки, уни штатли ва штатсиз воситалари билан тартиб бузувчи имкониятин щам бартараф этишга =аратилган. Вазифавий кафолатларни ва ахборотларга киришни чеклаш вазифаси ахборотларга рухсатсиз киришдан щимоялаш муаммосининг асоси былади.

Ахборотларга рухсатсиз киришни щимоялаш быйича талаблар щимояланаётган ахборотларнинг учта асосий хусусиятларига эришишга йыналтирилган:

- **махфийлик** (махфий ахборотларга фа=а тунга тегишли былган кишилар кириши керак);
- **яхлитилик** (мущим =арорлар =абул =илишда фойдаланилаётган ахборотлар ишончли ва ани= былиши ва =асддан, щамда \араз ма=садлари билан бузилиши имкониятларидан щимояланган былиши керак);

- **тайёргарлик** (ахборотлар ва тегишли ахборот хизматлари уларга зарурат ту\илган пайтда, щамма ва=т хизмат кырсатишга тайёр былишлари керак).

Маълумотларга киришнинг назорати остида ААТехдан фойдаланувчилар ва тизим томонидан ишлаб чи=илаётган ахборотлар ыртасида киришга чеклаш тизими былиши керак.

Банк ахборотларига киришни чеклашнинг щар =андай тизимини муваффа=иятли фаолият юритиш учун иккита вазифани ечиш зарур:

1. Таъминланган модел доирасида былган щаракатлар билан ахборотларга киришни чеклаш тизимини четлаб ытишни мумкин былмайдиган =илиш.
2. Маълумотларга киришни амалга ошираётган фойдаланувчининг идентификациясини (белгилаш) кафолатлаш.

Рыйхатга олиш ААТехнинг хавфсизлигини самарали таъминлаш усулларидан бири былади. Рыйхатга олиш =айд дафтари асосида жавобгар былганни рыйхатга ва щисобга олиш тизими =ылланилиб, унинг асосида ытмишда нима содир былганлигини кузатишга ва шунга кыра ахборотларни чи=иб кетиш каналини тысишга имкон беради. Рыйхатга олиш =айд дафтарида маълумотлар ва дастурларга киришнинг барча амалга оширилган ва амалга оширилмаган щаракатлар =айд этилади. Рыйхатга олиш =айд дафтарининг мазмуни даврий ва узлуксиз тащлил =илиниши мумкин.

Рыйхатга олиш =айд дафтарида БнААтнинг фойдаланувчилар томонидан амалга оширилаётган барча назорат =илинаётган сыровларнинг рыйхати олиб борилади.

Рыйхатга ва щисобга олиш тизими =уйидагиларни амалга оширади:

- Кириш субъектларини тизимга (тизимдан) кириши (чи=иши)ни рыйхатга олинишни ёки операцион тизимни иш билан тыла таъминлаш ва инициаллаштиришни ва унинг дастурий тыхташини рыйхатга олишни (ААТехни аппаратли узилиш пайтида тизимдан чи=иш ва тыхтатишни рыйхатга олиш ытказилмайди);
- нусхадаги босма (график) щужжатларни беришни рыйхатга ва щисобга олиш;
- щимояланган файлларни ишлаб чи=иш учун мылжалланган дастурлар ва жараёнлари (вазифалар, масалалар)ни ишга тушириш (тыхтатиш)ни рыйхатга олиш;
- дастурий воситалар, дастурлар, жараёнлар, вазифалар, масалалар щимояланаётган файлларга киришга =илинаётган щаракатларни рыйхатга олиш;
- ахборотларнинг щимояланадиган манбаларини щар =андай белгилаш (маркалаш) ёрдамида щисобга олиш (щимояланадиган манбаларни щисобга олиш =айд дафтарида, картотекада уларни бериш) =абул =илишни рыйхатга олиш билан ытказилади.
- **Ало=а тизимларида ахборотларни щимоялаш** щар хил турдаги ало=а каналларда айланиб юрувчи махфий ва =имматли ахборотларга

рухсатсиз киришнинг имкониятини бартараф этишга =аратилган. Унинг асосида щимоянинг бу тури =уйидаги ма=садларга =аратилади: ахборотлар махфийлиги ва яхлитлигини таъминлашга эришилишни кызлайди. Криптография ва махсус ахборот баённомаларини =ыллаш ало=али назорат =илинмайдиган каналлардаги ахборотларни щимоялашнинг энг самарали воситаси былади.

- **Электрон щужжатларнинг юридик ащамиятини щимоялаш** буйру=лар, тылов топшири=номалари, контрактлар ва бош=а фармойиш, шартнома ва молиявий щужжатларнинг са=ловчи ахборот объектларини ишлаб чи=иш, са=лаш ва узатиш учун тизимлар ва тармо=лардан фойдаланишда зарур былади. Ушбу муаммони ечиш учун «Ра=амли имзоларни» =ыллаш билан бо\ли= ахборот объектларининг ща=и=ийлигини текширишнинг замонавий криптографик усулидан фойдаланилади. Амалда электрон щужжатлар ащамиятини щимоялаш масаласи компьютерли ахборот тизимларини щимоялаш масаласи билан биргаликда щал =илинади.
- +ышимча электрон магнит нурланишлар ва узатиш каналлари быйича **ахборотларнинг чи=иб кетишдан щимоялаш**, ШКдаги махфий ва сирли ахборотларга бегона шахслар томонидан рухсатсиз киришдан щимоялашнинг мущим жищати былади. Щимоянинг ушбу тури ахборотли электрон магнит сигналларини =ыри=лаётган худуд таш=арисига чи=иб кетиш имкониятини бартараф =илишга =аратилган. Бунда шу нарса кызда тутиладики, =ыри=лаётган худуд ичида электрон магнитли сигналларни тутиб олиш, рыйхатга олиш ва тасвирлашнинг махсус аппаратларидан назоратсиз фойдаланиш имкониятларини йы==а чи=арувчи самарали чоралари =ылланилади. +ышимча электрон магнитли нурланишлар ва узатиш каналларидан щимояланиш учун щисоблаш техникасини жойлаштириш учун мылжалланган хоналарни экранлаштириш, щамда ускунанинг ызини (ШК ва ало=а воситаларини) ахборот нурланишининг интенсивлигини пасайтиришга имкон берувчи техник тадбирлар =ылланилади.
- Баъзи бир маъсулиятли щолларда **щисоблаш ускуналарини компьютернинг ахборот нурларишлари,** щамда нут=ли ва мущим былмаган кучсиз ахборотли сигналларни рыйхатга олиш ёки ёзиш ма=садида тадби= этиши мумкин былган молиявий жосусликнинг махсус =ыйилувчи =урилмаларини ани=лаш учун =ышимча текширувлар зарур.
- **Ахборотларни компьютер вируслари ва дастурларини тар=атиш каналлари быйича бош=а хавфли таъсирлардан щимоялаш** кейинги ва=тда алощида мущим ащамият касб этади. Вирусли касалликларни ща=и=ий ани=ланиш кыламлари ШКларни касалланишининг юз минглаб щолатлари билан бащоланади. Баъзи бир вирус дастурлари бутунлай зарарсиз былсалар щам, улардан кыпчилиги щароб =илувчи хусусиятларга эга. Айни=са, турли мащаллий щисоблаш тармо=лари таркиби га кирувчи компьютерлар учун вируслар хавфлидир. Замонавий ахборот тизимларининг баъзи бир хусусиятлари вирусни тар=алиши учун =улай шароитлар яратади. Уларга, хусусан, =уйидагилар киради:

- кыпгина фойдаланувчиларнинг дастурий таъминотдан биргаликда фойдаланишларининг зарурияти;
- дастурдан фойдаланишни чеклашнинг =ийинчилиги;
- щимоялашнинг мавжуд тизимларининг мавжуд тизимларининг ишончсизлиги;
- вирусга =арши щаракатга нисбатан ахборотларга киришнинг чекланганлиги.

Вирусдан щимояланиш усулларида иккита йыналиш мавжуд:

1. Рухсатсиз ызгартириш киритиш имкониятларидан щимояланган «иммуно бардошли» дастурий воситаларни (киришни чеклаш, ыз-ызини назорат =или шва ыз-ызини тиклаш усулларини) =ыллаш;
2. АДПлар фаолиятида четга чи=ишларнинг вужудга келишининг доимий назоратини, вирусли фаолликнинг эщтимол былган бош=а излари мавжудлигини даврий текширишни (масалан, даврий таъминланишни бузилишини топишни), щамда янги дастурни улардан фойдаланиш олдидан киришнинг назоратини (уларнинг танасида вирусли тузилмаларининг мавжудлигини ызига хос аломатлари быйича) амалга оширувчи махсус тащлилчи дастурларни =ыллаш.

- **Дастурлар ва =имматли банк ахборотларидан рухсатсиз нусха кычириш ва тар=атилишдан щимоялаш** ШК дастурлари ва маълумотларининг =имматли баъзалар кырынишида гавдаланган а=Лий мулкини са=лаш муаммосига мылжалланган мулкий щу=у=ларни щимоялашнинг муста=ил туридан иборат былади. Ушбу щимоялаш одатда щимояланаётган дастурлар ва маълумотлар базасини аввалдан ишлаб чи=увчи (пароли щимоя, калит ва калитли дискетларни са=лаш быйича =урилмаларга мурожаат =илиш быйича текшириш, ишчи ШКнинг ноёб таърифлари быйича текшириш) махсус дастурий воситалар ёрдамида амалга оширади. Бу ишлаб чи=иш щимояланаётган дастур ва маълумотлар базасининг бажарилаётган кодини, «бегона» машиналар бажаришга тыси= =ыювчи щолатга келтиради. Щимояланишни ошириш учун принтернинг узувчиси ёки ШКнинг тизимли шинасига уланувчи =ышимча аппарат блоклари, щамда дастурнинг фойдаланилаётган кодига эга шифрли файллар =ылланилади. Дастурларни рухсатсиз нусха кычиришдан щимоялашнинг умумий хусусиятлари бундай щимоялашнинг бар=арорлигини чекланишидир, якуний щол дастурдан фойдаланиладиган коди бажарилишда марказий процессорга очи= щолда келиб тушади ва аппартли созловчилар ёрдамида кузатиш мумкин. Аммо бу щол щимоялаш воситаларини истеъмол хусусиятларини нолгача тушурмайди, чунки улардан фойдаланишдан асосий ма=сад =имматли ахборотлардан рухсатсиз нусха кычириш имкониятини, ва=тинча былса щам, энг ю=ори даражага =ийинлаштиришдир.
- **Дастурий таъминотнинг яхлитлигини назорат =илиш** =уйидаги усулларда ытказилади:
- дастурий таъминотнинг яхлитлигини таш=и воситалар (яхлитликни назорат =илиш дастурлари) ёрдамида назорат =илиш;

- дастурий таъминотнинг яхлитлигини ички воситалар (дастурнинг ызига =урилган) ёрламида назорат =илиш.

Дастурларнинг яхлитлигини таш=и воситалар билан назорат =илиш тизимни ишга туширишда бажарилади ва дастурлар айрим блокларининг назоратли ми=дорларини уларнинг эталонли ми=дорлари билан та==ослашдан иборат былади.

Дастурларнинг яхлитлигини ички воситалар билан назорат =илиш дастурни ишлашга щар бир туширишда бажарилади ва дастурлар айрим блокларининг ми=дорларини уларнинг эталонли ми=дорлари билан та==ослашдан иборат былади. Бундай назоратда ички фойдаланиш учун дастурлардан фойдаланилади.

Амалий ва махсус дастурларни тартиб бузувчи томонидан махфий ахборотни олиш ма=садида рухсатсиз ызгартирилиши ахборотга рухсатсиз киришнинг эщтимол былган каналларидан бири былади. Бу ызгаришлар ёки уларни четлаб ытиш (амалий дастурларда щимоялаш тизими =ылланилганда) ёки бевосита амалий дастурлардан махфий ахборотларни олишнинг сезилмайдиган каналини ташкил =илиш усули ю=оридаги щолга =арама-=аршилик =илувчи усуллардан биридир. Аммо бу усул етарли эмас, чунки у яхлитликни назорат =илиш дастури тартиб бузувчи томонидан ызгартириш киритиш деб фараз =илади.

Тижорат ахборотларини щимоялашда =оидага кыра, маълумотларнинг рухсатсиз киришдан щимоялашнинг щар =андай воситалари ва тизимларидан фойдаланилади, аммо щар бир щолда щимояланаётган ахборотларнинг мущимлиги ва уни йы=отишдан олинадиган зарарларни ща=и=ий бащолаш керак.

Щимоялаш даражаси =анчалик ю=ори былса, шунчалик =имматдир. Щаражатларни =ис=артириш техник воситларни стандартлаштириш йыналишида кетмо=да. Бир =атор ани= ма=садлар ва шароитлардан келиб чи==ан щолда, аттестациядан ытган намунавий воситаларни, щатто улар баъзаси бир параметрлар быйича бышро= былсалар щам тавсия этилади.

Ахборотларни щимоялаш щар хил усуллар билан таъминланиши мумкин, аммо криптографик усуллар асосида =урилган тизимлар ва воситалар энг ишончли ва самарали (ало=а каналлари учун ягона ма=садга мувофи=) быладилар. Нокриптогрфик усуллардан фойдаланилган щолда амалга оширилган тадбирларнинг етарлилигининг исботи ва тизимга рухсатсиз киришдан щимояланганлигининг ишончлилигини асослаш катта =ийинчилик ту\диради.

Шуни назарда тутиш керакки, щимояланиши керак былган маълумотлар нафа=ат ишончлиликнинг етарлича даражаси билан олди олинган (масалан, барча маълумотлар фа=ат шифрланган щолда са=ланадиган) ЭЩМга «киришни» амалга ошириш щисобига, балки ЭЩМнинг энергия манбаи ва ерга уланиш занжири, щамда ало=а каналларидаги =ышимча электр магнитли нурланишлар щисобига щам олиниши мумкин. Истисносиз барча электр магнитли =урилмалар, ЭЩМнинг блоклари ва =исмлари у ёки бу даражада нурланади, бунинг устига бундай

=ышимча сигналлар етарлича =удратли былишлари ва бир неча метрдан бир неча километр масофагача тар=алишлари мумкин. Бунда «ра=иб» томонидан калит ща=идаги ахборотни олиш энг катта хавф ту\диради. Калитни тиклаб, шифрланган маълумотларни эгаллаш быйича бир =атор муваффа=иятли щаракатларни =илиш мумкин, улар =оидага кыра, тегишли очи= ахборотларга =араганда камро= ди==ат билан щимояланадилар. Ушбу ну=таи назардан худи рухсатчиз киришдан щимоялашнинг аппаратли ва дастурий-аппаратли воситалари фойдалиро= фар=ланади, улар учун калитли ахборотлар ща=идаги =ышимча сигналлар соф дастурий амалга оширишларга нисбатан пастро=дир.

Айтилганлардан щимоялаш воситаларини танлаш ва фойдаланишда щимоянинг ишончлилиги белгиловчи омил быладиган хулоса чи=аришга имкон беради.

Таянч иборалар

Электрон щужжат, =оида бузувчи, махфийлик, яхлитлик, идентификация, аутентификация, щимояланиш даражаси

Назорат саволлари

1. Ахборотларга рухсатсиз киришни амалга оширган субъектлар турлари.
2. Ахборотларни щимоялашдаги асосий хусусиятлари нимадан иборат.
3. Дастурий таъминотнинг яхлитлигини назорат =илиш усуллари.

Асосий адабиёт

1. Анохин М.И., Варнавский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. М. 1997г.

2. Брюс Шнайер. Прикладная криптография: 2– е издание. М. 2001.

3. Фомичев В.М. Дискретная математика и криптология. М. «Диалог МИФИ» 2003 г. http: ‖ www.library.mephi.ru – Библиотека МИФИ.

4. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М. «Радио и связь» 2001г.

5. Московский центр непрерывного математического образования. Материалы 1 – 9 олимпиад по криптографии. М. 2001 – 2003гг. http: ‖ www. ibc.ry./- электронная библиотека Московского Государственного Университета экономики, статистики и информатики.

6. В.А.Хорошко, А.А.Чекатков. Методы и средства защиты информации. Издательство «ЮНИОР» К. 2003.

Кушимча адабиёт

1. Анин Б. Защита компьютерной информации. Санкт – Петербург, 2002.

2. Завгородный В.И. Комплексная защита информации в компьютерных системах., М. «Логас», 2001.

3. А.В.Домашев, М.М.Грунтович, В.О.Попов, Д.И.Правиков, А.Ю.Щербаков, И.В.Ппокофьев. Программирование алгоритмов защиты информации. Учебное пособие. Издательство «Нолидж». М. 2002.

Маъруза 4

Криптосистемаларга =ўйиладиган талаблар

1. Симметрик криптосистема асослари.
2. Криптографик системаларнинг назарий ва амалий бордошлилиги.
3. Ырин алмаштириш усуллари.
4. Алмаштириш усуллари.

Маълумотларни мущофазалашнинг мущим масалалари билан бевосита муносабатда бўлмаган кишилар ахборотлар тизимида мущим маълумотлар мущофазаси =оидаларининг бузилиши мумкин бўлган сабабларни сон ва сифат жищатидан сер=ирралигини, табиийки, маълум бир =олипда тасаввур =ила олмайди. +уйида келтириладиган жадвалда кўп учрайдиган ва нисбатан я=олро= щис =илиш мумкин бўлган баъзи мущофазалаш =оидаларининг бузилиш сабаблари келтирилган.

Жадвал 1. Маълумотларни мущофазалаш =оидаларини бузувчининг ма=сади ва уни амалга ошириш услублари:

1) Рухсат этилмаган маълумотларни берухсат олиш ва унга эга бўлиш, яъни маълумотларнинг махфий са=ланиш =оидаларини бузиш.

2) Махфий ахборотлар тизимида фойдаланувчиларнинг бирор маълумот юзасидан ўзини жавобгарликдан (масъулликдан) халос этиш учун ўзини бош=а фойдаланувчи сифатида ифодалаш ёки бош=а фойдаланувчининг ваколатидан фойдаланиш ма=садида:

а) ёлгон маълумотларни ташкиллаштириш;

б) ща=и=ий (=онуний) маълумотларии ўзгартириш;

в) рухсат этилмаган маълумотни олиш учун ўзинн шу маълумотни олишга ваколати бўлган шахс спфатида ифодалаш;

г) ёл\он маълумотларни ахборотлар тизимига тушинишига йўл =ыйиб бериш ёки ёл\он маълумотларни тасди=лаш;

3) Мавжуд бўлган маълумотларни ташкиллаштиришни рад этиш.

4) +оидабузар томонидан ёлгон маьлумотлар ташкиллаштирилиб, шу ёл\он маълумотларни ахборотлар тизимининг бош=а бир фойдаланувчиси томонидан ташкиллаштирилган, деб ифодалаш.

5) Бирор ани= кўрсатилган ва=тда маълумотни олувчига юборилмаган маълумотни юборилган, деб ифодалаш ёки юборилган маълумотни юборилган ва=тини ёл\он кўрсатиш.

6) Ща=и=атан щам, олинган маълумотларни олинганлигини рад этиш ёки маълумотларнинг ща=и=ий олинган ва=тини сохталаштириш.

7) Ахборотлар тизимидан фойдаланувчиларнинг ўзларига берилган ваколатларини - маълумотларни ташкиллаштириш, узатиш, тар=атиш ва бош=а йўналишларда рухсат этилмаган щолда кенгайтириш.

8) Рухсат этилмаган щолда фойдаланувчиларнинг ваколатларини ўзгартириш.

9) Махфий бўлган маълумотни махфий бўлмаган маълумотлар каби ифодалаш.

10) Ало=а тизими фойдаланувчиларининг ўзаро ало=а шахобчаларига рухсат этилмагаи щолда бо\ланиб олиб, шу шахобчадан олинган маълумотларни бош=а ало=а тизимларига доимий равишда тар=атиб туриш.

11) Ало=а каналидаги маълумотлар о=имини тащлил =илиб, маълумотлар жам\армасининг тузилиш тартибига =араб, программалаш таъминоти ва бош=а хосликларга кўра, фойдаланувчилардан ким =андай маълутмотларни =ачон олиш ваколатига эгалигини ўрганиш.

12) Протокол (маълум тартиб щамда =оида) быйича щар =андай холда щам махфий =олиши керак бўлган маълумотни махфийлигига путур етказган щолда ушбу протокол маълумотларнинг софлигини таъминлашига шубща билан =араш.

13) Бирор я==ол сезилмайдиган йўл (процедура) билан маълумотларни мущофазалаш алгоритми дастурига ўзгартириш киритиш.

14) Ёл\он маълумотлар асосида бош=а фойдаланувчиларни мущофаза протоколни бузишга ундаш.

15) Очи=дан очи= протоколни бузши билаи ушбу мущофаза протоколига ишончни йў=отишга олиб келадиган щатти-щаракатлар.

16) Ахборотлар тизимининг бош=а фойдаланувчиларига маълумотларни сифатли узатилишига щала=ит бериш, хусусан, узатилаётган

маълумотга я==ол сезилмайдиган техник, дастурий ва бош=а услублар билан щала=ит бериб, узатилган маълумотнинг ща=и=ийлигини (аутентификациясини) рад этишга олиб келадиган щатти-щаракатлар.

Бу ю=орида келтирилган жадвални ихтиёрий муносабат (айни=са келишмовчилик) муаммоларини сабабларини манти=ан тащлил =илишда щам асос =илиб олиш мумкин.

Месси ўзининг "Щозирга замон криптология фанига кириш", деб номланган илмий ма=оласида =анчалик ишончли криптобардошли услуб яратилмасин бари-бир ўз ечимини кутаётган бош=а криптографик масалалар келиб чи=иши мумкинлигини таъкидлаб; фойдаланывчиларга протокол бўйича ўз вазифаларини бажаришлари учун махфий калитни =андан узатиш ва олинган маълумотларни ща=и=ийлигига ишонч щосил =илиш масалалари тў\рисида тыхталади. Мана шундай масаланинг =ўйилиши, хусусан, калитларни ахборотлар тизими фойдаланувчиларига та=симлашда келиб чи=адиган муаммоларни щал этувчи, очи= калитли криптография йўналишининг вужудга келишига сабаб бўлди. Бундан таш=ари, тизим фойдаланувчиларининг щар бири бутун тизим протоколи ичида ўзларининг =исм протоколи быйича фаолият кырсатаётганлигига щамда бош=а фойдаланувчиларнинг щам умумий тизим протоколини бузмаган щолда фаолият кўрсатаётганлигига ишонч щосил =илиниши, яъни умумий тизим протоколининг бардошлилик даражасига ишонч масалалари щам мущим ащамият касб этади. Содда =илиб ифодалаганда, ахборотлар тизимидаги щар бир фойдаланувчининг шахсий калитнинг мущофазасини таъминлаш долзарб масаладир.

Криптографик алгоритмнинг бардошлилик даражаси канчалик мустащкам бўлишидан =атьий назар, ахборотлар тнзиминнинг фаолият жараёнларини бузиш усуллари мавжуд бўлиб, бу усуллар криптографик алгоритмнинг бардошлилик даражасига бо\ли= эмас. Масалан, калитларни та=симлаш услубининг протоколини камчилиги билан, бнр нечта фойдаланувчиларнинг ўз калитларини бир-бирига ошкор =илингани щолда, криптографик алгоритимнинг махфийлигига зарар етказилиши мумкин. Умуман олганда, ахборотлар тизимининг протокол быйича ишлаш жараёни камчилиги криптоалгоритмнинг бардошлилик даражасини суньий равшида пасайишига олиб келади. Бундан камчиликларни олдини олишда протоколнинг бир =исми иккинчи =олган =исми ту\рисидаги маълумотни мущофазаланган щолда ахборотлар тизими бўйича очи= (махфий бўлмаган) ало=а тармо\и ор=али узатилишини таъминлаш имконини бериши керак.

Маълумотларни криптографик услублар билан мущофазалаш жараёнлари алгоритмик тиллар билан махсус криптобардошли алгоритмларни дастурлаш (программалаштириш) ор=али ёки махсус техник аппаратлар ёрдамида амалга оширилади. Бунда дастурлаш услублари ўзининг кўлланиш жищатидан =улайлиги билан ажралиб туради. Техник аппаратлардан фойдаланувчи услублар катта =ийматдаги моддий мабла\ талаб =илсада, ўзининг самарадорлиги, =улайлиги, ишончлилиги ва шу каби бош=а томонлари билан фар=ланади.

Ахборотлар тизими мущофазасининг замонавий криптографик услубларига =уйидаги умумий талаблар =ўйилади:

-шифрланган маълумотни ы=иш имконияти фа=ат дешифрлаш калити маълум бўлгандагина мумкин бўлсин;

-фойдаланилган шифрлаш калатини шифрматннинг бирор маълум =исми бўйича ёки унга мос келувчи очи= текст бўйича ани=лаш учун, бажарилиши зарур бўлган амаллар сони калитни ани= топиш учун бажарилиши керак бўлган барча амаллар сонидан кам былмаслиги керак, яъни калитни танлаб олиниши керак бўлган тыплам элементларининг сонидан кам бўлмаслиги керак;

-шифрлаш алгоритмининг маълумлиги шифрлаш алгоритмининг бардошлилигига салбий таъсир кўрсатмаслиги керак:

-калитнинг щар =андай даражадаги (озми, кўпми) ўзгариши шифрланган маълумотнинг жиддий ўзгаришига олиб келиши керак;

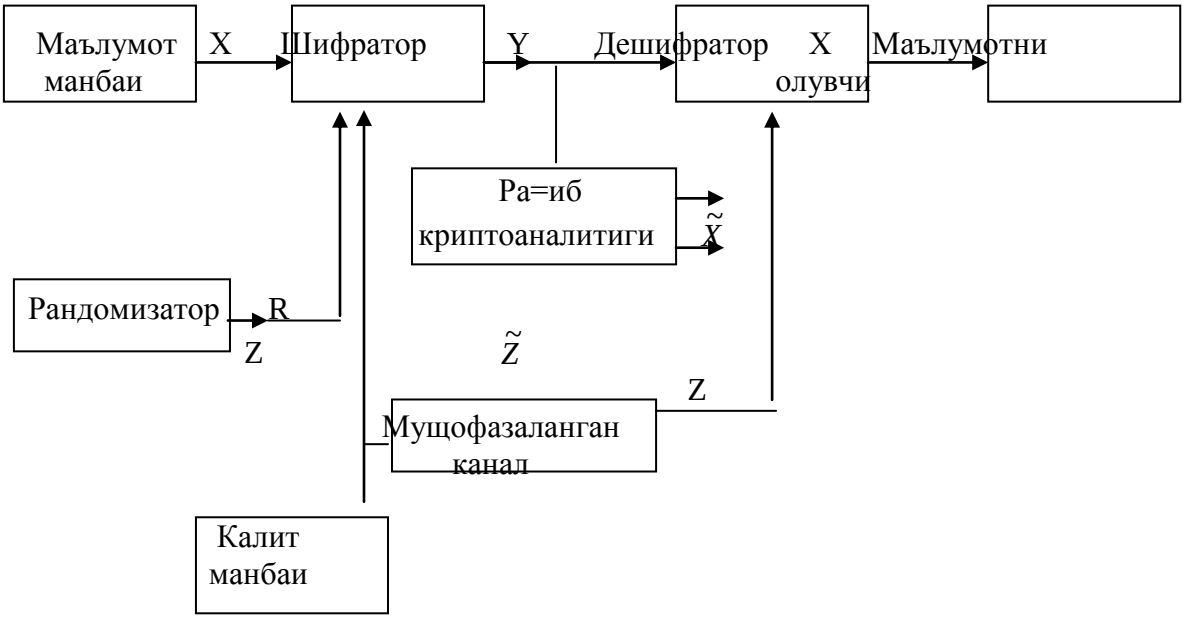
-шифрлаш алгоритмининг таркибидаги элементлар ўзгармас былиши керак;

-шифрлаш жараёни давомида маълумотларга киритиладиган =ышимча битлар шифрланган текстда тўла ва шнончли щолда =ўлланилган бўлиши керак;

-шифрлаш жараёнида =ўлланиладиган калитлар орасида содда ва осонлик билан ўрнатиладиган бо\ли=лар бўлмаслиги керак;

-калитлар таркиби тыпламидан олинган ихтиёрий калит ахборотларнинг ишончли мущофазасини таъминлаши керак;

-крипалгоритм дастурий щамда техник жищатдан амалий =ўлланишга =улай бўлиб, калит узунлигининг ўзгариши шифрлаш алгоритмининг сифатсизлигига олиб келмаслига керак.



Расм 1.

Ю=орида келтирилган расмдаги схема Шенноннинг 1949 йилдаги илмий ишларида [4,5] келтилрилган "Умумий махфий ало=а тизими схемаси"дан шифрлаш жараёнига рандомизатор киритилганлиги билан фар=ланади. Рандомизация аутентификация масалаларида мущим ўрин тутади. Рандомизатор ва рандомизация жараёнларини маъносини тушунтириб ўтамиз.

Инглиз тилидаги матн сўзларида "е" щарфи бош=а щарфларга нисбатан кыпро= такрорланади. Инглиз тилидаги матнларининг щарфларини инглиз тили алфатини белгиларидан кенг былган белгили (щарфли) алфавит белгиларига эга бўлган алфавитдаги матн билан алмаштириб ва бунда, хусусан, "е" щарфи ва шу каби бош=а кўп такрорланувчи щарфларни кенг бўлган алфавитнинг тасодифий белгилари (щарфлари) билан алмаштирилиб, кенг алфавит белгилари бир хил (текис) та=симланган (бир хил частота билан такрорланадиган) шифрматн олиш жараёни рандомизациялаш деб аталади. Бундай рандомизация =илинган шифрматнлар, бирор ани= тил алфавитида ёзилган текстлардаги сўзларда алощида олинган щарфларнинг такрорланиш частотасига асосланган щолда дешифрлаш услубларига бардошли бўлади. Яъни, рандомизация =илинган шифрматнларни алфавит щарфларининг матн сўзларида такрорланиш частотасига асосланган щолда дешифрлаш имкониятлари йы=. Аммо маълумотни ха=и=ий олиши керак бўлган эгаси олинган шифрматнни калит билан очиб очи= матнни олгандан сўнг рандомизация жараёнида =ўлланилган тасодифий белгиларни кенг такрорланувчи щарфлар билан алмаштириб, ща=и=ий очи= матнни олади. Рандомизация =илинган шифрматнлар "кўпкаррали алмаштиришли шифрматнлар" ёки "тенг частотали шифрматнлар" дейилади. Буюк математик Гаусс кып каррали алмаштиришли шифрлаш услубидан фойдаланиш дешифрлаш мумкин бўлмаган шифрматнларни беради, деб хатога йўл =ыйган. Чунки расм 1. да кетирилган рандомизаторли схема Шенноннинг "Умумий махфий ало=а тизими схемаси"га фа=атгина (вазифаси ю=орида баён =илиб ўтилган) рандомизаторнинг =ўшилгани билан фар= =илади.

Шу нарса мущимки, X, Y ва Z –ми=дорларни тасодифий деб тушунмо= керак. Бунда очи= матннинг статистик хоссалари маълумотлар манбаи билан ани=ланади, махфий калит Z ва рандомизациялаш кетма-кетлиги R ми=дорларнинг статистик хоссалари криптографга маълум. Расм 1. да келтирилган схемага асосан X, Z ва R ми=дорлар статистик ну=таи назардан бо\ли= эмас. Ра=иб томон криптоаналитиги фа=ат узатилаётган маълумотнниг Y-криитограммасига эга былган щолда X – очи= матнни тиклашга щаракат =илиб, Z - махфий калитнинг бирор $\tilde{Z}$ кўринишдаги щолатини (бащосини) олади ва унга кўра очи= текстнинг бирор $\tilde{X}$ кырынишини (бащосини) олади.

Криптографик системаларнинг назарий ва амалий бардошлилиги

Шеннон криптографик системаларнинг бардошлилиги масаласига икки хил ну=таи назар билан =аради. Биринчидан, назарий бардошлилик масаласини кырди: "Ра=иб криптоаналитиги криптографик системанинг криптоанализи учун етарли даражадаги техник ва бош=а керакли воситаларга эга бўлса щамда криптоанализ муддати чегараланмаган бўлса, ушбу криптографик системанинг бардошлилиги =андай?" ([5], с. 360). Криптографик системанинг назарий бардошлилиги тушунчаси криптографик системаларни бащолашга ани=лик киритади, лекин бардошлилиги ю=ори былган криптосистемаларнинг яратилиши ну=таи назардан тушкунликка олиб келади: амалда кўплаб щолларда назарий бардошли криптосистемаларнинг яратилиши махфий калитнинг щажмини чексиз катта бўлиб кетиши масаласи билан бо\ли=. Шунинг учун Шеннон криптосистемаларнинг амалий бардошлилиги масаласини щам кўрди: агарда ра=иб криптоаналитиги криптоанализ учун етарли даражадаги воситалар билан таъминланмаган бўлса ва анализ муддати чегараланмаган бўлса криптосистеманинг бардошлилиги =андай? Шу ерда алощида таъкидлаб ўтамизки, очи= калитли криптосистемалар амалий бардошли бўлиб, назарий бардошли бўлишлари шарт эмас.

Мутла=о махфийлик

Шеннон криптосистемаларнинг назарий бардошлилик масалаларида =уйидаги коидаларни =абул килди:

1) махфий калитдан фа=ат бир марта фойдаланилади, яъни X –очи= матннинг M та белгисини шифрлагандан сўнг Z - махфий шифрлаш калитини ва R - рандомизаторини алмаштириш керак;

2) ра=иб криптоаналитиги Y - криптограммага эга ва шунинг учун фа=ат шифрматнга асосланган щолда криптоанализ услубларидан фойдаланиб очи= матннинг $\tilde{Z}$ - бащосини щамда махфий калитнинг $\tilde{X}$ - бащосини олиши мумкин.

Шеннон мутла=о махфийлик тушунчасининг таърифини: X - очи= матн ва Y -криптограмма статистик бо\ли= эмас, яъни ихтиёрий очи= матн ва криптограмма учун $P(X = x/Y = y) = P(X = x)$, деб берди. Яна щам бош=ача =илиб айтганда мутла=о махфийлик: криптоаналитик очи= матннинг криптограммасига эга бўлган щолда, очи= матн бащосини ани=лигини барча дешифрлаш воситалари ва ва=ти чегаралланмаганлиги имконияти мавжуд бўлганда щам тыла щолда бащолай олмайди, деган маънони англатади. Шеннон мутла=о мащфийликнинг мана шундай ани= (математик) таърифини бериб, мутла=о махфий криптографик системаларнинг мавжудлигини кырсатади. Ща=и=атан щам белгилари шартли равишда $\{0, 1, ..., L-1\}$ тыпламдан (элементлари сони L та былган) иборат былган, махфий калит узунлиги K ва криптограмма узунлиги N очи= матн узунлиги M билан тенг былган, яъни $K = N = M$ былган, рандомизация =илинмаган шифрматинни

кырайлик. Шифрлаш жараёни L модул быйича =ышиш амалига асосланган былсин, яъни

$$Y_i = X_i \oplus Z_i, \quad i = 1, 2, ..., \ M \qquad (2)$$

Комбинаторика курсидан маълумки, L та белгидан фойдаланиб узунлиги *M* та тенг былган, яъни белгилари сони *M* та бўлган барча мумкин бўлган (шартли) сўзлар тўпламининг элементлари сони L^M та бўлади. Шунинг учун мумкин бўлган барча калитлар тўпламидан бирор элементнинг (калитнинг) анализ =илинаётган криптограмманинг (ю=орида айтиб ўтилган параметрли) калити эканлиги эщтимоли $P(Z = z) = L^M$ бўлади. Мос равишда $x_i \in X_i$ ва $y_i \in Y_i$ бўлган элементлар учун (2) тенгликни =аноатлантирувчи ягона $z_i \in Z_i$ элемент мавжуд. Шунинг учун X нинг статистик хоссаларига бо\ли= бўлмаган щолда ихтиёрий *x* ва ***y*** элементлар учун $P(Y = y / X = x) = L^M$ тенглик ўринли бўлади. Шундай =илиб, X ва *V* статистик бо\ли= эмас щамда L модул быйича =ышиш амалига асосланган Вернам криптосистемаси Шеннонниг мутла=о махфийлик таърифи шартларнинг =аноатлантиради. Всрнам криптосистемаси "шифр-блокнот" номи билан иккинчи жащон уруши ва ундан кейинги даврларда щам разведка хизмати ва бош=а шу каби хизмат ходимлари томонидан кенг =ўлланилган. Разведка ходимларига бирор (тасодифий) махфий калитли, яъни узунлиги шифрланаётган матннинг узунлигига (ёки криптограмма узунлигига) тенг бўлган 0 дан L гача бўлган сонлардан тузилган бирор тасодифий сонли кетма-кетликдан иборат бўлган "шифр-блокнот" берилиб, ундан маълумотни шифрлаш учун фа=ат бир марта фойдаланиш мумкинлиги таъкидланган. Криптография сощаси мутахассислари бундай усулнинг мутла=о бардошлилигига тыла ишонч щосил =илган былсаларда, бу усулнинг, ща=и=атан щам, тўла бардошлилигини, биринчи былиб Шеннон назарий жищатдан исботлаб берди. Вернам криптосистемасидан фойдаланишда махфий калитнинг битта белгисини, шифрланиши керак былган матннинг щам фа=ат битта белгисига бо\ли=лиги, бу криптосистемани махфийлиги ю=ори даражада таъминланиши керак бўлган кичик щажмдаги матнларгагина яро=ли былиб (мисол учун Тошкент – Вашингтон щукумат ало=а тизимида), катта щажмдаги матнларга =ылланиш имкониятларини баъзан чегаралаб =ыяди. Чунки катта щажмдаги матнни мущофазасида Вернам криптосистемасининг =ылланиши махфий калитнинг щам щажмини очи= матн щажми даражасида катта былишини талаб этади.

Таянч иборалар

Кодлаштириш криптотахлил, аутентификация идентификация, ыринларни алмаштириш усули, алмаштириш усули, гаммалаштириш, тахлилий ызгартириш.

Назорат саволлари

1. Криптография щимоясида шифрларга нисбатан =андай талаблар =ыйилади.
2. Криптография щимоясида =андай усуллар =ылланилади?

Асосий адабиёт

1. Анохин М.И., Варнавский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. М. 1997г.
2. Брюс Шнайер. Прикладная криптография: 2– е издание. М. 2001.
3. Фомичев В.М. Дискретная математика и криптология. М. «Диалог МИФИ» 2003 г. http: ‖ www.library.mephi.ru – Библиотека МИФИ.
4. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М. «Радио и связь» 2001г.
5. Московский центр непрерывного математического образования. Материалы 1 – 9 олимпиад по криптографии. М. 2001 – 2003гг. http: ‖ www. ibc.ry./- электронная библиотека Московского Государственного Университета экономики, статистики и информатики.
6. В.А.Хорошко, А.А.Чекатков. Методы и средства защиты информации. Издательство «ЮНИОР» К. 2003.

Кушимча адабиёт

1. Анин Б. Защита компьютерной информации. Санкт – Петербург, 2002.
2. Завгородный В.И. Комплексная защита информации в компьютерных системах., М. «Логас», 2001.
3. А.В.Домашев, М.М.Грунтович, В.О.Попов, Д.И.Правиков, А.Ю.Щербаков, И.В.Ппокофьев. Программирование алгоритмов защиты информации. Учебное пособие. Издательство «Нолидж». М. 2002.

Маъруза 5

Мутла=о махфий криптосистемаларнинг калитларига =ыйиладиган талаблар

1. Криптографик калитларни бош=ариш.
2. Мукаммал былмаган шифрларни очиш.
3. Ишончлилик ва алдов.
4. Амалий бардошлилик.

Назарий бордошлилик масалаларига тегишли былган саволлар билан шу\улланишда Шенноннинг ахборотлар назариясида аоссий сонли =иймат –

«ноани=лик» (ёки «энтропия») деб аталувчи тушунчадан фойдаланамиз. Ноани=лик – тасодифий ми=дорлар эщтимоллигига мос келувчи та=симот функцияси лагорифиминин манфий ишора билан олинган ифодасини математик =утилмасидан иборат. Яъни $H(X/Y)$ (бу ифода бирор ани= ми=дорда номаълум ми=дорнинг бащоси ноани=лиги, деб бы=илади) ноани=лик $P(X = x/Y = y)$ (эщтимоллик =иймати логарифиминин математик =утилмаси тенг:

$$H(X/Y) = \sum_x \sum_y P(X = x/Y = y)[-\log P(X = x/Y = y)]$$

бу ерда йи\индилар X, Y - тасодифий ми=дорларнинг барча мумкин бўлган =ийматлари бўйича щисобланади. Ноани=ликлар, табиий бўлган =уйидаги

$$H(X/Y)H(X) + (Y/X)$$

=оидани =аноантлантиради. Ноани=ликлар тушунчаси ор=али берилган ушбу:

$$H(X/Y,\ Z,\ R) = 0 \qquad (3)$$

$$H(X/Y,\ Z) = 0 \qquad (4)$$

ифодалар мос равишда =уйидагича тушунилади: (3) тенглик ўринли бўлади шунда ва фа=ат шунда, =ачонки, X, Z, R ми=дорлар биргаликда Y ми=дорни бир =ийматли ани=ласа ва (4) тенглик ўринли бўлади шунда ва фа=ат шунда, =ачонки, Y ва Z ми=дорлар биргаликда X ми=дорни бир =ийматли ани=ласа. Мутла=о махфийлик таърифини

$$H(X/Y) = H(X) \qquad (5)$$

кўринишида ифодалаш мумкин. Чунки бу охирги тенглик фа=ат ва фа=ат X ва Y ми=дорлар статистик ну=таи назардан бо\ли= былмагандагина ўринли былади.

Махфий калитли криптосистемалар учун ушбу тенгсизлик

$$H(X/Y) \le H(X,\ Z/Y) = H(Z/Y) + H(X/Y,\ Z) = H(Z/Y) \le H(Z) \qquad (6)$$

ўринли бўлади. Бу ерда (4) тенгликдан ва маълум маълумотларнинг щажмини =ис=ариши табиий холда ноани=лик =ийматининг ўсишига олиб келишлигидан фойдаланилган. Агарда криптосистема ахборотларни мутла=о махфийликни таъминласа, у щолда (5) ва (6) тенгликлардан ушбу

$$H(Z) \ge H(X) \qquad (7)$$

тенгсизлик келиб чи=ади.

Ю=оридаги (6) тенгсизлик – мутла=о махфий системалар учун Шеннон чегарасини ани=лайди: махфий калитнинг ноани=лик =ийматидаи шу калит билан шифрланадиган матннинг ноани=лик =ийматидаи кичик бўлмаслиги керак. Агарда махфий калит элеметлари сони L_z бўлган алфавитнинг белгиларидан тузилган бўлиб, унинг щажми (узунлиги) K га тенг (яъни калитни ташкил этувчи белиларнинг умумий сони Kга тенг) бўлса, у щолда махфий калитнинг ноани=лик =ийматн бащосини ифодаловчи ушбу

$$H(Z) \le \log(L_Z^K) = K \log L_Z , \qquad (8)$$

тенгсизликда тенглик фа=ат махфий калит мутла=о тасодифий бўлгандагина бажарилади. Худди шу каби очи= матн элементлари сони L_x бўлган алфавитниг белгиларидан тузилган бўлиб, уни ташкил этувчи белгиларнинг умумий сони бўлса, у щолда очи= матннинг =уйидаги ноани=лик =ийматн бащосида

$$H(X) \le M \log_X , \qquad (9)$$

тенглик фа=ат очи= матн бутунлай (мутла=о) тасодифий бўлгандагина бажарилади. Шундай =илиб, агарда $L_x = L_z$ бўлиб, очи= матн бутунлай тасодифий бўлса, охирги (8) ва (9) муносабатлардан Шеннон чегарасини ани=ловчи (7) муносабатдан $K \ge M$ тенгсизликка эга бўламиз. Бу муносабат эса калитнинг щажми (узунлига) очи= матн щажмидан кам бўлмаслиги кераклигини кўрсатади. Калит узунлигининг =уйи чегарасига Вернам шифрлаш криптосистемасидан фойдаланилганда эришилади ва бунда $K = M$ бўлиб, калит узунлиги очи= матн узуллигига тенг бўлади.

Мукаммал былмаган шифрларни очиш

Мукаммал бўлмаган шифрларни очиш деганда, бирор берилган (эга бўлинган) криптограммага асосан криптоанализ услубларидан фойдаланиб, шу берилган криптограммага мос келувчи очи= матнни тиклаб, шифрлаш алгоритимини топиш жараёни тушунилади. Шеннон, криптоаналитик томонидан мукаммал бўлмаган шифрларнинг очилиши назарий жищатдан мумкинлиги масалаларини кўриб чи=ди. Бунинг учун, у калитнинг ишончсизлиги (бардошсизлиги) функциясини

$$f(n) = H(Z / Y_1,\ Y_2, ..., Y_n)$$

криптограмманинг дастлабки n та белгисига асосан анализ (тащлил) =илинаётган шифрматн (криптограмма) учун калитнинг ноани=лик ўлчови сифатида киритди. Бундан таш=ари, Шеннон анализ =илинаётган крип-

тограмманинг Z калитни бир=ийматли ани=ловчи дастлабки *n* та белгисидан иборат $(Y_1, Y_2, \ldots, Y_n)$ белгилар тўпламининг энг кичик щажмда былганининг элеметлари сонини яни $f(n) = 0$ тенгликни =аноатлантирувчи энг кичик *n* сонини ягоналик масофаси сифатида ани=лади. Агарда шифрланган матнинг (u тадан щам былмаган ми=дордаги белгилари щам маълум былса (анализ =илинаётган шифрматн *u* та щар-хил белгиларнинг комбинацияларидан иборат бўлса), у щолда $Y_1, Y_2, \ldots, Y_n$ белгиларга асосан махфий калитнинг фа=ат битта =ийматини топиш мумкин, яъни етарли даражада ва=т ва бош=а керакли воситалар билан таъминланган криптоаналитик шу тахлил =илинаётган криптограмманинг махфий калитини топиб шифрни оча олади. Бирор берилган "тасодифий шифр" учун Шеннон

$$u = \frac{H(Z)}{r \log L_y} \qquad (12)$$

муносабат ырынли эканлигини кырсатди. Бу ерда

$$r = 1 - \frac{H(X)}{N \log L_y} \qquad (13)$$

тенглик билан ани=ланувчи сон r- белгилари сони L_y бўлган алфавитда тузилган, щажми N былган (яъни криптограммани ташкил этувчи белгиларнинг умумий сони N бўлган) криптограмма матнида алфавитниг барча белгиларини такрорланишини (даврларининг ўртача =ийматини) ани=лайди. Кўплаб криптосистемаларда N=M ва $L_x=L_y$ бундай щолда инглиз тилидаги очи= текстлар учун r=3/4. Агарда $L_x=L_y$ бўлса ва калитнинг ягоналик масофаси мутла=о тасодифий бўлса, у щолда (8) ифодани щисобга олиб (12) ифодага кўра ушбу

$$u \approx \frac{K}{r} \qquad (14)$$

муносабатга эга быламиз.

Шундай =илиб, агарда инглиз тилидаги матнни шифрлаш криптосистемасида $L_x=L_y=L_z$ муносабатлар ўринли бўлса, у щолда бундай криптограммани шифрматннинг N=(4/3)К га бўлган (ёки u=(4/3)К тадан кам бўлмаган) белгиларидан фойдаланиб очиш мумкин. Мисол учун щажми 56 битдан (ASCII кодида саккизта 7 битли белгилардан) иборат бўлган махфий калитни шифрматннинг дастлабки 11 та 7 битли белгисини анализ =илиш билан тиклаш мумкии.

Криптосистемаларнинг махфий калитларини ягоналик масофаларинибахолашда Шеннон кўрсатган (12) тенглик билан аи=ланувчи ифодадан кенг фойдаланилади.

Ща=ли равишда,r=*0* бўлган щолда (12) ва (14) ифодаларнинг мазмуни =андай былиши ты\рисида савол ту\лади, яъни N=M, L_x =L_y бўлиб, очи= матн

мутла=о тасодифий: $H(X)=M\ log\ L_к=N\ log\ L_y$, бўлган щолда. Амалда мана шундай щолатга кўпро= дуч келинади. Ю=орида =ўйилган саволга =уйидагича жавоб берилади: бир томондан $r\to 0$ бўлса (14) тенгликда $u\to\infty$ бўлиб, калитнинг узунли очи= матн узунлиги M га нисбатан жуда кичик бўлганда щам, яъни $K<M$/ бўлганда щам криптоаналитик щеч =ачон криптосистемага асосини ташкил этувчи алгоритмни оча олмайди;

иккинчи томондан эса $K < M$ бўлиши (10) тенгсизликка зид бўлиб, бундай крипосистема мутла=о махфийликни таъминлай олмайди. Бундай па радоксни (юзаки =араганда зиддиятли щолатни): мутла=о махфий криптосистемаларда криптограмма (шифрланган матн). У очи= матн ща=ида щеч =андай маълумотни ўз ичига олмаслиги, яъни Y ва X ми=дорларнинг статистик ну=таи назардан бо\ли= эмаслиги щамда X ми=дорни У ми=дор бир =ийматли ани=лаши учун Y ми=дорнинг X ми=дорга нисбатан бо\ли=лиги ща=ида мумкин =адар кыпро= маълумот былиши талаб этилиши билан тушунтирилади. Ща=и=атан щам, мутла=о тасодифий былган X-очи= матннинг Y – криптограммасини очиш учун Z – махфий калит мутла=о тасодифий танланади. У щолда щар бир Y – криптограмма X – очи= матннинг ва Z – махфий калитнинг L_z^K тадан мумкин былган ифодалари мос келадиган ва бу ифодаларнинг щар бири бир хил эщтимоллик билан Y – криптограммага мос келади. Маълум былган Y – криптограммага, ща=и=атан щам мос былган очи= текст X ва махфий калит Z ларни, ю=орида айтилган, мумкин былган барча тенг эщтимолли L_z^K та мос ифодалар ичидан танлаб олиш учун эса криптоаналитик щеч =андай =ышимча маълумотга эга эмас. Худди мана шу щолатда Шеннон табиий равишда: маълумотларни си=иш, яъни маълумотларни шифрлашда криптограмманинг узунлиги (щажми) очи= текст узунлигидан (щажмидан) кичик былиши – криптографияда фойдали восита, деб ты\ри хулоса чи=арди. Шундай =илиб, маълумотларнинг щажмини си=ишнинг мукаммал алгоритми маълумотлар манбаини мутла=о тасодифий былган маълумотлар манбаига айлантиради. Аммо шу пайтгача маълумотлар манбаи учун бир пайтнинг ызида мукаммал ва амалий жищатдан =улай былган маълумотларни си=иш алгоритми яратилган эмас. Шундай былсада, маълумотларни си=ишнинг мукаммал былмаган алгоритмлари щам r ми=дорнинг сезиларли камайишига ва бунинг натижасида ягоналик масофаси ми=дори u нинг ысишига олиб келади. Дастлабки, маълумотлар техник воситаларсиз тащлил =илиниб келинган даврларда щам, криптографлар очи= матндан маълумотни =абул =илувчи томонидан осон тикланиши мумкин былган алфавит белгиларини чи=ариб ташлаганлар. Мисол учун:

С+ШГАМСОЛД.

Ягоналик масофасининг (12) ифодасини Шеннон рандомизациялашни щисобга олмаган щолда келтириб чи=арган. Бу ифода рандомизациялаштирилган шифрматнлар учун щам былиши учун (13)

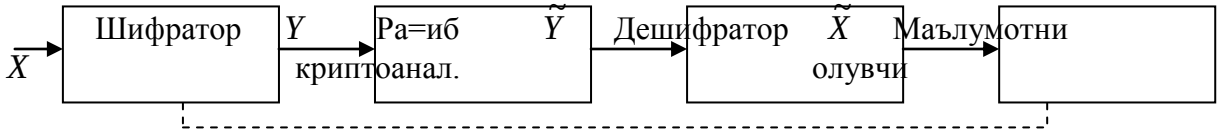
ифодада $H(X)$ ми=дорни $H(X, R)$ ми=дор билан алмаштириб =араш лозим. Бундан эса раномизациялаш щам r ми=дорни камайишига олиб келиши келиб чи=ади. Тажрибалар криптографлар ишида очи= матнни ташкил этувчи алфавит белгиларининг статистик хоссаларини асли щолатини яширишда (ызгартиришда) берилган матнга =ышимча белгилар киритишни =улай усул эканлигини кырсатди. Мисол учун:

+ЫШХИМХЧАХКХРИХ ТИШГАХМХИСОЛХ

Ишончлилик ва алдов

Биз ю=орида криптографиянинг ма=сади – ахборот ёки маълумотларнинг махфийлигини ва уларнинг ща=и=ийлигини таъминлашдан иборат эканлигини бир неча бор таъкидладик. Аммо ахборот ёки маълумотларнинг махфийлиги ва уларнинг ща=и=ийлиги масалалари алощида хоссаларга эга. Ща=и=атан щам криптограммани олиб ва уни дешифрлаб керакли очи= матнни олгандан сынг, бу криптограммани махфий калитга ваколатсиз эга былган шахс томонидан юборилмаганлигига, яъни махфий калитга эгаликка ваколати былган шахс томонидан юборилганлигига =андай тыла ишонч щосил =илиш мумкин? Мана шундай йыналишдаги масалаларнинг ечими билан, яъни аутентификация масалалари билан Г.Дж. Симмонс шу\улланиб, Шенноннинг махфий ало=а назарияси каби, ызининг аутентификация назариясини яратди [12].

Аутентификация системасининг назарий бардошлилиги ща=идаги масалани Симмонс криптоаналитик расм 1.да былган щолатидан =улайро= былган расм 2. щолатида былганда, яъни криптоаналитик сохталаштирилган $\bar{Y}$ - криптограммани маълумотни олиши керак былган шахснинг дешифраторига юбориш имкониятига эга былган щолатдан келиб чи=аб ырганди.



Расм 2.

Бундай сохталаштирилган криптограмманинг сохталиги ани=ланиб маълумотни олувчи шахсга жынатилмайди. Шунинг учун расм 2.да шифратор билан маълумотни олувчи шахс орасидаги ало=а узлукли чизи= билан белгиланган.

Симмонс, Шеннон каби махфий калит Z (ща=и=ий былган) криптограммани яратишда фа=ат бир марта фойдаланилади, деб =абул =илди. Шундай былганда щам криптоаналитик =уйидаги мущим имкониятларга эга эканлигини, Симмонс назардан =очирмади:

1. Ра=иб криптоаналитиги ща=и=ий былган Y – криптограмманинг келишини кутмай сощта $\overline{Y}$ - криптограммани ща=и=ий криптограмма юборилиши керак былган шахсга етказиши мумкин (бундай щолат иммитация =илиш щолати дейилади) ва шунинг учун расм 2.да маълумот манбаи шифратори билан криптоаналитик орасидаги ало=а узлукли чизи= билан кырсатилган. Иммитация =илиш муваффа=иятли кечган щисобланади, агарда ща=и=ий криптограммани олиши керак былган шахснинг дешифратори сохта $\overline{Y}$ - криптограммани ща=и=ий криптограмма Y сифатида =абул =илса (хаттоки, бунда кейинро= сохта $\overline{Y}$ - криптограмма билан ща=и=ий Y - криптограмма мос тушса щам).

2. Ра=иб криптоаналитиги сохта $\overline{Y}$ - криптограммани ща=и=ий Y - криптограммадан кейин щам етказиши мумкин (бундай щолат алмаштириш дейилади) ва алмаштириш жараёни муваффа=иятли кечган щисобланади, агарда сохта криптограмма $\overline{Y}$ дешифратор томонидан ща=и=ий криптограмма Y сифатида =абул =илиниб, $\overline{Y}$ га мос келувчи дешифрланган очи= матн $\overline{X}$ ща=и=ий криптограмма Y дешифрлангандаги очи= матнга мос келмаса, яъни $\overline{X} \neq X$ былса, иммитация ва алмаштириш жараёнларини муваффа=иятли кечиши эщтимолликларининг энг ю=ори =ийматларини мос равишда P_I ва P_S деб белгилаймиз. Симмонс $\max(P_I, P_S) = P_d$ ми=дорни алдов эщтимоллиги ми=дори сифатида киритди, яъни криптоаналитик Ра=иб томонни мана шундай эщтимоллик билан алдай олади. Аутентификация назариясининг масалалари кып =иррали ва ызига хос хусусиятларга эга былиб, алощида илмий изланишларни талаб этади.

Амалий бардошлилик

Ю=орида кыриб ытганимиздек, бирор ани= чекли щажмдаги калит билан шифрлаш криптосистемалари (яъни $K < H(X)$ былган) ягоналик масофаси ми=дори чексиз катта =ийматга эга былиши мумкин ва натижада бундай криптосистемалар мутла=о махфийликни таъминлайди. Шеннон шундай шундай системаларни идеал шифрлаш криптосистемалари деб атади ва бундай системаларни яратишда щал =илиб былмайдиган табиий тыси=лар келиб чи=ишини щам таъкидлади. Амалдаги кыплаб криптосистемаларнинг бардошлилиги уларнинг шифрлаш алгоритмнинг калитини назарий жищатдан топиш масаласининг ечиб былмаслигига эмас, балки алгоритм калитини топиш масаласининг амалий жищатдан мураккаблигига асосланган былиши керак. Ща=и=атан щам, Шеннон шифрматн ва унинг ташкил этувчи белгиларига асосан махфий шифрлаш калитини топиш учун энг замонавий воситалардан фойдаланган щолда сарф быладиган ыртача ва=тни (яъни шу шифраш криптосистемаси алгоритмининг) иш характеристикаси деб атади. Щажми n былган шифрнинг иш характеристикасини W(n) деб белгилаймиз. W(n) катталикни $n \to \infty$ былгандаги =иймати мущим былиб, бу =ийматни чексиз щажмдаги шифрматнни очиш учун бажарилиши зарур быладиган

ыртача ишни (ёки иш ва=тини) ифодалайди. Шундай =илиб, бирор криптосистема учун W(n) ми=дорни ани=лашда =уйидаги алощида мураккабликка эга былган масала келиб чи=ади: шифрни очишнинг энг яхши услубини топиш, яъни оптимал (самарали) тащлил билан W(n) ми=дорнинг =уйи =ийматини ани=лаш. Щозирда криптосистемалар учун W(n) ми=дорнинг $n \to \infty$ даги =ийматини =уйи чегарасини ани=ловчи бирор кенг мазмунли илмий асосланган услуб мавжуд эмас. Амалдаги криптосистемалар (шифрлар) одатда иш характеристикасининг эришилган бащоси деб аталувчи ми=дор билан бащоланади, $W_h(\infty)$ ми=дор шифрланган матнинг n та белгисига асосланиб, берилган шифрни энг самарали воситалардан фойдаланган щолда тащлил =илиб, шифрлаш алгоритмининг калитини топиш зарур былган, яъни сарфланиши керак былган ыртача ва=т ми=дори. Криптоанализ услубларининг такомиллашиб бориши W(n) ва $W_h(\infty)$ ми=дорларнинг тегишли криптосистемалар учун мумкин =адар ани= =ийматларини топиш имкониятларини кенгайиб боришини таъминлайди.

Мутла=о бардошли амалий шифрлаш алгоритмлари мавжудлиги

Шеннон ызининг «Махфий системаларда ало=а назарияси» илмий ишида шифрлаш алгоритмларининг амалий бардошлилиги масалаларини тащлил =илиб, бу борадаги натижаларни математик теоремалар кыринишида ифодалаш учун керак быладиган тушунчаларни (аксиомаларга ыхшаш былган дастлабки асосларни) ани=лаш мушкул эканлигини таъкидлаган. Иш характеристикаси W(n) ва унинг $n \to \infty$ былгандаги $W_h(\infty)$ =ийматларини щисоблашнинг ани= бирор умумий услубини яратиш масаласи ечилган эмас. К-битли калит билан ахборотлар билан ахборотлар матнини (белгиларини) группалаб ва рандомизациялаш билан шифрлаш криптосистемаси учун $W(\infty) \approx 2^{K/2}$ эканлиги маълум былиб, бунда иш характеристикаси бирлиги натижаси 0 ва 1 былган оддий имкониятларни танлашдан иборатдир. Ахборотни =абул =илиб олувчи шахс олинган криптограммани дешифрлашга киришиши учун [ ]та битнинг ало=а тизими воситалари ор=али етиб келишини кутишга мажбурдир. Агарда биз дешифрлаш имконияти ту\илгунча миллион йил кутишга рози былсак, у щолда ишонч билан айтишимиз мумкинки, криптоаналитикга бу криптограммани очиши учун минг йил керак былади

Таянч иборалар

Энтропия, ягоналик масофалари, Шеннон теглиги, сохта криптограмма, маълумотларни си=иш, радиомизация, аутентификация, имитация, шифрнинг иш характеристикаси функцияси.

Назорат саволлари

1. Калитнинг ишончсизлик функцияси тушунчаси.
2. Маълумотлар щажмининг си=ишнинг мукаммал алгоритм ища=ида.
3. Аутентификация системасининг назарий бардошлилиги ща=ида.

Асосий адабиёт

1. Анохин М.И., Варнавский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. М. 1997г.

2. Брюс Шнайер. Прикладная криптография: 2– е издание. М. 2001.

3. Фомичев В.М. Дискретная математика и криптология. М. «Диалог МИФИ» 2003 г. http: ‖ www.library.mephi.ru – Библиотека МИФИ.

4. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М. «Радио и связь» 2001г.

5. Московский центр непрерывного математического образования. Материалы 1 – 9 олимпиад по криптографии. М. 2001 – 2003гг. http: ‖ www. ibc.ry./- электронная библиотека Московского Государственного Университета экономики, статистики и информатики.

6. В.А.Хорошко, А.А.Чекатков. Методы и средства защиты информации. Издательство «ЮНИОР» К. 2003.

Кушимча адабиёт

1. Анин Б. Защита компьютерной информации. Санкт – Петербург, 2002.

2. Завгородный В.И. Комплексная защита информации в компьютерных системах., М. «Логас», 2001.

3. А.В.Домашев, М.М.Грунтович, В.О.Попов, Д.И.Правиков, А.Ю.Щербаков, И.В.Ппокофьев. Программирование алгоритмов защиты информации. Учебное пособие. Издательство «Нолидж». М. 2002.

Маъруза 6

Очи= калитли шифрлаш алгоритмлари
Очи= калитли криптосистемалар

1. Очи= калитли криптосистемалар.
2. Бир томонли функциялар.
3. Калитларнинг очи= та=симланиш алгортми
4. Очи= калитли RSA криптосистема

Криптографик система =анчалик мураккаб ва ишончли алгоритмга асосланган былмасин, унинг амалий =ылланишида келиб чи=адиган нозик масала, яъни криптосистемалардан фойдаланувчиларга калитларни та=симлаш масаласи мущим былиб =олаверади. Ща=и=атан щам, ахборотлар тизимида махфий ало=ани таъминловчи криптографик система фойдаланувчиларининг ызаро ало=аси учун калит уларнинг бири ор=али яратилган былиб, иккинчисига махфий щолда етказилиши лозим былади. Бундан келиб чи=адики, умуман олганда, калитни етказиш (узатиш) учун щам яна бош=а криптосистемадан фойдаланишга ты\ри келади. Бу масалани ечиш учун классик щамда замонавий фан ва техника юту=ларига, хусусан, алгебра фани юту=ларига асосланган щолда очи= калитли криптосистемалар яратиш йыналиши вужудга келди. Очи= калитли криптосистемаларнинг мощиятини =уйидагилар ташкил этади:

1. Ахборотлар тизими криптосистемасидан фойдаланувчиларнинг щар бири маълум =оида билан бо\ланган иккита калитни яратади (тузади).
2. Бу тузилган (яратилган) калитлардан бири очи= эълон =илинади, иккинчиси эса сир (махфий) са=ланади.
3. Дастлабки очи= калит билан шифрланиб, тегишли фойдаланувчига узатилади, бунда шифрланган матнни (криптограммани) бу очи= калит билан дешифрлаш имконияти йы=, яъни шифрланган матнни бу очи= калит билан очиш имконияти йы=.
4. Узатилган (етказилган) криптограмма фа=ат криптограмманинг ща=и=ий эгасигагина маълум былган иккинчи махфий калит билан дешифрланади.

Очи= калитли криптосистемалар тескариси мавжуд былмаган ёки тескарисини щозирги замонавий фан ва техника юту=ларидан фойдаланган щолда =опланмайдиган даражада жуда катта моддий сарф-харажатлар билан щамда керагидан кып ва=т сарфлаш билан ани=ланадиган функцияларга ёки алгоритмларга асосланади. Шундай функциялар ёки алгоритмларни =уйидаги хоссага эга былиши ма=садга мувофи=: берилган x =ийматда $f(x)$ функциянинг =иймати y етарли даражада осон щисобланади, аммо бирор номаълум x =ийматда функциянинг =иймати $y = f(x)$ маълум былса, x =ийматни топишнинг щам моддий жищатдан щам ва=т ну=таи назаридан етарли даражадаги имконияти йы=.

Очи= калитли криптосистемалар алгоритмлари уларнинг асосини ташкил этувчи бир томонли функциялар билан фар=ланади. Аммо щар =андай бир томонли функция щам очи= калитли криптосистемалар яратиш учун ва улардан амалдаги ахборотлар тизимида махфий ало=а хизматини ырнатиш алгоритмини =уриш учун =улайлик ту\дирмайди.

Бир томонли функцияларни ани=лаш таърифида назарий жищатдан тескариси мавжуд былмаган функциялар эмас, балки берилган функцияга тескари былган функциянинг =ийматларини щисоблаш амалий жищатдан ма=садга мувофи= былмаган функциялар тушунилиши таъкидланган эди. Шунинг учун маълумотнинг ишончли мущофазасини таъминловчи очи= калитли криптосистемаларга мущим былган =уйидаги талаблар =ыйилади:

1. Дастлабки очи= матнни шифрматн кыринишида ытказиш бир томонли жараён ва шифрлаш калити билан шифрматнни очиш – дешифрлаш мумкин эмас, яъни шифрлаш калитини билиш шифрматнни дешифрлаш учун етарли эмас.

2. Очи= калитнинг маълумлигига асосланиб, махфий калитни замонавий фан ва техника юту=лари ёрдамида ани=лаш учун быладиган сарф-харажатлар щамда ва=т ма=садга мувофи= эмас. Бунда, шифрни очиш учун бажарилиши керак быладиган энг кам ми=дордаги амаллар сонини ани=лаш мущимдир.

Очи= калитли шифрлаш алгоритмларидан ахборотлар тизимида маълумотларнинг махфийлигини таъминлашда замонавий ил\ор услуб сифатида фойдаланиб келинмо=да. Очи= калитли криптосистемаларни яратишнинг RSA алгоритми жощон стандарти сифатида =абул =илинган. Бу ща=ида кейинги былимларда алощида тыхталамиз.

Умуман олганда, замонавий очи= калитли криптосистемалар =уйидаги типдаги акслантиришларга (функцияларга) таянади:

1. Катта сонларни туб кыпайтувчиларга ёйиш.
2. Чекли сонли майдонларда логарифмларни щисоблаш.
3. Алгебраик тенгламаларнинг илдизларини щисоблаш.

Шу ерда таъкидлаш лозимки, очи= калитли криптосистемалар алгоритмларидан=уйидаги ма=садларда фойдаланилади:

1. Са=ланувчи ва узатиладиган маълумотларнинг махфийлиги мущофазасини таъминловчи муста=ил восита сифатида.
2. Калитлар та=симотининг мущофазасини таъминловчи восита сифатида. Очи= калитли криптосистемалар алгоритмлари анъанавий криптосистемалар алгоритмларига нисбатан мураккаб былиб, ундан кыпро= калитларни та=симлашда фойдаланилади. Сынгра катта щажмдаги маълумотларни узатишда соддаро= былган системалардан фойдаланилади.
3. Аутентификация, яъни маълумотларнинг ща=и=ийлигини ани=лаш услублари воситаси сифатида. Бу ща=ида «Электрон имзо» былиижа батафсил тыхталамиз.

+уйида нисбатан оммавийлашган очи= калитли криптосистемаларни =ис=а кыриб ытамиз.

Бир томонли функциялар

Ю=орида айтиб ытилгандек, Шенноннинг 1949 йилдаги ма=оласи [5] криптология сощасидаги очи= илмий изланишларнинг кыпайишига олиб келмади. Биринчидан, бу ма=олада келтиирлган «махфий ало=а системаларининг назарий бардошлилик назарияси» мощияти жищатидан атрофлича ва тыла былиб, бундай назарияга кыра махфий ало=а канали быйлаб узатиладиган калитнинг щажми, узатиладиган маълумотнинг щажмини катталишиб бориши билан катталашиб боради. Иккинчидан, Амалий бардошлилик масалаларининг ечимлари ща=идаги илмий натижалар, янги криптосистемалар яратиш йыналишларининг вужудга келишидан кыра, кыпро= мавжуд криптосистемаларнинг такомиллашувига олиб келди. Шундай былсада, Шенноннинг бу назариясидаги «етарли даражадаги (амалий) бардошли криптосистемалар яратиш масаласи, мощияти жищатидан, маълум шартларни =аноатлантирувчи ва ечими сарф-щаражатларни =опламайдиган мураккаб масалага асосланиши керак», деб ифодаланган изощи, станфордлик олимлари У.Диффи ва М.Е.Хеллманларнинг илмий изланишларининг самарали натижаларида ыз аксини топди. Уларнинг 1976 йилда «Криптология янги йыналиш» [6], деб номланган илмий ма=оласининг чоп этилиши, махфий ало=а тизимларида махфий калитини махфий ало=а канали быича узатишга щожат йы= былган амалий бардошли криптосистемалар яратишнинг асосини очиб бердилар. У.Деффи ва М.Е.Хеллманнинг илгари сурган \оялари «бир томонли фунция»нинг Р.М.Нидхэмнинг щисоблаш системаларига киришнинг мущофазаси ща=идаги ишларидан олинган таърифини криптосистемалар учун мослаштирилган ифодасидир.

Бир томонли функция – бу, таъриф быйича, шундай $y = f(x)$ функцияки, бу функциянинг ани=ланиш сощасидан былган ихтиёрий x учун $f(x) = y$ =ийматосон щисобланиб, =ийматлар сощасининг барча y =ийматларига мос келувчи x =ийматларни щисоблаб топишни амалий жищатдан имконияти йы=. Кыриниб турибдики, бир томонли функциянинг бундай таърифи ушбу: «осон щисобланадиган», «барча =ийматлар учун», «амалий жищатдан», «щисоблашнинг имконияти йы=» иборалар асосида берилиб, бу таъриф амалий криптосистема масалалари ну=таи назаридан етарли даражада ани= былиб, алощида олинган криптосистемалар учун такомиллаштирилиб, мутла=о ани= ифодаланишга келтириш мумкин. Шундай функциялардан криптографияда =андай фойдаланиши ща=ида =ис=ача тыхталамиз. Хуфёна (яширин ёки махфий) услубли бир томонли функция, таъриф быйича бирор $z \in Z$ параметрларга бо\ли= былиб, тескарисига эга былган шундай f_z функциялар синфики, берилган z параметрда ани=ланиш сощасидаги барча аргументлар учун =ийматларнинг

осон щисоблаш алгоритми мавжуд былиб, =ийматлар сощасидаги барча $x \in X$ =ийматлар учун $f_z(x) = y$ =ийматларни маълум былган, E_z алгоритм билан щисоблашнинг имконияти йы= (ёки бош=ача айтганда, $f_z^{-1}(y) = x$ =ийматларни щисоблаш сарф=щаражатлари ва ва=ти ма=садга мувофи= эмас). Бундай таъриф математика ну=таи назаридан ани= былмаса-да, амалий криптология масаларидан самарали =ылланилиши мумкинлигига шак-шубща йы=.

Калитларнинг очи= та=симланиш алгоритми ща=ида

У. Диффи ва М. Е. Хеллман бир томонли функция сифатида ушбу

$$f(x) = \alpha^x (\text{mod } p) \qquad (15)$$

p модуль бўйича дискрет даражага кўтариш функциясини таклиф этдилар. Бу ерда: x - бутун сон бўлиб, 1 дан (p-1) гача бўлган =илматларни =абул =илиши мумкин; p-жуда катта бўлган туб сон; α - бутун сон бўлиб, 1 дан *p* гача бўлган =ийматларни =абул =илади ва унинг даражалари $\alpha, \alpha^2, ..., \alpha^{p-1}$ =андайдир тартибда 1, ..., *p*-1 кийматларни =абул =илади. Мисол учун, p=7, α =3 бўлса, α =3, α^2=2, α^3=6, α^4 =4, α^5=5, α^6=1 ифодаларга эга бўламиз. Алгебрада мана шундай α сонини чекли GP(p) майдоннинг содда элементи дейилади ва маълумки, бундай α щар доим мавжуд бўлади. Агарда $y = \alpha(x) = \alpha^x$ бўлса, у щолда табиийки, бу функцияга тескари функция

$$x = f^{-1} = \log y \qquad (16)$$

бўлиб, берилган *y* лар бўйича x =ийматларни топиш дискрет логарифмларни топиш масаласи дейилади. Хаттоки, *p* нинг жуда катта бўлган =ийматларида щам мисол учун p=2^{1000} бўлганда щам, 1000 дан кўп бўлмаган квадратга кўтариш ва кўпайтириш амалларини бажариб, $f(x)$ функцияни осон щисоблаш мумкин.

Агарда дискрет даражага кўтариш функцияси ща=и=атан щам, бир томонли бўлса, у щолда $\log_\alpha y$ ифодани *y* нинг барча, яъни ушбу $1 \le y \le p$ тенгсизликни =аноатлантирувчи, барча =ийматларида щисоблашни амалий жищатдан имконияти йы= бўлиши керак. М.Е.Хеллман ва унинг шогирди Полиг, фа=атгина *p* сони катта туб сон бўлгандагина эмас, балки (p-1) сони катта туб кўпайтувчи q га эга (ёки шу q туб сон 2 га купайтирилган) бўлганда, (15) ифода билан анл=ланган функциянинг *y* =ийматларига кыра $\log_z y$ ифодани щисоблаш амалий жищатдан мураккаб эканлигини кўрсатдилар. У.Диффи ва М.Е.Хеллман махфий ало=а тизимлари фойдаланувчилари учун дискрет логорифмлардан фойдаланиб, махфий

калитларни ўзаро алмашувини алощида махфий каналисиз амалга ошириш алгоритмини яратдилар. Бу алгоритм бўйича:

1. α ва p сонлари щамма фойдаланувчиларга маълум;

2. Щар бир фойдаланувчи, масалан i - фойдаланувчи 1 билан (p-1) сонлари орали\идаги бирор бутун X_i сонини танлаб олади бу сонни махфий тутади;

3. i - фойдаланувчи $Y_i = \alpha^{Xi} (\mathrm{mod}\ p)$ =ийматни щисоблаб, бу Y_i =ийматни махфий тутмай щамма фойдаланувчилар томонидан тасди=ланган ва улар щар доим фойдалана оладиган очи= маълумотлар китобига киритади;

4. Агарда махфий ало=а тизимининг i - фойдаланувчисиз j - фойдаланувчи билан махфий ало=а ўрнатмо=чи бўлса, i- фойдаланувчи очи= маълумотлар китобидан Y_j ни олиб, ўзининг махфий калити X ёрдамида

$$Z_{ij} = (Y_j)^{Xi} = (\alpha^{Xj})^{Xi} = \alpha^{Xi\,Xj} (\mathrm{mod}\ p)$$

=ийматини щисоблайди.

5. Худди шу каби j-фойдаланувчи щам $Z_{ij} = Z_{ji}$ ни щисоблайди. Бунда $Z_{ij} = Z_{ji}$ бўлиб, i ва j фойдаланувчилар ўзларининг махфий ало=асини таъминловчи криптоситемасида Z_{ij} =ииматни махфий калит сифатида ишлатишлари мумкин. Агарда ра=иб томон дискрет логорифмларнинг щисоблаш масаласини еча олса эди, очи= маълумотлар китобидан Y_i ва Y_j. ларни олиб, X = $logY_i$ ва X= log Y_i кийматларни щисоблаб, махфий калитга эга бўлган бўлар эди (i ва j - фойдаланувчилар каби).

Шу ерда таъкидлаб ытиш жоизки, очи= маълумотлар китоби ахборотларнинг махфий ало=а тизими фойдаланувчиларигагина очи=.

Ю=орида келтирилтан алгоритмдан кыриниб турибдики, щали бу нарса назарий жищатдан тыла исботлалган былмаса-да, ра=иб томон Z_{ij} =ийматни бош=а бирор услуб билан щисоблай олмайди. Келтирилган алгоритм Диффи ва Хеллманнинг калитларни очи=, та=симлаш системаси дейилади. Бу махфий ало=а тизимида махфий калитларни махфий канал билан узатишни щожати йы=лигини таъминловчи биринчи система былиб, бугунги кунда щам энг бардошли ва =улай былган очи= калитли бош=а криптосистемаларнинг асосини ташкил этади.

Диффи ва Хеллманнинг калитларни очи= та=симлаш системаси очи= калитли бош=а криптосистемалар каби махфий калитли махфий канал ор=али узатилишининг щожати йы=лигини таъминлайди, аммо аутентификация масаласини ечмайди.

Махфий ало=а тизимида очи= маълумотлар китобини са=ловчи, махфий былмаган Y_i ни очи= маълумотлар китобига i фойдаланувчининг фа=ат ызи томонидангина киритилганига ишонч щосил =илиши керак, i фойдаланувчи

эса, ыз навбатида, Y_j ни фа=ат очи= маълумотлартлар китобини са=ловчи томонидан берилганига инюнч щосил =илиши керак.

Очи= калитли RSA криптосистемаси

Диффи ва Хеллман махфий услубли бир томонли функциянинг ани=ланишига асосланиб, махфий ало=а тизими фойдаланувчилари учун, ызларининг очи= калитли криптосистема структурасини (тузилишини) таклиф этдилар. Щар бир i фойдаланувчи бирор Z_i бутун сонни (даража кырсаткичини) танлайди ва уни махфий са=лайди. Сынгра бу Z_i асосида E_{zi} алгоритм тузиб очи= маълумотлар китобига бу алгоритмни жойлаштиради. Бундан таш=ари Z_i асосида махфий са=ланадиган D_{zi} алгоритмни щам тузади ва уни сир тутади. Агарда j - фойдаланувчи i - фойдаланувчига X махфий маълумотни узатмо=чи былса, у щолда j - фойдаланувчи очи= маълумотлар китобидан E_{zi} алгоритмни олиб, $Y = f_{Zi}(x), \quad x \in X$ услуб билан криптограммани тузиб (щосил килиб), i – фойдаланувчига жынатади. Махфий маълумотни криптограмма кырынишида =абул =илиб олган i - фойдаланувчи ызининг махфий алгоритмидан фойдаланиб $f_{Zi}^{-1}(Y) = X$ услуб билан очи= матнни щосил =илади. Агарда f_Z , ща=и=атан щам, махфий услубли бир томонли функция былса, у щолда бу функция асосида =урилган алгоритм, шак-шубщасиз, амалий бардошлиликни таъминлайди. Диффи ва Хеллман, агарда бир томонли f_Z функциянинг ани=ланиш сощадаги даражада кырсаткичининг барча $z \in Z$ =ийматлари тыплами билан айнан шу функциянинг =ийматлари тыплами устма-уст тушса, яъни f_Z функциянинг ани=ланиш сощаси билан =ийматлар сощаси бир хил тыпламни ташкил этса, бундай бир томонли функция асосида ра=амли имло мумкин дейди. Агарда (i - фойдаланувчи ало=а тизими быйича махфий былмаган маълумотни барча фойдаланувчиларга етказиб, бу махфий былмаган маълумотни жынатувчини маълумотни =абул килиб олувчилар томонидан бещато ани=лашлари учун ызининг махфий алгоритми $Y = f_{Zi}^{-1}(X)$ асосида ра=амли имзо =ыяди. Щар бир фойдаланувчи очи= алгоритм E_{zi} ни билган щолда $f_{Zi}^{-1}(Y) = X$ ни олади, лекин i - фойдаланувчидан бош=а фойдаланувчи X маълумотни $Y = f_{Zi}^{-1}(X)$ криптограмма кырынишидаги ра=амли имзо ифодасига ытказа олмайди, чунки фа=ат i - фойдаланувчининг ызигина очи= алгоритм асосланган f_{Zi} функцияга тескари былиб, махфий алгоритм асосини ташкил этувчи f_{Zi}^{-1} ни щисоблай олади. Ыз-ызидан

тушунарлики, агарда i – фойдаланувчи i - фойдаланувчига махфий маълумотни щам ра=амли имзо билан жынатиш мумкин. Бунинг учун, i – фойдаланувчи j – фойдаланувчининг f_{Zi} функцияга асосланган очи= алгоритми (очи= шифрлаш калити) E_{Zi} дан фойдаланиб, жынатилиши керак былган маълумотни шифрлайди. Бу шифрланган маълумотларни =абул =илиб олган j - фойдаланувчи ызининг f_{Zi}^{-1} функцияга асосланган махфий D_{Zi} дешифрлаш алторитми билаи очади.

1976 йилда Диффи ва Хеллман ызларининг "Криптологияда янги йыналиш" [6] илмий ишларида бир томонли функция сифатида (15) ифода билан ани=ланган дискрет даражага кытариш функциясини таклиф =илиб, (16) ифодадаги дискрет логарифмни щисоблашнинг амалий жищатдан мураккаблигига асосланган эдилар. 1978 йилда эса, Массачусетс технология институтининг олимлари: Р.Л.Ривест, А.Шамир, Л.Адлман ызларининг илмий ма=оласида биринчи былиб махфий услубли ва ща\и\атан щам, бир томонли былган функцияни таклиф этдилар. Бу ма=ола "Ра=амли имзоларни =уриш услублари ва очи= калитли криптосистемалар" деб аталиб, кыпро= аутентификация масалаларига =аратилган. Щозирги кунда, бу ю=орида номлари келтирилган олимлар таклиф этган функцияни шу олимларнинг шарафига RSA бир томонли функцияси дейилади. Бу функция мураккаб былмай, унинг ани=ланиши учун элементар сонлар назариясидан баъзи маълумотлар керак буыади.

Мусбат бутун былган I ва n сонларининг энг катта умумий былувчисини ЭКУБ (I, n) деб белгилаймиз. Мисол учун: ЭКУБ(12, 18)=6, ЭКУБ(9, 27)=9. Щар кандай мусбат бутун сон учун Эйлер функцияси $\varphi(n),\ n$ дан катта былмаган ЭКУБ(I, n)=1 шартни =аноатлантирувчи барча i сонларининг сано\ини билдиради. Мисол учун: $\varphi(2)=1,\ \varphi(3)=2,\ \varphi(4)=2,\ \varphi(5)=4,\ \varphi(6)=2$ ва хоказо. Ихтиёрий туб сон p учун $\varphi(1)=p-1$, щамда $\varphi(1)=1$ деб =абул =илинган. Бундан таш=ари, ихтиёрий p ва q туб сонлари учун ушбу

$$\varphi(p\ q)=(p-1)(q-1) \qquad (19)$$

ифода ырinли былади. Мисол учун $\varphi(6)=\varphi(2x3)=1\cdot 2=2$.

Буюк математик олим Эйлер(1707-1783) теоремасига кыра ихтиёрий мусбат бутун x ва n (0<x<n) сонлари учун ЭКУБ(x, n)=1 шартини =аноатлантирувчи $x^{\varphi(n)}=1(\mathrm{mod}\ n)$ тенглик бажарилади. Мисол учун:

$$\text{ЭКУБ}(5,6)=1 \text{ ва } 5^2=1(\mathrm{mod}\ n) \qquad (20)$$

Сонлар назарияси курсидан маълумки: агарда, e ва m бутун сонлар 0<e<m ва ЭКУБ(m, e)=1 шартларни =аноатлантирса, у щолда 0<d<m тенгсизликни ва

$$de=1(\mathrm{mod}\ n) \qquad (21)$$

тенгликни =аноатлантирувчи ягона d бутун сон мавжуд былиб, ЭКУБ(m, e)ни топишнинг "кенгайтирилган" Эвклид алгоритмидан фойдаланиб d ни топиш мумкин.

Ю=орида келтирилган маълумотлардан фойдаланиб, махфий услубли RSA бир томонли функциясини анни=ланишини кыриб чи=амиз. Бу функция бирор n сони модули быйича дискрет даражага кытариш функцияси, яъни

$$f_Z(x)=x^e(\mathrm{mod}\ n) \qquad (22)$$

кырнишида ани=ланади. Бу ерда: x- мусбат бутун сон былиб, n=pq сондан катта эмас; n=pq, яьни p ва q туб сонлари учун $\varphi(n)=(p-1)(q-1)$; бутун e сони $\varphi(n)$ дан кичик ва ЭКУБ$(e, \varphi(n))=1$. Шифрлашнинг E_z очи= алгоритмини асосини ташкил этувчи $y=f_Z(x)$ функция =ийматларини (22) ифода билан щисоблашни осонгина квадратга кытариш ва кыпайтириш амалларига келтириш мумкин. E_z алгоритмни очи= калитлар китобига киритиш, n ва e сонларини фойдаланувчилар учун очи= эълон =илиш демакдир ва бунда n сонининг кыпайтувчилари былган p ва q туб сонлари махфий тутилади. Тескари функция =уйидаги

$$f_{Zi}^{-1}(y)=y^d(\mathrm{mod}\ n) \qquad (23)$$

кырнишда былиб, бу ерда q сони n сонидан кичик ва ушбу

$$de=1(\mathrm{mod}\ n) \qquad (24)$$

тенгликни =аноатлантиради.

p, q, e - сонларидан иборат { p, q, e }=z параметрлар тыплами (22) тенглик билан ани=ланган бир томонли функциянинг криптографик махфийлик услуби хоссасининг асосини ташкил этади. Махфий D_z дешифрлаш алгоритиминининг асосини ташкил этувчи тескари f_{Zi}^{-1} функциянинг =ийматларини щисоблаш щам квадратга кытариш ва кыпайтириш амаллари ор=али амалга оширилади ва бунда даража кырсаткичи былган d сони ЭКУБ$(e, \varphi(n))$ ни щисоблашнинг Эвклид алгоритми быйича ани=ланади. Ю=орида (23) ифода билан ани=ланган функциянинг (22) ифода билан ани=ланган функцияга ща=и=атан щам,

тескари функция эканлиги =уйидагича кырсатилади. Бутун сонлар арифметикасидан маълумки, бирор бутун Q сонида

$$de = 1(\mathrm{mod}\ (n)) = \varphi(n) \cdot Q + 1 \qquad \textbf{(25)}$$

тенглик ыринли билади. Ю=оридаги (22) ва (25) тенгликларга ва Эйлер теоремасидаги (22) ифодага кыра

$$f_{Zi}^{-1}(y)^d \bmod(n) = (x^e)^d (\mathrm{mod}\, n) = {}^{\varphi(n)Q+1} \bmod n = x^{\varphi(n)Q} x(\mathrm{mod}\, n) = x(\mathrm{mod}\ n) \ \textbf{(26)}$$

тенгликка эга быламиз. Демак, (24) тенгликни =аноатлантирувчи d ва e сонлари учун: бирор x<n сонларнинг n модул быйича d даражага кытариш амали шу x сонларни худди шу n модул быйича e даражага кытариш амалига тескари экан. Энди нима учун Ривест, Шамир ва Адлман ю=орида (22) ифода билан ани=ланган $f_z(x)$ функцияни n ва e сонларини билган щолда, унга тескари $f_z^{-1}(x)$ функцияни щисоблаш мумкин эмаслигини таъкидлаганликларини кыриб чи=амиз. Бундан таш=ари p ва q туб сонларини кандай =илиб танланганда, ра=иб томоннинг бу сонларни била олмаслигини щам кыриб чи=амиз.

Ра=иб томонга n ва e сонлари маълум былсин. Агарда ра=иб томон n сонини туб былган p ва q сонларининг кыпайтмасидан иборат, яьни n=pq кырынишида ифодалай олса, у щолда махфийлик параметри z={ p, q, e }ни тыла ани=ланган щолда, маълумотлар криптограммасини, маълумотни, ха=и=атан щам, олиши керак былган фойдаланувчи каби =ийинчиликсиз дешифрлаш имкониятига эга билади. Шунинг учун RSA криптосистемасининг бардошлилик даражаси n сонини туб былган p ва q сонларининг кыпайтмасига ёйишнинг =ийинлик даражасига эквивалентдир, яъни тенг кучлидир. Агарда p ва q сонларининг узунлиги 100 дан орти= ынли ра=амдан иборат былса, щозирги замонавий щисоблаш техникаларидан фойдаланилганда, n сонини туб кыпайтувчиларга ажратиш учун сарфланадиган ва=т етарли даражада кып былиб, бундай туб кыпайтувчиларга ажратиш билан шу\улланишининг амалий жищатдан ма=садга мувофи= эмаслиги келиб чи=ади.

Ю=оридаги мулощазалардан табиий равишда "етарли даражада катта былган p ва q туб сонларини =андай ани=лаш мумкин?", деган савол ту\илади. Бундай саволга жавоб топиш учун Чебышев теоремасига мурожаат =иламиз: бирор бутун m сонидан кичик былган барча бутун сонлар тыпламидан танлаб олинган бирор сонни, туб сон былиш эщтимоллиги $(\ln m)^{-1}$ =ийматга я=ин. Мисол учун 10^{100} дан кичик былган барча мусбат бутун сонлар тыпламидан танлаб олинган бирор сонни туб сон былиш эщтимоллиги $(\ln\ 10^{100})^{-1} = \dfrac{2}{100 \ln 10} \approx \dfrac{1}{230}$ =ийматга эга. Бу эщтимоллик =иймати икки баробар кыпаяди, агарда бу танлаб олиш фа=ат 10^{100}дан кичик былган барча

бутун мусбат то= сонлар тыпламида амалга оширилаётган былса. То= сонлардан туб сонларни фар=лаш Ферма теоремасига асосланади: бирор р туб сонидан катта былмаган бутун мусбат сон учун

$$b^{p-1} = 1 \,(\mathrm{mod}\ (p)) \qquad (27)$$

тенглик ырынлидир.

Мисол учун, 2^4=1(mod 5) ёки 3^4=1 (mod 5). Бу келтирилган (27) муносабат (20) муносабатниинг хусусий щолидир. Агарда r сонининг туб ёки туб эмаслигини текширмо=чи былсак, шу r сонидан кичик былган бутун мусбат b сонини олиб

$$b^{r-1} = 1 \,(\mathrm{mod}\ (r)) \qquad (28)$$

тенглик бажарилишини текшириш кифоя:

-тенглик бажарилса r туб сон былиши мумкин, чунки (27) ёки (28) муносабат р нинг ёки r сонининг туб былишини зарурий шарти;

-тенглик бажарилмаса r туб сон эмас.

Шундай =илиб, агарда (28) муносабат ырынли былмаса, катьий щолда r сони туб эмас, деб айта оламиз. Аммо, (28) муносабат ырынли былса, фа=ат r сони туб былиши мумкин, лекин =атъий щолда r туб сон, деб тасди=лай олмаймиз.

Шунинг учун, r сони етарли даражада катта былиб, тасодифий олинган мумкин =адар кып бутун мусбат b(1<b<r) сонлари учун (28) муносабат бажарилса, r сонининг туб эканлигига шунчалик кып даражада ишонч щосил =илиш мумкин. Агарда b нинг юзта =ийматида (28) муносабат ырынли былса, у щолда r сонининг туб былмаслмгм щодисасининг эщтимоли =иймати

$$\frac{1}{2^{100}} = 2^{-100}$$

Ю=орида келтирилган алгоритмдан бугунги кунда щам бирор r сонининг тублигини ани=лашда фойдаланиб келинмо=да.

Щар =андай очи= калитли криптосистеманинт бардошлилиги очи= матнга ёки унинг бирор =исмига мос келувчи криптограмма маълум былганда, яъни шифрлаш алгоритми E_z маълум былганда, тыла шифр матнни (криптограммани) дешифрлаш имконияти =анчалик мураккаблиги билан бащоланади

Очи= калитли криптосистемалар ща=ида изощ

Ю=орида кыриб ытилган Диффи ва Хеллманнннг бир томонли функцияси щамда RSA бир томонли функцияси етарли даражада очи= калитли криптосистемаларнинг хоссаларини очиб беради. Бу бир томонли функциялардан таш=ари щам кыплаб бир томонли функциялар криптология сощасидаги илмий нашрларда эълон =илинган. Уларнинг баъзилари етарли даражада криптосистемлар талабларига жавоб бермаган. Шуни таъкидлаймизки, щозиргача очи= нашрётда щеч ким томонидан ща=и=атан щам бир томонли былган ёки махфий услубли бир томонли былган функция эълон =илинган эмас.

Таянч иборалар

Очи= калит, бир томонли функция, Эйлер функцияси, Эвклид алгоритми.

Назорат саволлари

1. Очи= калитли криптосистемалранинг мощияти.
2. Бир томонли функциялар тушунчаси.
3. Очи= калитли криптосистеманинг акслантириш типлари.
4. Диффи – Хеллман алгоритми

Асосий адабиёт

1. Анохин М.И., Варнавский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. М. 1997г.
2. Брюс Шнайер. Прикладная криптография: 2– е издание. М. 2001.
3. Фомичев В.М. Дискретная математика и криптология. М. «Диалог МИФИ» 2003 г. http: ‖ www.library.mephi.ru – Библиотека МИФИ.
4. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М. «Радио и связь» 2001г.
5. Московский центр непрерывного математического образования. Материалы 1 – 9 олимпиад по криптографии. М. 2001 – 2003гг. http: ‖ www. ibc.ry./- электронная библиотека Московского Государственного Университета экономики, статистики и информатики.
6. В.А.Хорошко, А.А.Чекатков. Методы и средства защиты информации. Издательство «ЮНИОР» К. 2003.

Кушимча адабиёт

1. Анин Б. Защита компьютерной информации. Санкт – Петербург, 2002.
2. Завгородный В.И. Комплексная защита информации в компьютерных системах., М. «Логас», 2001.

3. А.В.Домашев, М.М.Грунтович, В.О.Попов, Д.И.Правиков, А.Ю.Щербаков, И.В.Ппокофьев. Программирование алгоритмов защиты информации. Учебное пособие. Издательство «Нолидж». М. 2002.

Маъруза 7

Криптосистема калитларини фойдаланувчиларга та=симлашнинг тартиб ва =оидалари (протоколи)

1. RSA алгоритми быйича калитларни та=симлаш протоколига изощлар.
2. Гаммалаштириш.
3. Эль Гамаль криптосистемаси.
4. Эллиптик тенгламалар асосида криптосистемалар.

Махфий услубли бир томонли функцияга асосланган очи= калитли криптосистемалар ыз мощиятига кыра ундан фойдаланишнинг алощида тартиб ва =оидаларини (протоколини) талаб этади. Бу алощида тартиб ва =оидаларга кыра системанинг фойдаланувчилари ва система фойдаланувчиларигагина очи= былган очи= маълумотлар китобини са=ловчиси биргаликда шу криптосистема тизимида узатиладиган маълумотларнинг махфийлигини таъминлайдилар.

Очи=, калитли криптосистемаларнинг бардошлилигига тыла ишонч билдирмай ишончсизлик ва иккиланиш билан =арайдиган баъзи криптолог мутахассислар, фойдаланувчиларга мущофазаланган услубда очи=, калитларни та=симлаш ва махфий калитларни узатиш масалаларини, яъни калитлар билан бо\ли= жараёнларни ма=садли бош=аришни криптографиянинг бош амалий масаласи, деб биладилар. Мисол учун, агарда криптосистема фойдаланувчиларининг сони S та былса ва щар бир мумкин былган ало=а жуфтлари учун алощида махфий калит талаб этилса, уларнинг сони $c_S^2 = s(s-1)/2$ былиб, фойдаланувчилар сони кып былган системалар учун бундай щолат баъзида ма=садга мувофи= былмаслиги мумкин. Бирор фойдаланувчининг бош=а барча фойдаланувчиларга махфий былган маълумотни юбориши махфий ало=а мощиятига зид жараён. Бундан таш=ари махфий ало=а тизимида =айси фойдаланувчининг бош=а =айси бир фойдаланувчи билан махфий ало=а =илишни щощлаши олдиндан маълум

эмас. Мана шундай щолатлар фойдаланувчиларга калитларни та=симлаш тартиб ва =оидалари масалаларини келтириб чи=аради. Бундай масалаларнинг ечилиши эса ахборотлар тизимида маълумотларнинг махфийлиги мущофазасини таъминловчи критисистемада калитлар та=симотининг ишончли марказини (КТИМ) ташкил этишни та=азо этади. Калитларни та=симлаш тартиб ва =оидалари (протоколи) =уйидагича:

1. КТИМ мущофазаланган ало=а тармо\и ор=али барча i=1,2,...,S фойдаланувчиларга махфий Z_i калитларни та=дим этади.

2. Фойдаланувчи i-фойдаланувчи j билан махфий ало=а ырнатмо=чи былса, у умумий ало=а тармо\и ор=али (очи= текст билан былиши мумкин) КТИМга мурожаат =илиб, фойдаланувчи j - билан махфий ало=а =илиш калитини сырайди.

3. КТИМ махфий ало=а учун очи= матннинг бирор =исмини ташкил этувчи Z_{ij} махфий калитни танлаб олади. +олган =исмини i ва j фойдаланувчилар кысатилган "бош =исм" ("заголовка") ёки "номланиш =исми" деб аталувчи былак ташкил этади. КТИМ бу очи= матнни криптосистемада =абул =илинган шифрлаш алгоритмига кыра Z_i ва Z_j калитлар билан шифрлаб, умумий ало=а тармо\и ор=али Z_i калит билан шифрланган криптограммани j фойдаланувчига ва Z_j калит билан шифрланган криптограммани j фойдаланувчига жынатади.

4. Олинган криптограммаларни i ва j фойдаланувчилар дешифрлаб, кейинги олинган маълумотларни дешифрлашнинг махфий калитига эга быладилар.

Калитларни та=симлашнинг бундай тартиб ва =оидаси (протоколи) оддий былиб, унинг бардошлилиги шифрлаш алгоритмининг бардошлилиги билан белгиланади. Ща=и=атан щам, 3-бандда (=адамда) келтирилганидек, криптоаналитикка щар хил калитлар билан шифрланган бир хил очи= текстнинг криптограммаси маълум былиб, бундай щолат унга криптотащлил =илишда =ыл келади. Шундай =илиб, очи= текст шифрлаш алгоритми криптотащлилга бардошли былса, калитларни та=симлаш протоколи щам бардошли былади. Бу ерда шуни щам унутмаслик керакки, калитларни та=симлашда шифрлаш алгоритмидан фойдаланиш шу та=симлаш тартиб ва =оидаларини бузилишига, криптобардошсизликка ва шу каби номутоносибликларга олиб келмаслиги керак.

RSA алгоритми быйича калитларни та=симлаш протоколига хулосавий изощлар

Банклар тизимида =айси шахс =айси шахс билан ызаро тылов амаллари бажарганлигини банк билмаслигини таъминловчи RSA бир томонли функциясига асосланган тартиб ва =оидаларни бош=ариш криптосистемаси мавжуд. Бу криптосистемани калитларни та=симлаш тартиб ва =оидаларини бош=ариш криптосиетемаси учун щам =ыллаш мумкин. Тартиб ва =оидаларни бош=ариш масалалари, криптосистемаларига доир криптологик илмий изланишлар щозирда замонавий, бардошли криптографик системаларни

яратишда кенг ва жадал ривожланиб бормо=да. Бу сощада RSA бир томонли функциясидан фойдаланишнинг =улайлиги ызини щар томонлама о=лаб келмо=да.

RSA алгоритмини =ылланишига доир кичик бир мисол келтирамиз.

Мисол: Учта харфдан иборат былган "САВ" маълумотини шифрлаймиз.

Биз =улайлик учун кичик туб сонлардан фойдаланамиз. Амалда эса мумкин =адар катта туб сонлар билан иш кырилади.

1. Туб былган p=3 ва q=11 сонларини танлаб оламиз.

2. Ушбу n=pq=3*11=33 сонини ани=лаймиз.

3. Сунгра, $\varphi(33)=(p-1)(q-1)=2\cdot 10=20$ сонини топамиз, щамда бу сон билан 1 дан фар=ли бирор умумий былувчига эга былмаган d сонини, мисол учун d=3 сонини оламиз.

3. Ю=орида келтирилган (24) шартни =аноатлантирувчи e сонини 3e=1 (mod 20) тенгликдан топамиз. Бу сон e=7.

4. Шифрланиши керак былган "САВ" маълумотини ташкил этувчи харфларни: $A\to 1,\ B\to 2,\ C\to 3$ мосликлар билан сонли кыринишга ытказиб олиб, бу маълумотни мусбат бутун сонларнинг кетма-кетлигидан иборат деб =араймиз. У щолда маълумот (3,1,2) кыринишда былади ва уни {e;n}={7;33} очи= калит билан бир томонли функция билан шифрлаймиз:

x=3 да ШМ1=(3^7)(mod 33)=2187(mod 33)=9,
x=1 да ШМ2=(1^7)(mod 33)=1,
x=2 да ШМ 3=(2^7)(mod 33)=128(mod 33)=29

5.Бу олинган шифрланган (9,1,29) маълумотни махфий {d;n}={3;33} калит билан $f_z^{-1}(x)=x^7(\mathrm{mod}\,33)$ ифода ор=али дешифрлаймиз:

y=9да ОМ1 = (9^3) (mod33)= 729(mod33)=3,
y=1 да ОМ2=(1^3) (mod33) = 1(mod33)=1,
y=29 да ОМ3=(29^3)(mod33)=24389(mod33)=2.

Шундай =илиб, критосистемаларда RSA алгоритмининг =ылланиши =уйидагича: щар бир фойдаланувчи иккита етарли даражада катта былмаган p ва q туб сонларни танлайдилар ва ю=орида келтирилган алгоритм быйича d ва e туб сонларини щам танлаб олади. Бунда n=pq былиб, {e;n} очи= калитни {d;n}эса махфий калитни ташкил этади. Очи= калит очи= маълумотлар китобига кириталади. Очи= калит билан шифрланган шифрматнни шу калит билан дешифрлаш имконияти йы= былиб, дешифрлашнинг махфий калити фа=ат шифр маълумотининг ща=и=ий эгасигагина маълум.

Гаммалаштириш

Гаммалаштириш амалда кып =ылланиладиган криптографик акслантириш былиб, ю=орида кыриб ытилган Вижинер ва чексиз калитли шифрлаш услублари кабидир.

Гаммалаштириш билан шифрлаш услубининг мощияти очи= матнга (ёки шифрматнга) шу матн алфавит белгиларидан тузилган псевдотасодифий деб аталувчи матндан ажратиб олиб ташлаш мумкин былган кетма - кетликни, яъни гаммани =ышишдан (=ориштиришдан) иборат. Мисол учун 2 модул быйича =ышишдан фойдаланиш мумкин:

Очи= матн:	0110011100100011…
Гамма:	1110110010110101…
Гаммалаштирилган матн:	1000101110010110…
Гамма:	1110110010110101…
Очи= матн:	0110011100100011…

Бу мисолдан кыринадики, дешифрлаш учун калит быйича (яъни гамма быйича) шифрматнни 2 модул быйича =ышишдан фойдаланиб =айта гаммалаштириш кифоя.

Агарда гаммашифр =айтарилувчи даврга эга былган битлардан иборат былмаса, олинган шифрматнни очиш етарли даражада =ийин былади. Шунинг учун гаммашифр битлари тасодифий ызгариши керак. Амалда гамманинг даври бутун шифрматн узунлигидан катта былиб, очи=матннинг щеч бир =исми маълум былмаса, бундай шифрматнга мос келувчи очи= пакетни топиш ыта мушкул иш. Бундий щолларда шифрни фа=ат шифркалитни таваккалига танлаш билан очилади.

Агарда ра=иб томонга очи= матннинг бирор =исми ва унга мос келувчи шифрматн маълум былиб =олса, у щолда шифрташнинг гаммалаштириш услуби ыз кучини йы=отали. Чунки бундай щолда ра=иб томон очи= матнни маълум былган =исми мазмунига кыра бутун шифрматнни очишга щаракат =илади. Мисол учун, кыплаб махфий щужжатлар «Мутла=о махфий» ёки бош=а шу каби сызлар билан бошланиб, криптоаналитик учун тащлил йыналишини ани=лашга ёрдам беради. Бундай щолатларни ахборот тизими мущофазаси криптосистемасининг амалдаги =ылланишларида албатта щисобга олиш керак.

Эль - Гамаля криптосистемаси

Эль - Гамаля системаси RSA системасига му=обил (алтернатив) былиб, бу криптосистемаларнинг калитларининг ылчов узунликлари тенг былганда бир - хил криптобардошлиликга эга быладилар.

Эль - Гамаля криптосистемаси Диффи-Хеллман алгоритмига ыхшаш былиб, дискрет логарифмларни щисоблаш масаласи ечимининг мураккаблигига асосланган. Бу криптосистема асосини туб былган p ва бутун былган g сонлари ташкил этади. +уйида ушбу системанинг мощиятини очиб берувчи мисолни келтирамиз.

Бирор фойдаланувчи (А) махфий калит *a* сонини танлаб олади ва $y = g^a (\mathrm{mod}\, p)$ былган очи= калитни щисоблайди. Агарда мана шу фойдаланувчи (А) билан бирор бош=а фойдаланувчи (Б) махфий маълумотни жынатмо=чи былса, у щолда (Б) *p* сонидан кичик былган бирор криптосистема сонини танлаб олиб

$$y_1 = g^k \bmod p \quad \text{ва} \quad y_2 = m \otimes y^k$$

сонларини щисоблайди, бу ерда $\otimes$ белгиси 2 модул быйича битларни =ышиш амалини билдиради, яъни m ва y^k сонлари иккилик сано= системасида, деб тушинилади. Сынгра (Б) ($y_1 > y_2$) маълумотларини (А)га жынатади. Ыз навбатида (А) бу шифрлангаи маълумотни =абул =илиб, =уйидаги

$$(y_1^a \bmod p) \otimes y_2 = m$$

былган щисоблаш билан маълумотнинг очи= матнини тиклайди.

Эллиптик тенгламалар асосида криптосистемалар

+уйида

$$y^2 = x^3 + ax + b$$

тенгламани =аноатлантирувчи барча (x,y) текислик ну=таларининг геометрик ырни эллиптик эгри чизи=ни ташкил этади. Эгри чизи= ну=таларини =ышиш амали, RSA ва Элг-Гамаля системаларидаги кыпайтириш амали каби, =ийиичиликсиз ани=ланади.
Кыплаб маълум былган криптосистемаларда

$$y^2 = x^3 + ax + b \bmod p$$

бу ерда p - туб сон кырынишдаги эллиптик тенглама асос =илиб олинади.

Эллиптик эгри чизи=ларда дискрет логарифмлаш масаласининг мощияти =уйидагича, эллиптик эгри чизи=да берилган $G = (x_G, y_G)$ ва $Д = (x_Д, y_Д)$ ну=талар учун $Д = \varphi G$, яъни $(x_Д; y_Д) = \varphi (x_C; y_C)$ тенгликнт =аноатлантирувчи ягона φ ни топишдан иборат.

Таянч иборалар

Протокол, криптосистемада калитлар та=симотининг ишончли ркази, RSA алгоритми, гаммалаштириш, Эль – Гамаль криптосистемаси, Эллиптик тенглама.

Назорат саволлари

1. RSA алгоритмининг =ыллашини изощланг.
2. Гаммалаштириш билан шифрлашни мощиятини нимада?
3. Эль – Гамаль криптосистемаси билан RSA криптосистемасининг му=обиллиги нимада?

Асосий адабиёт

1. Анохин М.И., Варнавский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. М. 1997г.
2. Брюс Шнайер. Прикладная криптография: 2– е издание. М. 2001.
3. Фомичев В.М. Дискретная математика и криптология. М. «Диалог МИФИ» 2003 г. http: ‖ www.library.mephi.ru – Библиотека МИФИ.
4. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М. «Радио и связь» 2001г.
5. Московский центр непрерывного математического образования. Материалы 1 – 9 олимпиад по криптографии. М. 2001 – 2003гг. http: ‖ www. ibc.ry./- электронная библиотека Московского Государственного Университета экономики, статистики и информатики.
6. В.А.Хорошко, А.А.Чекатков. Методы и средства защиты информации. Издательство «ЮНИОР» К. 2003.

Кушимча адабиёт

1. Анин Б. Защита компьютерной информации. Санкт – Петербург, 2002.
2. Завгородный В.И. Комплексная защита информации в компьютерных системах., М. «Логас», 2001.
3. А.В.Домашев, М.М.Грунтович, В.О.Попов, Д.И.Правиков, А.Ю.Щербаков, И.В.Ппокофьев. Программирование алгоритмов защиты информации. Учебное пособие. Издательство «Нолидж». М. 2002.

Маъруза 8

Электрон имзо

1. RSA алгоритми асосида электрон имзо.
2. Калитлар билан бош=ариш.
3. Катта щажмдаги маълумотларни шифрлаш.
4. Криптографик услубларнинг амалдаги =ылланишлари ща=ида.

+абул =илиб олинган маълумотларни ща=и=ийлигини ёки ща=и=ий эмаслигини ани=лаш масаласини, яъни маълумотларни аутентификацияси масаласининг мощияти ха=ида тыхталамиз.

Щар =андай ёзма хат ёки щужжатнинг охирида шу щужжатни бажарувчиси ёки бажарилиши учун жавобгар былган шахснинг имзоси былиши табиий щолдир. Бундай щолат одатда =уйида иккита ма=саддан келиб чи=илди. Биринчидан, маълумотни олган томон ызида бор былган имзо намунасига олинган маълумотдага имзони солиштирган щолда шу маълумотнинг ща=и=ийлигига ишонч щосил =илади. Иккинчидан, шахсий имзо маълумот щужжатига юридик жищатдан авторликни кафолатлайди. Бундай кафолат эса савдо-соти=, ишончнома, мажбурият ва шу каби битмларда алощида мущимдир.

Щужжатлардаги =ыйилган шахсий имзоларни сохталаштириш нисбатан мураккаб былиб, шахсий имзоларниинг авторларини щозирги замонавий ил\ор криминалистика услубларидан фойдаланиш билан ани=лаш мумкин. Аммо электрон имзо хусусиятлари бундан фар=ли былиб, иккилик сано= системаси хусусиятлари билан белгиланадиган хотира регистрлари битларига бо\ли=. Хотира битларининг маълум бир кетма -кетлигидан иборат былган электрон имзони кычириб бирор жойга =ышиш ёки ызгартириш

компьютерлар бо\лами системаси асосидаги ало=а тизимларида мураккаблик ту\дирмайди.

Бугунги ю=ори даражада ривожланган бутун дунё цивилизациясида щужжатларни, жумладан, махфий щужжатларни щам, электрон кыринишда ишлатилиши ва ало=а тизимларида узатилиши кенг тармо=ли =ылланилиб борилаётганлиги, электрон щужжатлар ва электрон имзоларнинг ща=и=ийлигни ани=лаш масалаларининг мущимлигини келтириб чи=армо=да.

Очи= калитли криптографик системалар былимида таъкидлаб ытганимиздек, бундай криптосистемалар =анчалик =улай ва криптобардошли былмасин, аутентификация масаласини тыла ечилишига жавоб бера олмайди. Шунинг учун аутентификация услуб ва воситалари криптографик алтритмлар билан биргаликда комплекс щолда =ылланилиши талаб этилади.

+уйида иккита (А) ва (Б) фойдаланувчиларнинг ало=а муносабатларида аутентификация системаси ра=иб томоннинг ыз ма=сади йылидаги =андай щатти-щаракатларидан ва криптосистема фойдаланувчиларининг фойдаланиш протоколини ызаро бузишларидан са=лаши кераклигини кырсатувчи щолатларни кыриб чи=амиз.

Рад этиш (ренегатство)

Фойдаланувчи (А) фойдаланувчи (Б) га ща=и=тан щам маълумот жынатган былиб, узатилган маълумотни рад этиш мумкин.
Бундай =оида бузилишини (тартибсизликни) олдини олиш ма=садида электрон (ра=амли) имзодан фойдаланилади.

Модификациялаш (ызгартириш)

Фойдаланувчи (Б) =абул =илиб олинган маълумотни ызгартириб, шу ызгартирилган маълумотни фойдаланувчи (А) юборди, деб таъкидлайди (даъво =илади).

Сощталаштириш

Фойдаланувчи (Б)нинг ызи маълумот тайёрлаб, бу сощта маълумотни фойдаланувчи (А) юборди деб даъво =илади.

Фаол модификациялаш (ызгартириш)

(А) ва (Б) фойдаланувиларнинг ызаро ало=а тармо\ига учинчи бир (В) фойдаланувчи но=онуний щолатда бо\ланиб, уларнинг ызаро узатаётган маълумотларини ызгартирган щолда деярли узлисиз узатиб туради.

Ни=облаш (имитациялаш)

Учинчи фойдаланувчи (В) фойдаланувчи (Б)га фойдаланувчи (А) томонидан маълумот жынатади.

Ю=орида санаб ытилган: модификациялаш, сощталаштириш, фаол модификациялаш, ни=облаш каби ало=а тизими =оидаларининг бузилишини олдини олиш ма=садида ра=амли сигнатурдан – ра=амли имзо ва узатиладиган маълумотни бирор =исмини тыла ыз ичига олувчи ра=амли шифрматндан иборат былган маълумотдан фойдаланилади.

Такрорлаш

Фойдаланувчи (В) фойдаланувчи (А) томонидан фойдаланувчи (Б)га жынатилган маълумотни такроран (Б)га жынатади. Бундай но=онуний хатти-щаракат ало=а усулидан банклар тармо=ларида электрон щисоб-китоб тизимидан фойдаланишда но=онунийлик билан ызгалар пулларини талон-тарож =илишда фойдаланилади. Ана шундай но=онуннй усуллардан мущофазаланиш учун:

-имитациялашга бардошлилик - имитабардошлилик;

-криптосистемага кираётган маълумотларни мущофаза ма=садларидан келиб чи=иб тартиблаш;

чора тадбирлари кырилади.

RSA алгоритми асосида электрон имзо

Кыплаб электрон (ра=амли) имзо алгоритмлари мавжуд былиб, =улай ва кенг тар=алган электрон имзо RSA алгоритмига асосланган. +уйида шу алгоритм асосида электрон имзо =андай яратилишини кыриб чи=амиз.

RSA алгоритмини асосини ташкил этувчи d, p, q- сонлари махфий былиб, бу сонлар билан бо\ли= былган ***e*** ва *n=p q* сонлари маълум былсин. Бу ерда:

1. $\varphi(n) = (p-1)(q-1)$ былиб, $\varphi(n)$ ва ***e*** сонларини билган щолда (25)

муносабатдан, яъни $de = \varphi(n)Q + 1$ тенгликдан бирор ***q*** сонида ***d*** сонини ани=лаб олиш мумкин.

2. ***e*** ва ***d*** сонларини билган щолда $\varphi(n)$ сонига каррали былган сонларни ва уларни =анчалигини топиш мумкин былиб, бундан ***n*** сонининг былувчиларни топиш мумкин.

Агарда фойдаланувчи (А) фойдаланувчи (В) га "САНА" сызини имзо сифатида узатмо=чи былса, ызининг d_A ва p_A - q_A =n_A махфий сонлар билан ани=ланувчи махфий калитли алгоритми ва (Б) нинг $e_Б$ ва $n_Б$ сонлари билан ани=ланувчи очи= калитдан фойдаланиб электрон (ра=амли) имзо =ыяди. Бу имзо =уйдаги кырынишдаги

$$\text{Tsp}\, Ee_{Б},\ n_{Б}\{Ed_{A},\ n_{A}\{CAHA\}\}$$

акслантиришлар (алгоритмлар) кетма - кетлиги билан аникланади.

Ыз навбатида бу имзони фойдаланувчи (Б) дастлаб ызининт махфий калитли $Ed_{Б},\ n_{Б}$ алгоритми билан

$$Ed_{Б},\ n_{Б}\{Ed_{A},\ n_{A}\{CAHA\}\} = Ed_{A},\ n_{A}\{CAHA\}$$

маълумотни щосил =илади. Сынгра (Б) фойдаланувчи (А)нинг очи= алгоритми $Ed_{A},\ n_{A}$ ор=али

$$Ee_{A},\ n_{A}\{Ed_{A},\ n_{A}\{CAHA\}\} = CAHA$$

маълумотни олади.

Бу келтирилган электрон имзо =оидаси (схемаси) ало=а тизимларида бир неча тур =оида бузилишларидан мущофаза =илинишни таъминлайди, яъни:

- махфий калит фа=ат фойдаланувчи (А)нинг ызигагина маълум былса, у щолда фойдаланувчи (Б) томонидан =абул =илиб олинган маълумотни фа=ат (А) томонидан жынатилганлигини рад этиб былмайди;

- =онунбузар (ра=иб томон) махфий калитни билмаган щолда модификациялаш, сощталаштириш, фаол модификациялаш, ни=облаш ва бош=а шу каби ало=а тизими =оидаларини бузилишига имконият ту\дирмайди;

-ало=а тизимидан фойдаланувчиларнинг ызаро бо\ли= щолда иш юритиши муносабатидаги кыплаб келишмовчиликларни бартараф этади ва бундай келишмовчиликлар келиб чи==анда воситачисиз ани=лик киритиш имконияти ту\илади.

Кып щолларда узатилаётган маълумотларни шифрлашга щожат былмай, уни электрон имзо билан тасди=лаш керак былади. Бундай щолатларда очи= матн жынатувчининг ёпи= калити билан шифрланиб, олинган шифрматн очии= матн билан бирга жынатилади. Маълумотни =абул =илиб олган томон жынатувчининг очи= калити ёрдамида шифрматнни дешифрлаб, очи= матн билан солиштириши мумкин.

1991 йилда А+Ш даги Стандартлар ва Технологиялар Миллий Институти DSA (Digital Signature Algarithm) ра=амли имзо алгоритмининг стандартини DSS (Digital Signature Standart) биз ю=орида келтирган Эль-Гамаля ва RSA алгоритмлари асосида яратиб, фойдаланувчиларга таклиф этган.

Калитлар билан бош=ариш

Ахборотлар тизимига мос келувчи криптографик системани яратиш билан бир =аторда шу системада калитлар билан бош=ариш масаласини оптимал (=улай ва ишончли) щал этиш мущим ырин тутади. Чунки танланган криптосистема =анчалик мураккаб ва ишончли былмасин, бари-бир ундан амалда фойдаланиш жараёнлари калитлар билан бо\ли=дир. Агарда маълумотларнинг махфий алмашинуви оз сондаги фойдаланувчилар доирасида былса, калитлар алмашинуви жараёнида но=улайликлар ту\илмайди. Аммо ахборотлар тизимида маълумотларнинг махфий алмашинуви юзлаб, минглаб ва хатто миллионлаб фойдаланувчилар доирасида былса (мисол учун модем ва ИНТЕРНЕТ ало=а тизимлари ор=али банк, савдо-соти=, давлат ащамиятига бо\ли= щамда бош=а мущим сощалардаги ало=а жараёни фойдаланувчилари доирасида) калитлар билан бош=аришнинг ызига хос алощида мущим масалалари келиб чи=ади.

Калитлар ща=идаги маълумот деганда ахборотлар тизими криптосистемасида мавжуд былган барча калитлар тыплами ва уларнинг мущофазаси билан бо\ли= маълумотлар тушунилади. Агарда калитлар ща=идаги маълумотларни етарли даражадаги ишончли мущофазали бош=аруви таъминланмаса, табиийки, ра=иб томонга ахборотлар тизимидаги деярли ихтиёрий маълумотни олиш учун тыла имконият ту\илади.

Калитлар билан бош=ариш жараёни =уйидаги учта мущим былган:

-барча калитларнинг ызаро бо\ли= щолда, яъни бир бутун щолда ишлаши жараёнини таъминлаш (калитлар генерацияси);

-калитлар тыпламининг ма=садли кенгайиб боришини таъминлаш (калитларларнинг тыпланиши);

-калитларларни фойдаланувчилар доирасида та=симлаш (калитлар-ларнинг та=симланиши);

жараёнларига ащамият беришни талаб этади.

КРИПТОГРАФИК СИСТЕМАЛАРНИНГ МУЩИМ МАСАЛАЛАРИ ВА РИВОЖИ

Катта щажмдаги маълумотларни шифрлаш

Катта щажмдаги маълумотларни шифрлаш масалалари мультимедия ва ю=ори даражадаги ытказиш щамда узатиш имкониятларига эга былган ало=а тармо=лари воситаларининг вужудга келиши билан бо\ли=.

Ахборотларни мущофазалаш ты\рисида гап борганда кенг маънодаги бирор алфавитда ёзилган ани= матн тушинилди. Аммо щозирги замонавий ахборот тизимларидаги маълумотлар матн кыринишдаги хусусиятдан фар=ли ыларо= ю=ори даражада ривожланиб бораётган ало=а технологиларининг мащсули былган:

-факс, тасвир ва сыз ало=а тизимлари;

-овозли почта;

-тасвирли конференциялар ытказишда тасвирли (видно) ало=а

тизимлари;

ва бош=а шу кабиларни ыз ичига олади. Бундан эса криптология юту=ларидан фойдаланиб шу ало=а тизимлари маълумотларини мущофазалашнинг ызига хос услубларни ишлаб чи=иш масалаларини ечиш вазифалари келиб чи=ади.

Ахборотларни шифрлаш, кодлаштириш ва си=иш

+уйида келтирилаётган жадвалда ахборотларни шифрлаш, кодлаштириш ва си=иш жараёнларининг ма=сад ну=таи назаридан турлича эканлиги кыринади.

Ахборотни акслантириш тури.	Ма=сади	Акслантиришдан сынг ахборот щажмининг ызгариши
Шифрлаш	- махфий маьлумотни ало=а канали тизимида жынатиш; - маьлумотни ра=иб томонидан ызгартирилишига йыл =ыймасдан унинг ха=и=ийлигини таъмннлаш	Одатда ызгармайди, фа=ат ра=амли сигнатура ва имзо щисобига кыпаяди
Щар хил щала=ит берилишларига бардошли былган кодлаштириш	Маълумотларни ало=а канали тизимида хар-хил щала=ит беришлар эвазига ызгаришидан мущофазалаш	Кыпаяди
Си=иш (компрессиялаш)	Са=ланаётган ва узатилаётган маълумотлар щажмини кис=артириш	Камаяди

Кыриниб турибдики, бу уч турдаги маълумотларни акслантириш бир-бирини тылдиради ва уларнинг щаммасидан биргаликда фойдаланиш ало=а тармо\и (канали) тизимларидан самарали фойдаланишга олиб келади.

Криптографик услубларнинг амалдаги =ылланишлари ща=ида

Маълумотларни мущофазалаш услубларининг амалда =ылланиши масаласи =уйидаги ызининт мущим томонларига эга:

-криптографик алгоритмларнинг амалда =ылланишини таъминловчи воситаларни яратиш ёки ишлаб чи=ариш;

-яратилган ёки ишлаб чи=илган воситалардан фойдаланиш услублари.

Щар бир крипторафик услуб бирор алгоритммик тилда дастур тузишга ёки шу услубни амалдаги =ылланишини таъминловчи асбоб-ускуна жищозлари кырин ишидаги яратилишнинг табиий омилларини ту\дириши керак.

Криптографик алгоритмнинг дастурлаш воситаси амалда =ылланилганда формал математик алмаштириш амалларининг бирор чекли кетма-кетлигига асосланади.

Шифрлаш ва дешифрлаш амалларининг асбоб-ускуналар воситасида таъминланиши махсус электрон схемалар асосида амалга оширилади ва бунда гаммалаштириш услубини =ышиб олиб борилади. Чунки гаммалаштириш услуби ю=ори даражадаги криптобардошлиликни таъминлаб, нисбатан соддаро= амалий =ылланиш имкониятларига щам эга. Гаммалаштиришнинг асосини ташкил этувчи тасодифий битлар кетма-кетлигини ишлаб чи=арувчи генератор сифатида чизи=ли ва чизи=ли былмаган сонли акслантириш амалларини бажарувчи кычиш (силжиш) регистрларидан фойдаланилади.

Бундай бош=аришнинг мощияти электрон =урилмаларда бирор щажмдаги маълумотни шифрлаб былингандан сынг, электрон =урилманинг хотира регистрларига жойлашган мана шу шифрланган маълумотнинг белгиларини бирор услуб билан даврий равишда ызгартирилиши билан бо\ли=. Чизи=ли былмаган акслантириш амалларини бажарувчи кычиш регистрларидан фойдаланиш тасодифий битлар кетма-кетлигидан иборат былган гамманинг мураккаб щолда вужудга келиши билан бо\ли= былиб, криптоанализ масалаларининг ечилишини мураккаблаштиради.

Дастурлаш услубларидан фойдаланиб маълумотларни музофазалашнинг =улайлиги ва юту\и унинг асосини ташкил этувчи криптографик шифрлаш алгоритмининг маълумотларни математик амаллар билан тез ва ма=садли ызгартиришни таъминлаш имкониятларининг мавжудлигидадир.

Дастурлаш услубининг асосий камчилиги эса унинг электрон схемалар кырин ишдаги асбоб-ускуналар воситасида шифрлаш ва дешифрлашга нисбатан секин ишлашидадир.

Дастурлаш ва асбоб-ускуналар воситаларини =ышиб олиб боришга асосланган шифрлаш щамда дешифрлаш криптографик услублари компьютерлар тизими билан бо\ли= былган ахборотларни мущофазалаш сощасида компьютерларга "криптографик =ышимча-процессор"ларнинг ишлаб чи=арилиши ва ырнатилиши билан бо\ли=. Бу "криптографик =ышимча-процессор" щисоблаш курилмаси былиб, криптографик амаллар: модул быйича =ышиш, регистрларнинг силжишини таъминлаш ва бош=а шу каби вазифаларни бажаради. Бундай =урилмалар учун дастурлаш алгоритмини ызгартириш билан шифрлаш жараёнида фойдаланилаётган услубларнинг ызгаришини бош=ариш мумкин.

Шундай =илиб, бирор ахборотлар тизимида маълумотларни крип-тографик услублар билан мущофазалаш, шу ахборотлар тизими сощасининг ызига хос мущим былган хусусиятли томонларини чу=ур ва кенг тащлил =илган щолда мос келувчи криптографик мущофаза услубини танлашни та=азо этади.

Таянч иборалари

Электрон имзо, ра=амли сигнатур, модификациялаш, сохталаштириш, имитациялаш.

Назорат саволлари

1. Калитлар билан бош=ариш жараёнини тушунтиринг.
2. Ахборотларни шифрлаш, кодлаштириш ва си=иш жараёнларининг тушунтириб беринг.

Асосий адабиёт

1. Анохин М.И., Варнавский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. М. 1997г.
2. Брюс Шнайер. Прикладная криптография: 2– е издание. М. 2001.
3. Фомичев В.М. Дискретная математика и криптология. М. «Диалог МИФИ» 2003 г. http: ‖ www.library.mephi.ru – Библиотека МИФИ.
4. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М. «Радио и связь» 2001г.
5. Московский центр непрерывного математического образования. Материалы 1 – 9 олимпиад по криптографии. М. 2001 – 2003гг. http: ‖ www. ibc.ry./- электронная библиотека Московского Государственного Университета экономики, статистики и информатики.
6. В.А.Хорошко, А.А.Чекатков. Методы и средства защиты информации. Издательство «ЮНИОР» К. 2003.

Кушимча адабиёт

1. Анин Б. Защита компьютерной информации. Санкт – Петербург, 2002.
2. Завгородный В.И. Комплексная защита информации в компьютерных системах., М. «Логас», 2001.
3. А.В.Домашев, М.М.Грунтович, В.О.Попов, Д.И.Правиков, А.Ю.Щербаков, И.В.Ппокофьев. Программирование алгоритмов защиты информации. Учебное пособие. Издательство «Нолидж». М. 2002.

Маъруза 9

Щимоялаш тизимининг комплекслилиги

1. Электрон тыловлар тизими асослари.
2. Идентификацияловчи шахсий номерни щимоялаш.
3. POS тизими хавфсизлигини таъминлаш.
4. Банкоматлар хавфсизлигини таъминлаш.

Щимоя тизимининг комплекслилигига ундан щу=у=ий, ташкилий, мухандис-техник ва дастурий – математик элементларининг мавжудлиги билан эришилади. Элементлар нисбати ва уларнинг мазмуни ташкилотларнинг ахборотни щимоялаш тизимининг ызига хослигини ва унинг такрорланмаслигини щамда бузиш =ийинлигини таъминлайди.

Ани= тизимни кып турли эементлардан иборат, деб тасаввур =илиш мумкин. Тизим элементларининг нафа=ат унинг ызига хослигини, балки ахборотнинг =имматлилигини ва тизимнинг =ийматини щисобга олган щолда белгиланган щимоя даражасини ани=лайди.

Ахборотни щу=у=ий щимоялаш элементи щимоялаш чораларининг ща=ли эканлиги маъносида ташкилот ва давлатларнинг ызаро муносабатларини юридик мустащкамлаш щамда персоналнинг ташкилот =имматли ахборотини щимоялаш тартибига риоя =илиши ва ушбу тартибни бузилишида жавобгарлиги тасаввур =илинади.

Электрон тыловлар тизимида ахборотларни щимоялаш.

Электрон тыловлар тизими асослари.

Электрон тыловлар тизими деб банк пластик карталарини тылов воситаси сифатида =ылланилишидаги усуллар ва уларни амалга оширувчи субъектлар мажмуасига айтилади.

Пластик карта – шахсий тылов воситаси былиб, у мазкур воситадан фойдаланадиган шахсга товар ва хизматларни на=дсиз пулини тылаш, бундан таш=ари банк муассасалари ва банкоматлардан на=д пулни олишга имкон беради.

Пластик картани тылов воситаси сифатида =абул =илувчилар, савдо ва хизмат кырсатувчи корхоналар, банк былимлари щамда бош=алар шу пластик карталарга хизмат кырсатувчи =абул =илувчилар тармо\ини ташкил этади.

Электрон тыловлар тизимини яратишда пластик карталарга хизмат кырсатиш =онун-=оидаларини ишлаб чи=иш ва уларга риоя =илиш асосий масалалардан бири былиб щисобланади. Ушбу =оидалар нафа=ат техникавий (маълумотларни стандартлаш, ускуналар ва бош=алар), балки молиявий масалалар (корхоналар билан щисобларни бажариш тартиби) ни щам =амраб олади.

Электрон тыловлар тизимининг фаолиятини =уйидагидек тасаввур =илиш мумкин.

Электрон тыловлар тизими билан биргаликда фаолият кырсатадиган банк икки, яъни **банк-эмитент ва банк – эквайер** тоифасида хизмат кырсатади:

Банк – эмитент пластик карталарни ишлаб чи=аради ва уларнинг тылов воситаси сифатида =ылланилишига кафолат беради.

Банк – эквайер савдо ва хизмат кырсатувчи ташкилотлар томонидан =абул =илинган тыловларни банк былимлари ёки банкоматлар ор=али амалга оширади.

Щозирги кунда автоматлаштирилган савдо POS(Point-Of-Sale- сотилган жойда тылаш)-терминали ва банкоматлар кенг тар=алган.

POS- терминалда пластик картадан маълумотлар ы=илади ва мижоз ыз PIN- коди (Personal Identification Number-идентификацияловчи шахсий номер)ни киритади ва клавиатура ор=али тылов учун зарурий =иймат терилади.

Агар мижозга на=д пул керак былса, бу щолда у банкоматдан фойдаланиши мумкин.

Ушбу жараёнларни бажаришда **жараёнлар маркази** имкониятларидан фойдаланилади.

Жараёнлар маркази – махсуслаштирилган сервис ташкилот былиб, банк – эквайерларидан ёки хизмат кырсатиш манзилларидан келадиган муаллиф сыровномаларини ва транзакция протоколларини =айта ишлашни таъминлайди. Ушбу ишларни амалга ошириш учун жараёнлар маркази маълумотлар базасини киритади. Бу маълумотлар базаси тылов тизими, банк

аъзолари ва пластик карта сощиблари ты\рисидаги маълумотларни ыз таркибига олади.

Пластик карталар тылов быйича **кредитли** ва **дебетли** былиши мумкин.

Кредитли карталар быйича капта сощибига кыпинча мущлати 25 кунгача былган ва=тинча =арз берилади. Буларга Visa, Master Card, American Express карталари мисол была олади.

Дебетли карталарда карта сощибининг банк – эмитентидаги щисобига олдиндан маълум ми=дорда мабла\жойлаштиради. Ушбу мабла\дан харид учун ишлатилган мабла\лар суммаси ошиб кетмаслиги лозим.

Ушбу карталар фа=атгина шахсий эмас, балки корпоратив щам былиши мумкин.

Щозирги кунда **микропроцессорли карталар** ишлаб чи=илмо=да. Ушбу карталарнинг олдингиларидан асосий фар=и бу мижознинг барча маълумотлари унда акс эттирилган былиб, барча **транзакциялар,** яъни маълумотлар базасини бир щолатдан иккинчи щолатга ытказувчи сыровномалар, off-line режимда амалга оширилади, шу боис улар ю=орри даражада щимояланган деб эътироф этилган. Уларнинг нархи =имматро= былсада, телекоммуникация каналларида фойдаланилмаслик муносабати билан унда фойдаланиш =иймати арзондир. Электрон тылов тизимларининг =уйидаги заиф =исмлари мавжуд:

- банк ва мижоз, банклараро, банк ва банкомат орасида тылов маълумотларини жынатиш;
- ташкилот доирасида маълумотларни =айта ишлаш.

Булар ыз навбвтида =уйидаги муаммоларни юзага келтиради:

- абонентларнинг ща=и=ийлигини ани=лаш;
- ало=а каналлари ор=али жынатилаётган электрон щужжатларни щимоялаш;
- электрон щужжатларининг юборилганлигига ва =абул =илинганлигига ишонч =осил =илиш;
- щужжатларнинг бажарилишини таъминлаш.

Электрон тыловлар тизимида ахборотларни щимоялаш функцияларини таъминлаш ма=садида =уйидагилар амалга оширилиши керак:

- тизимнинг четки бы\инларига киришни бош=ариш;
- ахборотларнинг яхлитлигини назорат =илиш;
- абонентларни ызаро аутентификациялаш;
- хабарнинг муаллифлигидан воз кеча олмаслик;
- хабарни етказилганлигини кафолатлаш;
- хабар быйича бажариладиган чора-тадбирлардан воз кеча олмаслик;
- хабарларни кетма-кетлигини =айд =илиш;
- кетма – кет хабарлар яхлитлигини таъминлаш.

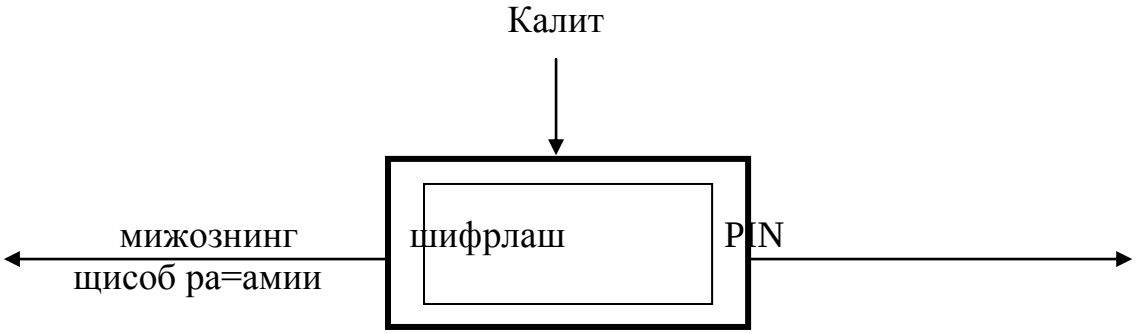
Идентификацияловчи шахсий номерни щимоялаш.

PIN- кодларини щимоялаш тылов тизимини щавфсизлигини таъминлашда асосий омилдир. Шу боис, у фа=атгина карта сощибга маълум былиб, электрон тыловлар тизимида са=ланмайди ва бу тизим быйича юборилмайди.

Умуман олганда, PIN банк томонидан берилиши ёки мижоз томонидан таналаниши мумкин. Банк томонидан бериладиган PIN =уйидаги икки вариантдан бири быйича амалга оширилади:

1) мижоз щисоб ра=ами быйича криптография усули билан ташкиллаштирилади;

Ушбу жараённи =уйидагича тасвирлаш мумкин.



Ушбу усулнинг афзаллиги PIN коди электрон тыловлар тизимида са=ланиши шарт эмаслигидадир, камчилиги эса ушбу мижоз учун бош=а PIN берилиши лозим былса, унга бош=а щисоб ра=амии очилиши зарурлигида, чунки банк быйича бита калит =ылланилади.

2) банк ихтиёрий PIN кодни таклиф =илади ва уни ызида шифрлаб са=лайди. PIN кодни хотирада са=лаш =ийинлиги ушбу усулнинг асосий камчилиги былиб щисобланади.

Мижоз томонидан танланадиган PIN код =уйидаги имкониятларга эга:

- барча ма=садлар учун ягона PIN кодни =ыллаш;
- щарфлар ва ра=амлардан ашкил этилган PIN кодни хотира са=лашнинг енгиллиги.

PIN коди быйича мижозни идентификациялаштиришнинг икки усули билан бажариш мумкин: **алгоритмлашган ва алгоритмлашмаган.**

Алгоритмлашмаган текшириш усулида элемент киритган PIN код маълумотлар базасидаги шифрланган код билан та==осланилади.

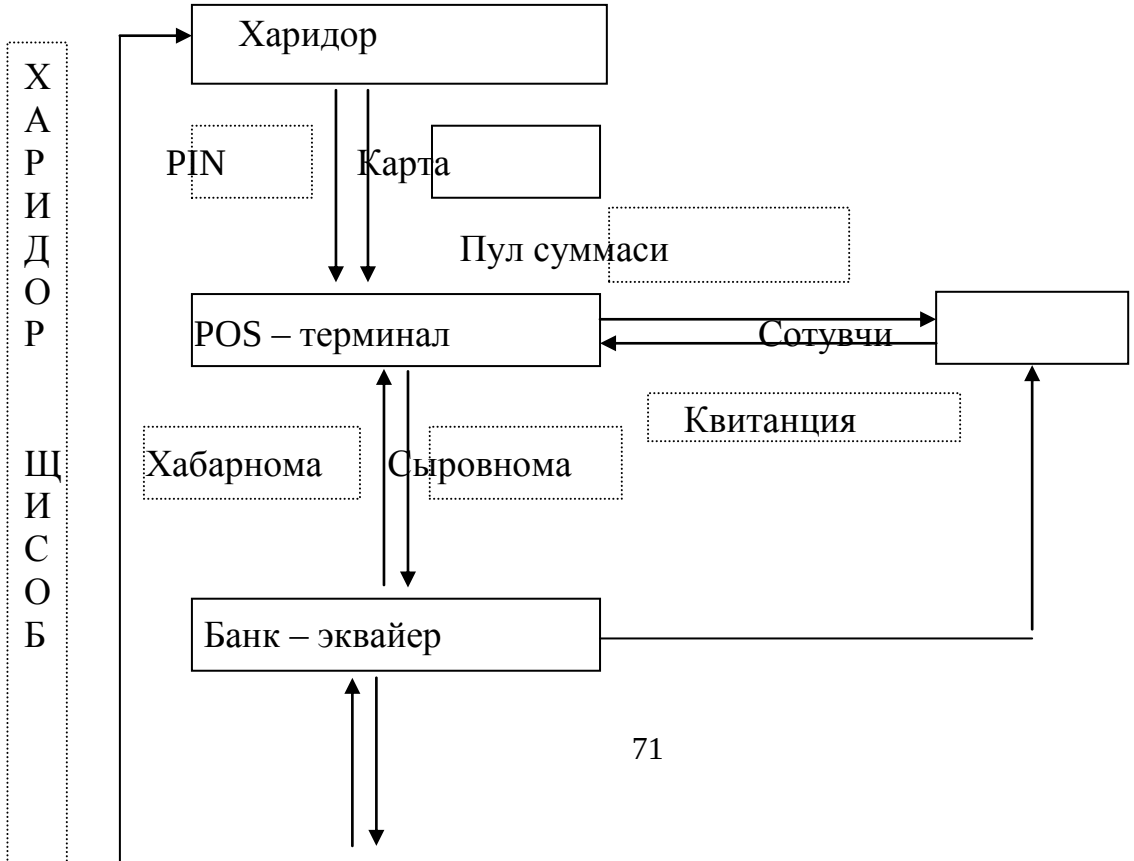
Алгоритмлашган текшириш усулида эса мижоз киритган PIN код, махфий калитдан фойдаланган щолда, махсус алгоритм быйича ызгартирилади ва картадаги ёзув билан та==осланилади.

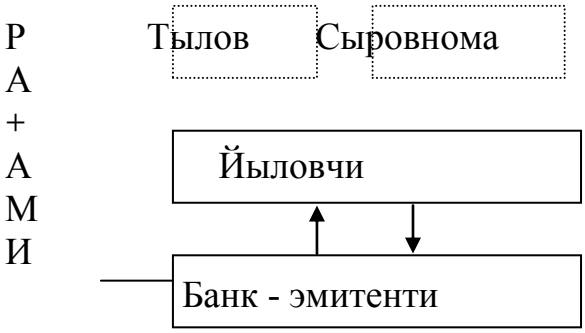
Ушбу усулнинг афзалликлари:

- асосий компьютерда PIN са=ланмайди ва натижада персонал томонидан
- ы\ирланмайди;
- PIN код телекоммуникация ор=али жынатилмайди.

POS тизими хавфсизлигини таъминлаш

POS тизимини ани= тасаввур =илиш учун =уйидаги чизмани келтирамиз





Ушбу чизма быйича харидор ыз пластик картасини ырнатиб, PIN кодини киритади.

Сотувчи ыз навбатида пул суммасини киритади. Шундан сынг, банк – эквайерга (сотурвчи банки) пулни кычириш учун сыровнома юборилади

Банк – эквайер, ыз навбатида, картанинг ща=и=ийлигини ани=лаш учун сыровномани банк – эмитентга жынатади. Натижада, банк – эмитент пулни банк – эквайерга сотувчи щтсобига кычиради. Пул кычирилгандан сынг, банк – эквайер томонидан POS – терминалга хабарнома жынатилади. Ушбу хабарда транзакция бажарилганлиги ща=ида маълумот былади.

Шундан сынг, сотувчи харидор мах\щсулот ва квитанциясини та=дим этади.

ЫЗ – ызидан кыриниб турибдики, ушбу жараёнда щар хил во=еалар содир былиши мумкин.

POS тизимининг энг заиф =исми бу POS – терминалдир. Бундаги асосий хавф былиб терминалдаги махфий калитнинг ы\ирланиши щисобланади.

Бунинг о=ибатлари =уйидагилар былиши мумкин:

- олдинги транзакцияларда ишлатилган PIN кодни тиклаш;
- кейинги транзакцияларда =ылланиладиган PIN кодни тиклаш.

Ушбу хавфлардан щимояланишнинг 3 та усули таклиф этилади:

- щар бир транзакциясидан сынг калитни ызгартириш;
- POS – терминал ва банк – эквайер орасидаги маълумотларни махсус калит билан шифрлаш щамда калитни щар бир транзакциядан сынг ызгартириш;
- очи= калитлар усули ёрдамида узатиладиган маълумотларни шифрлаш.

Банкоматлар хавфсизлигини таъминлаш

Банкоматлар на=д пул олиш, щисоб ра=амнинг щолати ва пул кычириш имкониятларига эга.

Банкомат икки режимда ишлайди, off – line ва on – line.

Off – line режимда банкомат банк компьютерларидан муста=ил ишлайди ва бажариладиган транзакциялар ща=идаги ёзувларни ыз ыз хотирасида са=лайди щамда принтерга узатиб, уларни чоп =илади.

On – line режимда банкомат бевосита банк компьютерлари билан телекоммуникация ор=али уланган былади. Транзакциясини амалга ошириш ма=садида банкомат банкдаги компьютерлар билан =уйидаги хабарлар билан алмашади:

- банкомат сыровномаси;
- банкнинг жавоб хабари;
- банкоматнинг тыловини бажарганлиги ща=идаги хабарни бериш.

Щозирги кунда банкоматлар тармо=ларидан бир неча банкларгина фойдаланади. Бу ерда мавжуд былган асосий муаммо бу банкларнинг махфий ахборотларини (масалан, махфий калит) бир – биридан щимоялашдир.

Ушбу муаммонинг ечими сифатида PIN кодни, марказлаштирилган щолда, щар бир банк томонидан текшириш таклиф =илинади.

Бундан таш=арии банкоматлар тармо\и зоналарга та=симланади ва щар бир зона ZCMK (Zone Control Master Key) калитлари, ыз навбатида, компьютер тармо\идаги калитларни шифрлашда =ылланилади. Маълумотларни шифрлашда эса IWK (Issuer Working Key) калитлар ишлатилади.

Ахборотларни ташкилий щимоялаш элементлари

Щимоялаш технологияси персонални ташкилотнинг =имматли ахборотларини щимоялаш =оидаларига риоя =илишга ундовчи бош=ариш ва чеклаш характерига эга былган чора-тадбирларни ыз ичига олади.

Ташкилий щимоялаш элементи бош=а барча элементларни ягона тизимга бо\ловчи омил былиб щисобланади. Кыпчилик мутахассисларнинг фикрича, ахборотларни щимоялаш тизимлари таркибида ташкилий щимоялаш 50-60% ни ташкил =илади. Бу щол кып омилларга бо\ли=, жумладан, ахборотларни ташкилий щимоялашнинг асосий томони амалда щимоялашнинг принципи ва усулларини бажарувчи персонални танлаш, жойлаштириш ва ыргатиш щисобланади.

Ахборотларни щимоялашнинг ташкилий чора - тадбирлари ташкилот хавфсизлиги хизматининг меъёрий услубий щужжатларида ыз аксини топади. Шу муносабат билан кып щолларда ю=орида кырилган тизими элементларининг ягона номи – ахборотни ташкилий – ху=у=ий щимоялаш элементини ишлатадилар.

Ахборотларни мущандис – техник щимоялаш элементи – техник воситалар комплекси ёрдамида худуд, бино ва =урилмаларни =ыри=лашни ташкил =илиш щамда техник текшириш воситаларига =арши суст ва фаол кураш учун мылжалланган. Техник щимоялаш воситаларнинг нархи баланд былсада, ахборот тизимини щимоялашда бу элемент мущим ащамиятга эга.

Ахборотни щимоялашнинг дастурий – математик элементи компьютер, локал тармо= ва турли ахборот тизимларида =айта ишланадиган ва са=ланадиган =имматли ахборотларни щимоялаш учун мылжалланган.

Ахборот тизимларида маълумотларга нисбатан

хавф – хатарлар

Компьютер тизими (тармо\и)га зиён етказиши мумкин былган шароит, щаракат ва жараёнлар **компьютер тизими (иармо\и) учун хавф – хатарлар,** деб щисобланади.

Автоматлаштирилган ахборот тизимларига тасодифий таъсир кырсатиш сабаблари таркибига =уйидагилар киради.

Маълумки, компьютер тизим (тармо\)ининг асосий компонентлари – техник воситалари, дастурий – математик таъминот ва маълумотлардир.

Назарий томондан бу компонентларга нисбатан тырт турдаги хавфлар мавжуд, яъни **узилиш, тутиб =олиш, ызгартириш ва сохталаштириш:**

- узилиш - =андайдир таш=и щаракатлар (ишлар, жараёнлар)ни бажариш учун щозирги ишларни ва=тинча марказий прочессор =урилмаси ёрдамида тыхтатишдир, уларни бажаргандан сынг процессор олдинги щолатига =айтади ва тыхтатиб =ыйилган ишни давом эттиради. Щар бир узилиш тартиб ра=амига эга, унга асосан марказий процессор =урилмаси =айта ишлаш учун =исм – дастурни =идириб топади. Процессорлар икки турдаги узилишлар билан ишлашни вужудга келтириши мумкин: дастурий ва техник. Бирор =урилма фав=улодда хизмат кырсатилишига мущтож былса, унда техник узилиш пайдо былади. Одатда бундай узилиш марказий процессор учун кутилмаган щодисадир. Дастурий узилишлар асосий дастурлар ичида процессорнинг махсус буйру=лари ёрдамида бажарилади. Дастурий узилишда дастур ыз – ызини ва=тинча тыхтатиб, узилишга талу=ли жараённи бажаради.

- тутиб олиш – жараёни о=ибатида \аразли шахслар дастурий воситалар ва ахборотларнинг турли магнитли ташувчиларига киришни =ылга киритади. Дастур ва маълумотлардан но=онуний нусха олиш, компьютер тармо=лари ало=а каналларидан номуаллифлик ы=ишлар ва щоказо щаракатлар тутиб олиш жараёнларига мисол была олади.

- ызгартириш – ушбу жараён ёвуз ниятли шахс нафа=ат компьютер тизими компонентларига (маълумотлар тыпламлари, дастурлар, техник элементлари) киришни =ылга киритади, балки улар билан манипуляция (ызгартириш, кыринишини ызгартириш) щам =илади. Масалан, ызгартириш сифатида \аразли шахснинг маълумотлар тыпламидаги маълумотлар тыпламидаги маълумотларни ызгартириш, ёки умуман компьютер тизими файлларини ызгартириши, ёки =андайдир =ышимча но=онуний =айта ишлашни амалга ошириш ма=садида фойдаланилаётган дастурнинг кодини ызгартириши тушунилади;

- сохталаштириш – щам жараён саналиб, унинг ёрдамида \аразли шахслар тизимда щисобга олинмаган вазиятларни ырганиб, ундаги камчиликларни ани=лаб, кейинчалик ызига керакли щаракатларни бажариш ма=садида тизимга =андайдир сохта жараённи ёки тизим ва бош=а фойдаланувчиларга сохта ёзувларни юборади.

Ахборотларни криптографик щимоялаш усуллари

Криптография ща=ида асосий тушунчалар

«Криптография» атамаси дастлаб «яшириш, ёзувни беркитиб =ыймо=» маъносини билдиради. Биринчи, марта у ёзув пайдо былган даврлардаё= айтиб ытилган. Щозирги ва=тда криптография деганда щар =андай шаклдаги, яъни дискда са=ланадиган сонлар кырининшида ёки щисоблаш тармо=ларида узатиладиган хабарлар кырининшидаги ахборотни яшириш тушунилади. Криптографияни ра=амлар билан кодланиши мумкин былган щар =андай ахборотга нисбатан =ыллаш мумкин. Махфийликни таъминлашга =аратилган криптография кенгро= =ылланилиш доирасига эга. Ани=ро= айтганда, криптографияда =ылланиладиган усулланинг ызи ахборотни щимоялаш билан бо\ли= былган кып жараёнларда ишлатилиши мумкин.

Криптография ахборотни рухсатсиз киришдан щимоялаб, унинг махфийлигини таъминлайди. Масалан, тылов вара=ларини электрон почта ор=али узатишда унинг ызгартирилиши ёки сохта ёзувларнинг =ышилиши мумкин. Бундай щолларда ахборотнинг таъминлаш зарурияти пайдо былади. Умуман олганда компьютер тармо\ига рухсатсиз киришнинг мутла=о олдини олиш мумкин эмас, лекин уларни ани=лаш мумкин. Ахборотнинг яхлитлигини текширишнинг бундай жараёни, кып щолларда, ахборотнинг ща=и=ийлигини таъминлаш дейилади. Криптографияда =ылланиладиган усуллар кып былмаган ызгартиришлар билан ахборотларнинг ща=и=ийлигини таъминлаши мумкин.

Нафа=ат ахборотнинг компьютер тармо\идан маъноси бузилмасдан келганлигини билиш, балки унинг муаллифдан кеганлигига ишонч щосил =илиш жуда мущим. Ахборотни узатувчи шахсларнинг ща=и=ийлигини тасди=ловчи турли усуллар маълум. Энг универсал процедура пароллар билан алмашувдир, лекин буж уда самарали былмаган процедура. Чунки паролни =ылига киритган щар =андай шахс ахборотдан фойдаланиши мумкин былади. Агар эщтиёткорлик чораларига риоя =илинса, у щолда паролларнинг самарадорлигини ошириш ва уларни криптографик усуллар билан щимоялаш мумкин, лекин криптография бундан кучлиро= паролни узлуксиз ызгартириш имконини берадиган процедураларни щам таъминлайди.

Криптография сощасидаги охирги юту=лардан бири – ра=амли сигнатура – махсус хосса билан ахборотни тылдириш ёрдамида яхлитликни таъминловчи усул, бунда ахборот унинг муаллифи берган очи= калит маълум былгандагина текширилиши мумкин. Ушбу усул махфий калит ёрдамида яхлитлик текшириладиган маълум усуллардан кыпро= афзалликларга эга.

Криптография усулларини =ыллашнинг баъзи бирларини кыриб чи=амиз. Узатиладиган ахборотнинг маъносини яшириш учун икки хил ызгартиришлар =ылланилади: **кодлаштириш** ва **шифрлаш.**

Кодлаштириш учун тез – тез ишлатиладиган иборалар тыпламини ыз ичига олувчи китоб ёки жадваллардан фойдаланилади. Бу иборалардан щар

бирига, кып щолларда, ра=амлар тыплами билан бериладиган ихтиёрий танланган кодли сыз ты\ри келади. Ахборотни кодлаш учун худи шундай китоб ёки жадвал талаб =илинади. Кодлаштирувчи китоб ёки жадвал ихтиёрий криптографик ызгартиришга мисол былади. Кодлаштиришнинг ахборот технологиясига мос – талаблар - =аторли маълумотларни сонли маълумотларга айлантириш ва аксинча ызгартиришларни бажара билиш. Кодлаштириш китобини тезкор щамда таш=и хотира =урилмаларида амалга ошириш мумкин, лекин бундай тез ва ишончли криптографик тизимни муваффа=иятли деб былмайди. Агар бу китобдан бирор марта рухсатсиз фойдаланилса, кодларнинг янги китобини яратиш ва уни щамма фойдаланувчиларга тар=атиш зарурияти пайдо былади.

Криптографик ызгартиришнинг иккинчи тури **шифрлаш** ыз ичига – бошлан\ич матн белгиларини англаб олиш мумкин былмаган шаклга ызгартириш алгоритмларини =амраб олади. Ызгартиришларнинг бу тури ахборот – коммуникациялар технологияларига мос келади.бу ерда алгоритмни щимоялаш мущим ащамият касб этади. Криптографик калитни =ыллаб, шифрлаш алгоритмининг ызида щимоялашга былган талабларни камайтириш мумкин. Энди щимоялаш объекти сифатида фа=ат калит хизмат =илади. Агар калитдан нусха олинган былса, уни алмаштириш мумкин ва бу кодлаштирувчи китоб ёки жадвални алмаштиришдан енгилдир. Шунинг учун щам кодлаштириш эмас, балки шифрлаш ахборот – коммуникациялар технологияларида кенг =ыламда =ылланилмо=да. Сирли (махфий) ало=алар сощa **криптология** деб айтилади. Ушбу сыз юнонча **«kripto»** - сирли ва **«logus» -** щабар маъносини билдирувчи сызлардан иборат. Криптология икки йыналиш, яъни **криптография** ва **криптотащлил**дан иборат.

Криптографиянинг вазифаси хабарларнинг махфийлигини ва ща=и=ийлигини таъминлашдан иборат.

Криптотащлилнинг вазифаси эса криптографлар томонидан ишлаб чи=илган щимоя тизимини очишдан иборат.

Щозирги кунда **криптотизим**ни икки синфга ажратиш мумкин:

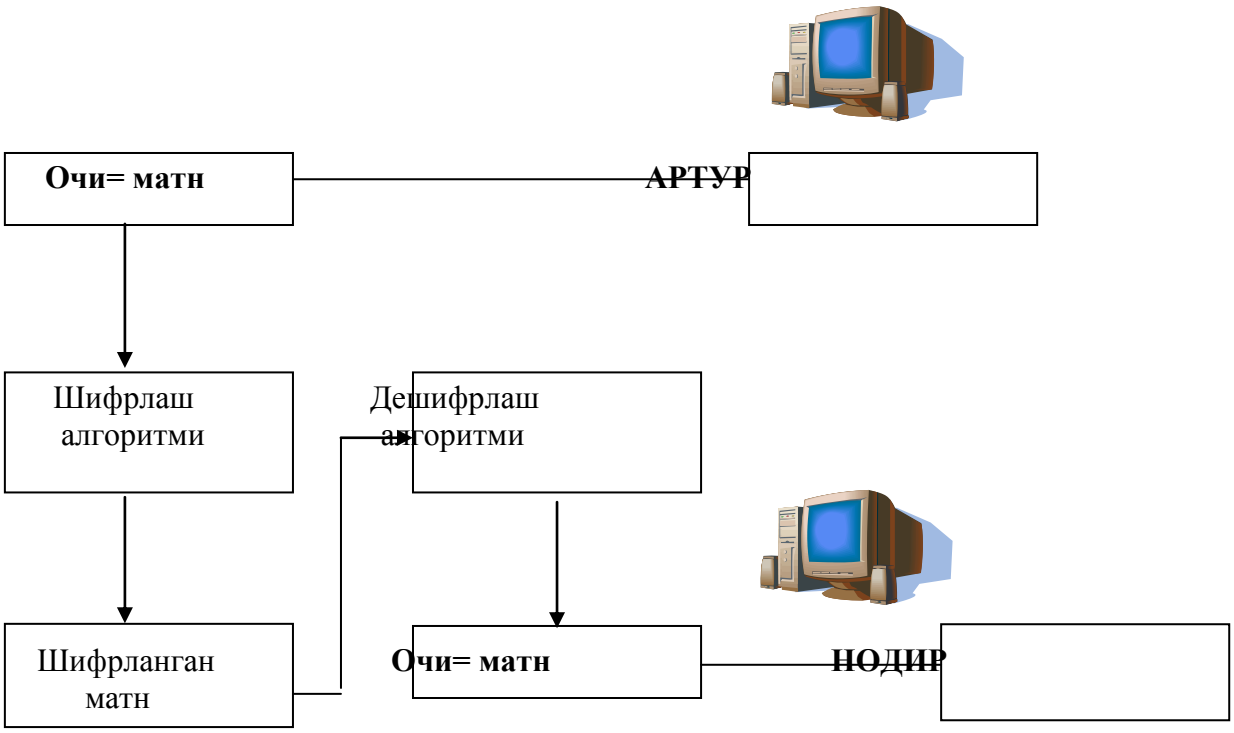
- симметрияли бир калитлик (махфий калит);
- ассиметрияли тизимларда =уйидаги иккита муаммо мавжуд:

1) Ахборот алмашувида иштирок этувчилар =андай йыл билан махфий калитни бир – бирларига узатишлари мумкин?
2) Жынатилган хабарнинг ща=и=ийлигини =андай ани=ласа былади?

Ушбу муаммоларнинг ечими очи= калитли тизимларда ыз аксини топди.

Очи=калитли асимметрияли тизимда иккита калит =ылланиладию биридан иккинчисини щисоблаш усуллари билан ани=лаб былмайди.

Биринчи калит ахборот жынатувчи томонидан шифрлашда ишлатилса, иккинчиси ахборотни =абул =илувчи томонидан ахборотни тиклаш =ылланилади ва у сир са=ланиши лозим.



Ушбу усул билан ахборотнинг махфийлигини таъминлаш мумкин. Агар биринчи калит сирли былса, у щолда уни электрон имзо сифатида =ыллаш мумкин ва бу усул билан ахборотни аутентификациялаш, яъни ахборотнинг яхлитлигини таъминлаш имкони пайдо былади.

Ахборотни аутентификациялашдан таш=арии =уйидаги масалаларни ечиш мумкин:

- Фойдаланувчини аутентификациялаш, яъни компьютер тизими захираларига кирмо=чи былган фойдаланувчини ани=лаш;
- Тармо= абонентлари ало=асини ырнатиш жараёнида уларни ызаро аутентификациялаш.

Щозирги кунда щимояланиши зарур былган йыналишлардан бири бу электрон тылов тизимлари ва Internet ёрдамида амалга ошириладиган электрон савдолардир.

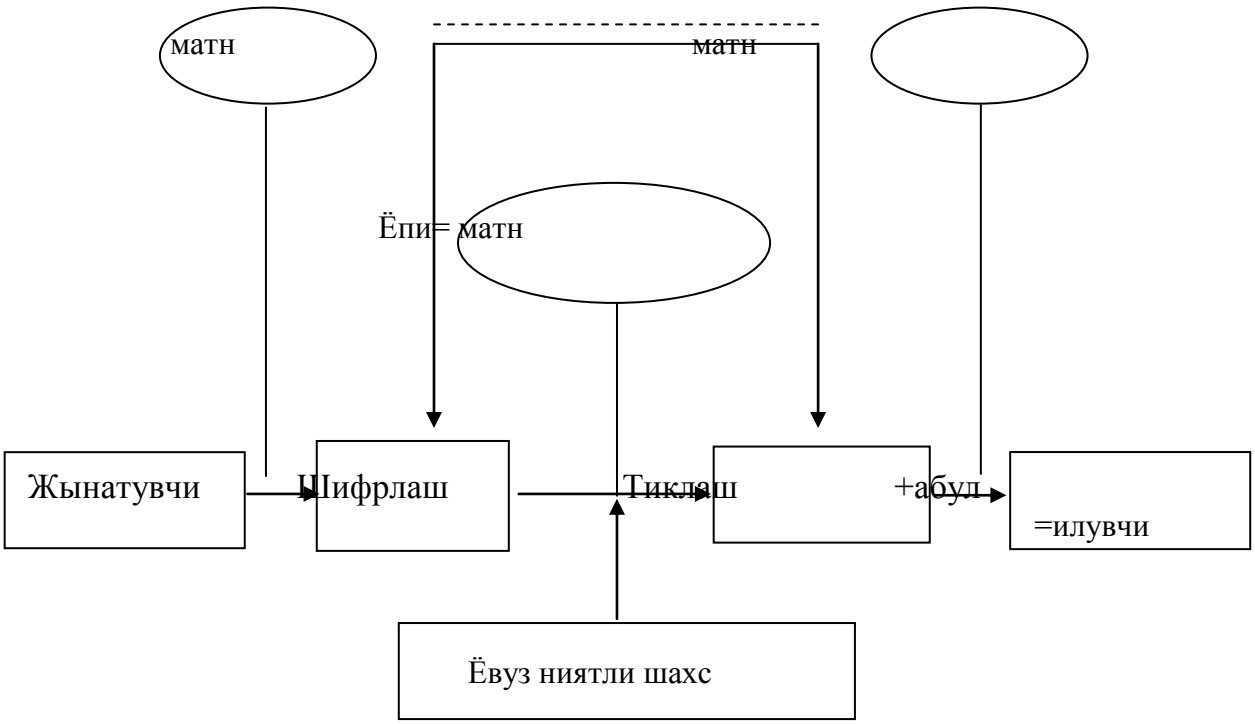
Ахборотларни криптографияли щимоялаш тамойиллари

Криптография – маълумотларни ызгартириш усулларининг тыплам былиб, маълумотларни щимоялаш быйича =уйидаги иккита асосий муаммоларни щал =илишга йыналтирилган: махфийлик; яхлитлик.

Махфийлик ор=али ёвуз ниятли шахслардан ахборотни яшириш тушунилса, **яхлитлик** эса ёвуз ниятли шахслар томонидан ахборотни ызгартира олмаслик ща=ида далолат беради.

Криптография тизимини схематик равишда =уйидагича тасвирлаш мумкин.

КАЛИТ



Бу ерда калит =андайдир щимояланган канал ор=али жынатилади (чизмада пунктир чизи=лар билан тасвирланган). Умуман олганда, ушбу механизм симметрияли бир калитлик тизимига талу=лидир.

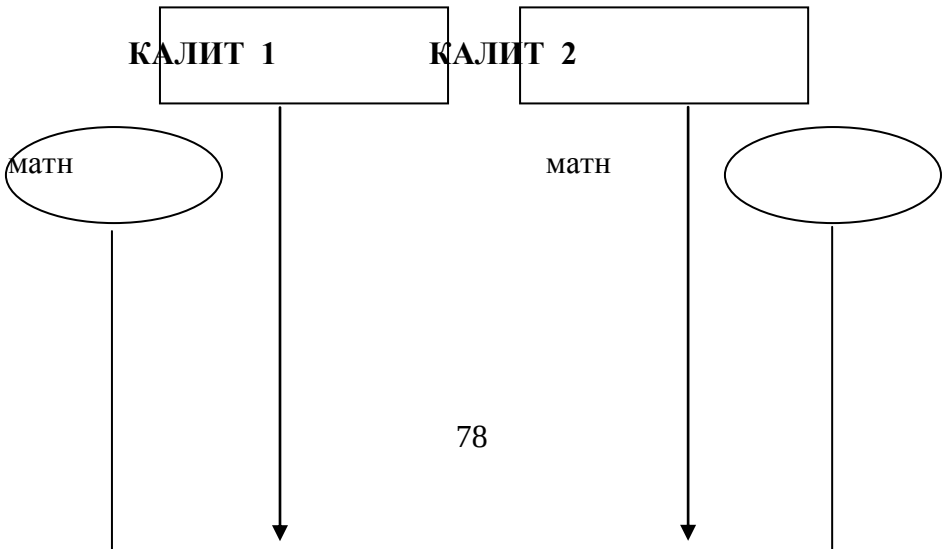
Асимметрия икки калитлик тасвирлаш мумкин:

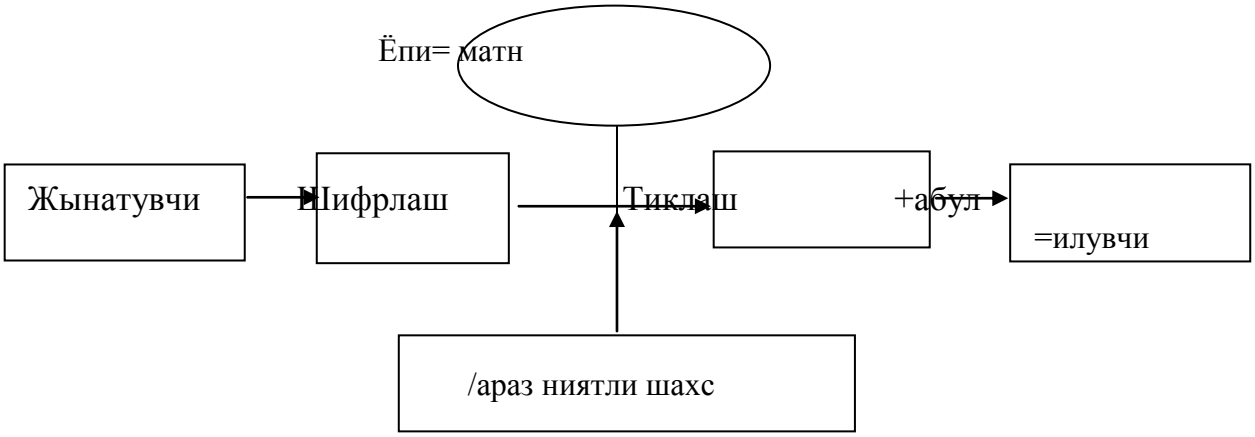
Бу щолда щимояланган канал быйича очи= калит жынатилиб, махфий калит жынатилмайди.

Ёвуз ниятли шахслар ыз ма=садларига эриша олмаса ва криптотащлилчилар калитни билмасдан туриб, шифрланган ахборотни тиклай олмаса, у щолда криптотизим **криптомустащкам тизим** деб айтилади.

Криптотизимнинг мустащкамлиги унинг калити билан ани=ланади ва бу криптотащлилнинг асосий =оидаларидан бири былиб щисобланади.

Ушбу таърифнинг асосий маъноси шундан иборатки, криптотизим барчаларга маълум тизим щисобланиб, унинг ызгартирилиши кып ва=т ва мабла\ талаб =илади, шу боис щам фа=атгина калитни ызгартириб туриш билан ахборотни щимоялаш талаб =илинади.





I. *Фойдаланувчиларни идентификациялаш ва аутентификациялаш тизими.* Ушбу тизим фойдаланувчидан олинган маълумот быйича шахсини текшириш, ща=и=ийлигини ани=лаш ва шундан сынг унга тизим билан ишлашга рухсат бериш лозимлигини белгилаб беради.

Бу щолда асосан фойдаланувчидан олинадиган маълумотни танлаш муаммоси мавжуд былиб, унинг =уйидаги турлари мавжуд:

- фойдаланувчига маълум былган махфий ахборот, масалан, пароль, махфий калит ва бош=алар;
- шахснинг физиологик параметрлари, масалан, бармо= излари, кызнинг тасвири ва бош=алар.

Биринчиси анъанавий, иккинчиси эса биометрик идентификациялаш тизими, дейилади.

II. *Диск маълумотларини шифрлаш тизими.* Ушбу тизимнинг асосий ма=сади дискдаги маълумотларни щимоялашдир. Бу щолда мантии=ий ва жисмоний бо=ичлар ажратилади. Мантии=ий бос=ичда файл асосий объект сифатида былиб, фа=атгина баъзи бир файллар щимояланади. Бунга мисол =илиб, архиватор дастурларини келтириш мумкин. Жисмоний бос=ичда диск тылалигича щимояланади. Бунга мисол сифатида Norton Utilities таркибидаги Diskreet шифрловчи дастурни келтириш мумкин.

III. *Тармо= быйича узатиладиган маълумотларни шифрлаш тизими.* Ушбу тизимда икки йыналишни ажратиш мумкин:

- канал быйича, яъни ало=а каналлари быйича жынатиладиган барча маълумотларни шифрлаш;
- абонентлар быйича, яъни ало=а каналлари быйича жынатиладиган маълумотларнинг фа=атгина мазмуний =исми шифрланиб, =олган хизматчи маълумотларни очи= =олдириш.

IV. *Электрон маълумотларни аутентификациялаш тизими.* Ушбу тизимда тармо= быйича бажариладиган электрон маълумотлар алмашинуви щужжатни ва унинг муаллифини аутентификациялаш муаммоси пайдо былади.

V. *Таянч ахборотларни бош=ариш воситалари.* Ушбу тизимда таянч ахборотлар сифатида компьютер сифатида компьютер тизими ва тармо\ида

=ыланиладиган барча криптографик калитлар тушунилади. Бу щолда калитларни генерациялаш, са=лаш ва та=симлаш каби бош=арув функцияларини ажратишади.

Симметрияли криптотизим асослари

Криптография ну=таи – назаридан шифр – бу калит демакдир ва очи= маълумотлар тыпламини ёпи= (шифрланган) маълумотларга ызгартириш криптография ызгартиришлар алгоритмлари мажмуаси щисобланади.

Калит – криптография ызгартиришлар алгоритмининг баъзи – бир параметрларининг махфий щолати былиб, барча алгоритмлардан ягона вариантини танлайди. Калитларга нисбатан ишлатиладиган асосий кырсаткич былиб, **криптомустащкамлик** щисобланади.

Криптография щимоясида ширларга нисбатан =уйидаги талаблар =ыйилади:

- етрали даражада криптомустащкамлик;
- шифрлар ва =айтариш жараёнининг оддийлиги;
- ахборотларни шифрлаш о=ибатида улар щажмини ортиб кетмаслиги;
- шифрлашдаги кичик хатоларга таъсирчан былмаслиги;

Ушбу талабларга =уйидаги тизимлар жавоб беради:

- ыринларини алмаштириш;
- алмаштииириш;
- гаммалаштириш;
- аналитик ызгартириш.

Ыринларни алмаштириш шифрлаш усули быйича бошлан\ич матн белгиларининг матнли маълум бир =исми доирасида махсус =оидалар ёрдамида ыринлари алмаштирилади.

Алмаштириш шифрлаш усули быйича бошлан\ич матн белгилари фойдаланилаётган ёки бош=а бир алифбо белгиларига алмаштирилади.

Гаммалаштириш усули быйича бошлан\ич матн белгилари шифрлаш гаммаси белгилари, яъни тасодифий белгилар кетма-кетлиги билан бирлаштирилади.

Тащлилий ызгартириш усули быича бошлан\ич матн белгилари аналитик формулалар ёрдамида ызгартирилади, масалан, векторни матрицага кыпайтириш ёрдамида. Бу ерда вектор матндаги белгилар кетма-кетлиги былса, матрица эса калит сифатида хизмат =илади.

Ыринларни алмаштириш усуллари

Ушбу усул энг оддий ва энг =адимий усулдир. Ыринларни алмаштириш усулларига мисол сифатида =уйидагиларни келтириш мумкин:

- шифрловчи жадвал;
- сещрли квадрат.

Шифрловчи жадвал усулида калит сифатида =уйидагилар =ылланилади:

- жадвал ылчовлари;
- сыз ёки сызлар кетма-кетлиги;
- жадвал таркиби хусусиятлари.

Мисол.

+уйидаги матн берилган былсин:

КАДРЛАР ТАЙЁРЛАШ МИЛЛИЙ ДАСТУРИ

Ушбу ахборот устун быйича кетма-кет жадвалга киритилади:

К	Л	А	Л	И	Й	Т
А	А	Й	А	Л	Д	У
Д	Р	Ё	Ш	Л	А	Р
Р	Т	Р	Ь	И	С	И

Натижада, 4х7 ылчовли жадвал ташкил =илинади. Энди шифрланган матн =аторлар быйича ани=ланади, яъни ызимиз учун 4 тадан белгиларни ажратиб ёзамиз.

КЛАЛ ИЙТА АЙАЛ ДУДР ЁШЛА РРТР МИСИ

Бу ерда калит сифатида жадвал ылчовлари хизмат =илади.

Ушбу усулни мураккаблаштириш ма=садида таянч сызини киритса былади. Ю=оридаги мисол учун =уйидаги

МАГИСТР

сызини оламиз ва олдинги жадвалга жойлаштирасиз:

М	А	Г	И	С	Т	Р
4	1	2	3	6	7	5
К	Л	А	Л	И	Й	Т
А	А	Й	А	Л	Д	У
Д	Р	Ё	Ш	Л	А	Р
Р	Т	Р	М	И	С	И

Иккинчи =атордаги ра=амлар харфларнинг алифбо таркибидан келиб чи=ади. Шу =атордаги ра=амлар быйича устунларни тартиблаймиз:

А	Г	И	М	Р	С	Т
1	2	3	4	5	6	7
Л	А	Л	К	Т	И	Й
А	Й	А	А	У	Л	Д
Р	Ё	Ш	Д	Р	Л	А
Т	Р	М	Р	И	И	С

Шифрланган матн =уйидаги кыринишда былади:

ЛАЛК ТИЙА ЙААУ ЛДРЁ ШДРЛ АТРМ РИИС

Сещрли квадрат деб, катакчаларига 1дан бошлаб сонлар ёзилган, ундаги щар бир устунда сатр ва диогонал быйича сонлар йи\индиси 1 та сонга тенг былган квадрат шаклидаги жадвалга айтилади. Сещрли квадратга сонлар тартиби быйича белгилар киритилади ва бу белгилар сатрлар быйича ы=илганда матн щосил былади.

Мисол.

4х4 ылчовли сещрли квадратни оламиз, бу ерда сонларнинг 880 та щар хил комбинацияси мавжуд. +уйидагича иш юритамиз:

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

Бошлан\ич матн сифатида =уйидаги матнни оламиз:

ДАСТУРЛАШ ТИЛЛАРИ

ва жадвалга жойлаштирамиз.

И	С	А	Л
У	Т	И	А
Ш	Р	Л	Л
Т	Р	А	Д

Шифрланган матн жадвал элементларини сатрлар быйича ы=иш натижасида ташкил топади:

ИСАЛ УТИА ШРЛЛ ТРАТ

Алмаштириш усуллари

Алмаштирш усуллари сифатида =уйидаги усулларни келтириш мумкин:

- Цезар усули;
- Афин тизимидаги Цезар усули;
- Таянч сызли Цезар усули ва бош=алар.

Цезар усулида алмаштирувчи щарфлар k та силжиш билан ани=ланади. Юли Цезар бевосита $k = 3$ былганда ушбу усулдан фойдаланган.

$k = 3$ былганда ва алифбодаги харфлар $m = 26$ та былганда =уйидаги жадвал щосил =илинади:

A→D J→M S→V

B→E	K→N	T→W
C→F	L→O	U→X
D→G	M→P	V→Y
E→H	N→Q	W→Z
F→I	O→R	X→A
G→J	P→S	Y→B
H→K	Q→T	Z→C
I→L	R→U	

Мисол.

Матн сифатида SAMARQAND сызини оладиган былсак, Цезар усули натижасида =уйидаги шифрланган ёзув щосил былади:

VDPDUTDQG

Цезар усулининг камчилиги бу бир хил щарфларнинг, ыз навбатида, бир хил щарфларга алмашишидир.

Аффин тизимидаги Цезар усулида щар бир щарфга алмашитирилувчи щарфлар мащсус формула быйича ани=ланади: $at+b(\mathrm{mod}\, m)$, бу ерда a, b – бутун сонлар, $0 \le a,\ b < m,\ \ ЭКУБ(a,\ m) = 1.$

$m = 26,\ a = 3,\ b = 5$ былганда =уйидаги жадвал щосил =илинади:

T	0	1	2	3	4	5
$3t+5$	5	8	11	14	17	20

6	7	8	9	10	11	12
23	0	3	6	9	12	15

13	14	15	16	17	18	19
18	21	24	1	4	7	10

20	21	22	23	24	25
13	16	19	22	25	2

Шунга мос равишда щарфлар =уйидагича алмашади:

A	B	C	D	E	F	G	H
F	I	L	O	R	U	X	A

I	J	K	L	M	N	O	P
D	G	J	M	P	S	V	Y

Q	R	S	T	U	V	W	X
B	E	H	K	N	Q	T	W

Y	Z
Z	C

Натижада ю=орида келтирилган матн =уйидагича шифрланади:

HFPFEBFSO

Таянч сызли Цезар усулида силжитиш билан бирга биргаликда таянч сыз =ылланилади. Таянч сызни =ыллашдан ма=сад щосил =илинадиган алифбода щарфлар кетма-кетлигини ызгартиришдир.

Мисол. $к = 5$ ва DIPLOMAT таянч сызини оламиз ва бу сыз $к-$ыриндан ёзилади:

0	1	2	3	4	5	6	7	8	9	10	11	12	13
A	B	C	D	E	F	G	H	I	J	K	L	M	N
					D	I	P	L	O	M	A	T	

14	15	16	17	18	19	20	21	22	23	24	25
O	P	Q	R	S	T	U	V	W	X	Y	Z

Ушбу таянч сыз алифбодаги кырсатилган жойда жойлаштирилади, ундаги щарфлар инобатга олинмасдан, =олган щарфлар тартиб быйича таянч сыздан кейин кетма-кет ёзилади ва натижада, =уйидаги кыриниш щосил =илинади:

0	1	2	3	4	5	6	7	8	9	10	11	12	13
V	W	X	Y	Z	D	I	P	L	O	M	A	T	B

14	15	16	17	18	19	20	21	22	23	24	25
C	E	F	G	H	J	K	N	Q	R	S	U

Ю=орида кыриб чи=илган SAMARQAND сызи эса мазкур усул ёрдамида HVTVGFVBY га ытказилади.

Щозирги ва=тда компьютер тармо=ларида тижорат ахборотлари билан алмашишда 3 та асосий алгоритмлар, яъни DES, CLIPPER ва PGP алгоритмлари =ылланилмо=да. DES, ва CLIPPER алгоритмлари интеграл схемаларда амалга оширилади. DES алгоритмининг криптомустащкамлигини =уйидаги мисол ор=али щам бащолаш мумкин: 10 млн. А+Ш доллари щаражат =илинганда DES шифрини очиш учун 21 минут, 100 млн. А+Ш доллари щаражат =илинганда эса 2 минут сарфланади. CLIPPER тизими SKIPJACK шифрлаш алгоритмини ыз ичига олади ва бу алгоритм DES

алгоритмидан 16 млн. марта кучлиро=дир. PGP алгоритми эса 1991 йил Филипп Циммердан (А+Ш) томонидан ёзилган ва электрон почта ор=али узатиладиган хабарларни шифрлаш учун ишлатиладиган PGP дастурлар пакети ёрдамида амалга оширилади. PGP дастурий воситалари Internet тармо\ида электрон почта ор=али ахборот жынатувчи фойдаланувчилар томонидан шифрлаш ма=садида кенг фойдаланилмо=да.

Таянч иборалари

Электрон тыловлар тизими, иластик карта, банк – эмитент, банк – эквайер, жараёнлар маркази, кредитли карталар, дебетли карталар, микропроцессорли карталар, транзакция, POS тизими, банкомат

Назорат саволлари

1. Электрон тыловлар тизими нима ва у =андай фаолият кырсатади?
2. Пластик карталар =андай ма=сада ишлатилади?
3. Жараёнлар маркази ща=ида маълумот келтиринг.
4. Электрон тыловлар тизимининг =андай заиф =исмлари мавжуд?
5. Электрон тыловлар тизимларида ахборотларни щимоялаш =андай амалга оширилади?
6. POS тизимининг заиф =исмлари ва бу тизимда щимоялашни усулларини келтиринг.

Асосий адабиёт

1. Анохин М.И., Варнавский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. М. 1997г.
2. Брюс Шнайер. Прикладная криптография: 2– е издание. М. 2001.
3. Фомичев В.М. Дискретная математика и криптология. М. «Диалог МИФИ» 2003 г. http: ‖ www.library.mephi.ru – Библиотека МИФИ.
4. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М. «Радио и связь» 2001г.
5. Московский центр непрерывного математического образования. Материалы 1 – 9 олимпиад по криптографии. М. 2001 – 2003гг. http: ‖ www. ibc.ry./- электронная библиотека Московского Государственного Университета экономики, статистики и информатики.
6. В.А.Хорошко, А.А.Чекатков. Методы и средства защиты информации. Издательство «ЮНИОР» К. 2003.

+ышимча адабиёт

1. Анин Б. Защита компьютерной информации. Санкт – Петербург, 2002.

2. Завгородный В.И. Комплексная защита информации в компьютерных системах., М. «Логас», 2001.

3. А.В.Домашев, М.М.Грунтович, В.О.Попов, Д.И.Правиков, А.Ю.Щербаков, И.В.Ппокофьев. Программирование алгоритмов защиты информации. Учебное пособие. Издательство «Нолидж». М. 2002.