ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АХБОРОТ ТЕХНОЛОГИЯЛАРИ ВА КОММУНИКАЦИЯЛАРИНИ РИВОЖЛАНТИРИШ ВАЗИРЛИГИ
ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

Ҳимояга
кафедра мудири
Иргашева Д.Я._____
«___»_____2015 й.

БАКАЛАВР БИТИРУВ ИШИ

Мавзу: «Аутентификациялаш усули асосида ҳужжатларни қалбакилаштиришдан ҳимоялаш»

Битирувчи _____ Уринов Т.Т

Раҳбар _____ Ғаниев С.К

Тақризчи _____ _____

ҲФХ
маслаҳатчиси _____ Қодиров .Ф.М

Тошкент – 2015

ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АХБОРОТ ТЕХНОЛОГИЯЛАРИ ВА КОММУНИКАЦИЯЛАРИНИ РИВОЖЛАНТИРИШ ВАЗИРЛИГИ
ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

Факультет *Компьютер инжиниринги*
Кафедра *Ахборот хавфсизлиги*
Йўналиш (мутахассислик) *5330300 - Ахборот хавфсизлиги*

«ТАСДИҚЛАЙМАН»
«АХ» кафеда мудири
*Иргашева Д.Я.*_____
«_____» _____ 2015 й.

Битирув ишини бажаришга

ТОПШИРИҚ

Уринов Темур Тулкинович
(фамилия, исми, отасини исми)

1. БМИ мавзуси: Аутентификациялаш усули асосида ҳужжатларни қалбакилаштиришдан ҳимоялаш

2. Университет қарори билан тасдиқланган: «*17*» *январь* 20*15* й. № *59-15*

3. Ишни тўлиқ бажариш учун берилган вақт: *20.03.2015*

4. Ишнинг бошланғич маълумотлари: *Мавзуга доир илмий - техник адабиётлар, Интернет маълумотлари, Microsoft Visual Studio 2010*

5. Ҳисоб тушунтириш матни мундарижаси (ишни бажаришдаги масалалар рўйхати)

Кириш
1. Назарий қисм
2. Асосий қисм
3. Ҳаёт фаолияти хафсизлиги
Хулоса

6. График материаллар рўйхати: *Microsoft Office Power Point 2007 иловасида тайёрланган презентация слайдлари*

7. Топшириқ берилган кун *20.01.2015 г.*

Раҳбар _____(имзо)

Топшириқни олди _____(имзо)

8. БМИнинг ҳар бир бўлимида бажариладиган ишларга маслаҳатлар:

Бўлим	Раҳбар Ф.И.О	Имзо	
		Топшириқ берди	Топшириқ олди
Кириш			
1-бўлим			
2-бўлим			
3-бўлим			
Хулоса			

9. Ишни бажариш графиги:

№	БМИ бўлимларининг номлари	Бажариш муддати	Бажарилганлиги хақида раҳбар имзоси
1.	*Кириш, масаланинг қўйилиши*	*19.01.15-24.01.15*	
2.	*Масаланинг қўйилиши, фан соҳасининг таҳлили*	*26.01.15-14.02.15*	
3.	*Таҳлил қилинган усулларни тадқиқ этиш*	*16.01.15-07.03.15*	
4.	*Ҳаёт фаолияти хавфсизлиги*	*09.03.15-14.03.15*	
5.	*Хулоса*	*16.03.15-20.03.15*	
6.	*Презентация слайдларини ишлаб чиқиш*	*23.03.15-28.03.15*	
7.	*Дастлабки ҳимоя*		

Битирувчи _____ «_____» _____ 2015 й.
(имзо)

Раҳбар _____ «_____» _____ 2015 й.
(имзо)

Ушбу битирув ишида аутентификация усули асосида хужжатларни калбакилаштиришдан химоялаш масалалари кўриб чиқилган. Дастурий таъминот асоси сифатида электрон рақамли имзо танланди. Ҳужжатларни қалбакилаштиришдан ҳимоялашга имкон берувчи дастур ишлаб чиқилди.

В данной выпускной работе расмотрены вопросы защиты документов от подделки на основе метода аутентификации. В качестве основы программного обеспечения выбрана электронная цифровая подпись.Разработана программа,позволяющая защитить документов от подделки.

This paper examined the qualification rasmotreiey the protection of documents against forgery rasmotreiey naosnove authentication methods. As a basis programmenogoh obespecheneya expressed electronic digital podpis.Razrabotana program pazvolyayuschaya protect documents from forgery.

МУНДАРИЖА

Кириш

Маълумки, ҳар қандай давлатнинг ахборот ресурслари уни иқтисодий ва ҳарбий салоҳиятини белгиловчи омилларидан бири ҳисобланади. Ушбу ресурсдан самарали фойдаланиш мамлакат хавфсизлигини ва демократик ахборотлашган жамиятни муваффақиятли шакллантирилишини таъминлайди. Бундай жамиятда,ахборот алмашинув тезлиги юксалади, ахборотларни йиғиш, сақлаш,қайта ишлаш ва улардан фойдаланиш бўйича илғор ахборот-коммуникациялар технологияларини қўллаш кенг кўламда амалга оширилади.

Ахборот дунёсида давлат чегаралари деган тушунча йўқолиб бормоқда. Жаҳон компьютер тармоғи давлат бошқарувини тубдан ўзгартирмоқда.Ҳудудий жойлашишидан қатъи назар, кундалик ҳаётимизга турли хилдаги ахборотлар Internet халқаро компьютер тармоғи орқали кириб келди. Шунинг учун ҳам мавжуд ахборотларга ноқонуний кириш, улардан фойдаланиш ва ўзгартириш, йўқотиш каби муаммолардан ҳимоя қилиш долзарб масала бўлиб қолди.Ахборотлаштириш соҳасидаги давлат сиёсати ахборот ресурслари, ахборот технологиялари ва ахборот тизимларини ривожлантириш ҳамда такомиллаштиришнинг замонавий жаҳон тамойилларини ҳисобга олган ҳолда миллий ахборот тизимини яратишга қаратилган.«Ахборот эркинлиги принциплари ва кафолатлари тўғрисида»ги Қонуннинг қабул қилиниши ҳар кимнинг ахборотни эркин вамонеликсиз олиш ҳамда фойдаланиш ҳуқуқларини амалга оширишда, шунингдек, ахборотнинг муҳофаза қилиниши, шахс,жамият ва давлатнинг ахборот борасидаги хавфсизлигини таъминлашда муҳим аҳамият касб этди»[1,2]

Дарҳақиқат, 2002 йил 12 декабрда қабул қилинган бу қонунда ахборот хавфсизлигини таъминлаш соҳасидаги давлат сиёсати ахборот соҳасидаги ижтимоий муносабатларни тартибга солишга қаратилган бўлади ҳамда шахс,жамият ва давлатнинг ахборот борасидаги хавфсизлигини таъминлаш

соҳасида давлат ҳокимияти ва бошқарув органларининг асосий вазифалари ҳамда фаолият йўналишларини белгилайди.

Компьютер тизимлари ва тармоқларида ахборотни муҳофаза қилиши деганда, узатилаётган, сақланаётган ва ишланилаётган ахборотни ишончлилигини тизимли тарзда таъминлаш мақсадида турли восита ва усулларни қўллаш, чораларни кўриш ва тадбирларни амалга оширишни тушуниш қабул қилинган.Давлатнинг ахборот хавфсизлигини таъминлаш муаммоси миллий хавфсизликни таъминлашнинг асосий ва ажралмас қисми бўлиб, ахборотни муҳофаза қилиш эса давлатнинг бирламчи масалаларига, давлат сиёсати даражасига айланмоқда. [1,3]

Ушбу битирув малакавий иши аутентификация усули асосида ҳужжатларни қалбакилаштиришдан ҳимоялаш масалаларига бағишланади. Битирув малакавий иши 3-та боб хулоса, фойдаланилган адабиётлар, рўйхати ва иловалардан иборат.

Биринчи боб маьлумотларнинг ҳақиқийлигини текшириш тизимларининг тавсифига бағишланган бўлиб ахборот хавфсизлиги тамойили ,аутентификациялаш тизимлари хамда аутентификациялашда электрон рақамли имзодан ва хеш-функциялардан фойдаланиш масалалари акс эттирилган.

Иккинчи боб электрон рақамли имзодан фойдаланган холда ҳужжатларнинг қалбакилаштиришдан ҳимоялашга биноан унинг дастурий модули акс эттирилган.

Учинчи боб ҳаёт фаолияти хавфсизлигини таьминлаш масаласига биноан ишлаб чиқаришда ходимлар саломатлигига зарар етиши ва иш берувчи маьсулияти, техноген хусусиятли фавқулотда вазиятлар ва улардан мухофазаланиш, ўзбекистонда экологик хавфсиликни таьминлаш масалалари акс эттирилган.[1,4]

1.БОБ.Маълумотнинг ҳақиқийлигини текшириш тизимлари

1.1.Ахборот хавфсизлиги тамойили

Идентификация (Identification) - фойдаланувчини унинг идентификатори (номи) буйича аниклаш жараёни. Бу фойдаланувчи тармокдан фойдаланишга уринганида биринчи галда бажариладиган функциядир. Фойдаланувчи тизимга унинг сўрови бўйича ўзининг идентификаторини билдиради, тизим эса ўзининг маълумотлар базасида унинг борлигини текширади.

Аутентификация (Authentication) - маълум қилинган фойдаланувчи, жараён ёки қурилманинг ҳақиқий эканлигини текшириш муолажаси. Бу текшириш фойдаланувчи (жараён ёки қурилма) ҳақиқатан айнан ўзи эканлигига ишонч хосил қилишига имкон беради. Аутентификация ўтказишда текширувчи тараф текширилувчи тарафнинг ҳақиқий эканлигига ишонч хосил қилиши билан бир қаторда текширилувчи тараф ҳам ахборот алмашинув жараёнида фаол қатнашади. Одатда фойдаланувчи тизимга ўз хусусидаги ноёб, бошқаларга маълум бўлмаган ахборотни (масалан, парол ёки сертификат) киритиши орқали идентификацияни тасдиқлайди. Идентификация ва аутентификация субъектларнинг (фойдаланувчиларнинг) ҳақиқий эканлигини аниқлаш ва текширишнинг ўзаро боғланган жараёнидир. Муайян фойдаланувчи ёки жараённинг тизим ресурсларидан фойдаланишига тизимнинг рухсати айнан шуларга боғлиқ. Субъектни идентификациялаш ва аутентификациялашдан сўнг уни авторизациялаш бошланади.[4,5]

Авторизация (Authorization) - субектга тизимда маълум ваколат ва ресурсларни бериш муолажаси, яъни авторизация субъект ҳаракати доирасини ва у фойдаланадиган ресурсларни белгилайди. Агар тизим авторизацияланган шахсни авторизацияланмаган шахсдан ишончли ажрата олмаса бу тизимда ахборотнинг конфиденциаллиги ва яхлитлиги бузилиши мумкин.

Аутентификация ва авторизация муолажалари билан фойдаланувчи харакатини маъмурлаш муолажаси узвий боғланган.

Маъмурлаш (Accounting) - фойдаланувчининг тармоқдаги харакатини, шу жумладан, унинг ресурслардан фойдаланишга уринишини қайд этиш. Ушбу хисобот ахбороти хавфсизлик нуқтаи назаридан тармоқдаги хавфсизлик ходисаларини ошкор қилиш, тахлиллаш ва уларга мос реакция кўрсатиш учун жуда мухимдир. Маълумотларни узатиш каналларини ҳимоялашда *субъектларнинг ўзаро аутентифшацияси,* яъни алоқа каналлари орқали боғланадиган субъектлар ҳақиқийлигининг ўзаро тасдиғи бажарилиши шарт. Ҳақиқийликнинг тасдиғи одатда сеанс бошида, абонентларнинг бир-бирига уланиш жараёнида амалга оширилади. "Улаш" атамаси орқали тармоқнинг иккита субъекти ўртасида мантиқий боғланиш тушунилади. Ушбу муолажанинг мақсади - улаш қонуний субъект билан амалга оширилганлигига ва барча ахборот мўлжалланган манзилга боришлигига ишончни таъминлашдир.[5,4]

Ўзининг ҳақиқийлигининг тасдиқлаш учун субъект тизимга турли асосларни кўрсатиши мумкин. Субъект кўрсатадиган асосларга боглиқ холда аутентификация жараёнлари қуйидаги категорияларга бўлиниши мумкин:

бирор нарсани билиш асосида. Мисол сифатида парол, шахсий идентификация коди PIN (Personal Identification Number) хамда "сўров жавоб" хилидаги протоколларда намойиш этилувчи махфий ва очиқ калитларни кўрсатиш мумкин;[3,5]

бирор нарсага эгалиги асосида. Одатда булар магнит карталар, смарт-карталар, сертификатлар ва touch memory қурилмалари;

кандайдир дахлсиз характеристикалар асосида. Ушбу категория ўз таркибига фойдаланувчининг биометрик характеристикаларига (овозлар, кўзининг рангдор пардаси ва тўр пардаси, бармоқ излари, кафт геометрияси ва х.) асосланган усулларни олади. Бу категорияда криптографик усуллар ва воситалар ишлатилмайди. Беометрик характеристикалар бинодан ёки қандайдир техникадан фойдаланишни назоратлашда ишлатилади.

Парол - фойдаланувчи хамда унинг ахборот алмашинувидаги шериги биладиган нарса. Ўзаро аутентификация учун фойдаланувчи ва унинг шериги ўртасида парол алмашиниши мумкин. Пластик карта ва смарт-карта эгасини аутентификациясида шахсий идентификация номери PIN синалган усул хисобланади. PIN - коднинг махфий қиймати фақат карта эгасига маълум бўлиши шарт. [6,5]

Динамик - (бир марталик) парол - бир марта ишлатилганидан сўнг бошқа умуман ишлатилмайдиган парол. Амалда одатда доимий паролга ёки таянч иборога асосланувчи мунтазам ўзгариб турувчи қиймат ишлатилади.

"Суров-жавоб" тизими - тарафларнинг бири ноёб ва олдиндан билиб бўлмайдиган "суров" қийматини иккинчи тарафга жўнатиш орқали аутентификацияни бошлаб беради, иккинчи тараф эса сўров ва сир ёрдамида хисобланган жавобни жўнатади. Иккала тарафга битта сир маълум бўлгани сабабли, биринчи тараф иккинчи тараф жавобини туғрилигини текшириши мумкин.

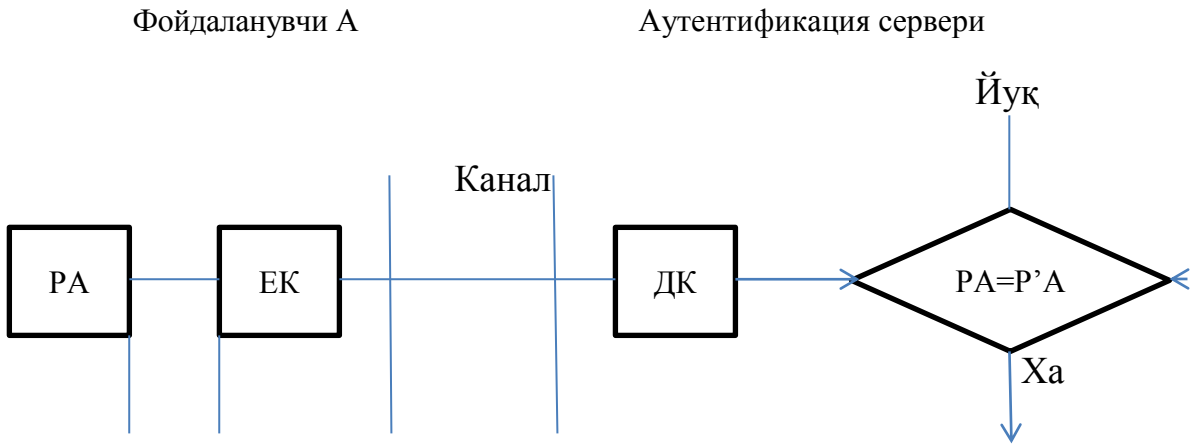
Сертификатлар ва рақамли имзолар - агар аутентификация учун сертификатлар ишлатилса, бу сертификатларда рақамли имзонинг ишлатилиши талаб этилади. Сертификатлар фойдаланувчи ташкилотининг масъул шахси, сертификатлар сервери ёки ташқи ишончли ташкилот томонидан берилади. Internet доирасида очиқ калит сертификатларини тарқатиш учун очиқ калитларни бошқарувчи қатор тижорат инфратузилмалари PKI (Public Key Infrastructure) пайдо бўлди. Фойдаланувчилар турли даража сертификатларини олишлари мумкин.[7,6]

1.2.Аутентификациялаш тизимлари

Пароллар асосида аутентификациялаш

Аутентификациянинг кенг тарқалган схемаларидан бири *оддий аутентификациялаш* бўлиб, у анъанавий кўп мартали паролларни ишлатишига асосланган. Тармоқдаги фойдаланувчини оддий аутентификациялаш муолажасини қуйидагича тасаввур этиш мумкин. Тармоқдан фойдаланишга уринган фойдаланувчи компьютер

клавиатурасида ўзининг идентификатори ва паролини теради. Бу маълумотлар аутентификация серверига ишланиш учун тушади. Аутентификация серверида сақланаётган фойдаланувчи идентификатори бўйича маълумотлар базасидан мос ёзув топилади, ундан паролни топиб фойдаланувчи киритган парол билан таққосланади. Агар улар мос келса, аутентификация муваффақиятли ўтган хисобланади ва фойдаланувчи легал (қонуний) мақомини ва авторизация тизими орқали унинг мақоми учун аниқланган худудларни ва тармоқ ресурсларидан фойдаланишга рухсатни олади.[7]



Равшанки, фойдаланувчининг паролини шифрламасдан узатиш орқали аутентификациялаш варианти хавфсизликнинг хатто минимал даражасини кафолатламайди. Паролни ҳимоялаш учун уни ҳимояланмаган канал орқали узатишдан олдин шифрлаш зарур. Бунинг учун схемага шифрлаш $E_к$ ва расшифровка қилиш D_K воситалари киритилган. Бу воситалар бўлинувчи махфий калит К орқали бошқарилади. Фойдаланувчининг ҳақиқийлигини текшириш фойдаланувчи юборган парол P_A билан аутентификация серверида сақланувчи дастлабки қиймат P_A ни таққослашга асосланган. Агар P_A ва P_A қийматлар мос келса, парол P_A ҳақиқий, фойдаланувчи A эса қонуний хисобланади. Оддий аутентификацияни ташкил этиш схемалари нафақат паролларни узатиш, балки уларни сақлаш ва текшириш турлари билан ажралиб туради. Энг кенг тарқалган усул - фойдаланувчилар паролини тизимли файлларда, очиқ холда сақлаш усулидир. Бунда файлларга ўқиш ва ёзишдан ҳимоялаш атрибутлари ўрнатилади (масалан, операцион тизимдан

фойдаланишни назоратлаш рўйхатидаги мос имтиёзларни тавсифлаш ёрдамида). Тизим фойдаланувчи киритган паролни пароллар файлида сақланаётган ёзув билан солиштиради. Бу усулда шифрлаш ёки бир томонлама функциялар каби криптографик механизмлар ишлатилмайди. Ушбу усулнинг камчилиги - нияти бузуқ одамнинг тизимда маъмур имтиёзларидан, шу билан бирга тизим файлларидан, жумладан парол файлларидан фойдаланиш имкониятидир.[8,5]

Хавфсизлик нуқтаи назаридан паролларни бир томонлама функциялардан фойдаланиб узатиш ва сақлаш қулай хисобланади. Бу холда фойдаланувчи паролнинг очиқ шакли ўрнига унинг бир томонлама функция h(.) дан фойдаланиб олинган тасвирини юбориши шарт. Бу ўзгартириш ғаним томонидан паролни унинг тасвири орқали ошкор қила олмаганлигини кафолатлайди, чунки ғаним ечилмайдиган сонли масалага дуч келади. Кўп мартали паролларга асосланган оддий аутентификациялаш тизимининг бардошлиги паст, чунки уларда аутентификацияловчи ахборот маъноли сўзларнинг нисбатан катта бўлмаган тўпламидан жамланади.

Кўп мартали паролларнинг таъсир муддати ташкилотнинг хавфсизлиги сиёсатида белгиланиши ва бундай паролларни мунтазам равишда алмаштириб туриш лозим. Паролларни шундай танлаш лозимки, улар луғатда бўлмасин ва уларни топиш қийин бўлсин.[8]

Бир мартали паролларга асосланган аутентификациялашда фойдаланишга хар бир сўров учун турли пароллар ишлатилади. Бир мартали динамик парол фақат тизимдан бир марта фойдаланишга яроқли. Агар, хатто кимдир уни ушлаб қолса хам парол фойда бермайди. Одатда бир мартали паролларга асосланган аутентфикациялаш тизими масофадаги фойдаланувчиларни текширишда қўлланилади. Бир мартали паролларни генерациялаш аппарат ёки дастурий усул орқали амалга оширилиши мумкин. Бир мартали пароллар асосидаги фойдаланишнинг аппарат воситалари ташқаридан тўлов пластик карточкаларига ўхшаш микропроцессор ўрнатилган миниатюр қурилмалар кўринишда амалга оширади. Одатда калитлар деб аталувчи бундай карталар клавиатурага ва катта бўлмаган дисплей дарчасига эга.

Фойдаланувчиларни аутентификациялаш учун бир мартали паролларни қўллашнинг қуйидаги усуллари маълум:[9]

- ягона вақт тизимига асосланган вақт белгилари механизмидан фойдаланиш.
- легал фойдаланувчи ва текширувчи учун умумий бўлган тасодифий пароллар рўйхатидан ва уларнинг ишончли синхронлаш механизмидан фойдаланиш.
- фойдаланувчи ва текширувчи учун умумий бўлган бир хил дастлабки қийматли псевдотасодифий сонлар генераторидан фойдаланиш.

Биринчи усулни амалга ошириш мисоли сифатида SecurlD аутентикациялаш технологиясини кўрсатиш мумкин. Бу технология Security Dynamics компанияси томонидан ишлаб чиқилган бўлиб, қатор компанияларнинг, хусусан Cisco Systems компаниясининг серверларида амалга оширилган. Вақт синхронизациясидан фойдаланиб аутентификациялаш схемаси тасодифий сонларни вактнинг маълум оралиғидан сўнг генерациялаш алгоритмига асосланган.

Аутентификация схемаси қуйидаги иккита параметрдан фойдаланади .Хар бир фойдаланувчига аталган ва аутентификация серверида хамда фойдаланувчининг аппарат калитида сақланувчи ноёб 64-битли сондан иборат махфий калит жорий вақт қиймати.[9,5]

Масофадаги фойдаланувчи тармоқдан фойдаланишга уринганида ундан шахсий идентификация номери РЕЧни киритиш таклиф этилади. PIN тўртта ўнли рақамдан ва аппарат калити дисплейида аксланувчи тасодифий соннинг олтита рақамидан иборат. Сервер фойдаланувчи томонидан киритилган PIN-коддан фойдаланиб маълумотлар базасидаги фойдаланувчининг махфий калити ва жорий вақт қиймати асосида тасодифий сонни генерациялаш алгоритмини бажаради. Сўнгра сервер генерацияланган сон билан фойдаланувчи киритган сонни таққослайди. Агар бу сонлар мос келса, сервер фойдаланувчига тизимдан фойдаланишга рухсат беради. Аутентификациянинг бу схемасидан фойдаланишда аппарат калит ва сервернинг қатъий вақтий синхронланиши талаб этилади. Чунки аппарат калит бир неча йил ишлаши ва демак сервер ички соати билан аппарат ка-

литининг мувофиқлиги аста-секин бузилиши мумкин. Ушбу муаммони хал этишда Security Dynamics компанияси қуйидаги икки усулдан фойдаланади:

аппарат калити ишлаб чиқилаётганида унинг таймер частотасининг меъёридан четлашиши аниқ ўлчанади. Четлашишнинг бу қиймати сервер алгоритми параметри сифатида ҳисобга олинади; сервер муайян аппарат калит генерациялаган кодларни кузатади ва зарурият туғилганида ушбу калитга мослашади. Аутентификациянинг бу схемаси билан яна бир муаммо боглиқ. Аппарат калит генерациялаган тасодифий сон катта бўлмаган вақт оралиғи мобайнида ҳақиқий парол хисобланади. Шу сабабли, умуман, қисқа муддатли вазият содир бўлиши мумкинки, хакер PIN-кодни ушлаб қолиши ва уни тармоқдан фойдаланишга ишлатиши мумкин. Бу вақт синхронизациясига асосланган аутентификация схемасининг энг заиф жойи хисобланади. Бир мартали паролдан фойдаланувчи аутентификациялашни амалга оширувчи яна бир вариант - «сўров-жавоб» схемаси бўйича аутентификациялаш. Фойдаланувчи тармокдан фойдаланишга уринганида сервер унга тасодифий сон кўринишидаги сўровни узатади. Фойдаланувчининг аппарат калити бу тасодифий сонни масалан DES алгоритми ва фойдаланувчининг аппарат калити хотирасида ва серверниг маълумотлар базасида сақланувчи махфий калити ёрдамида расшифровка қилади. Тасодифий сон - сўров шифрланган кўринишда серверга қайтарилади. Сервер хам ўз навбатида ўша DES алгоритми ва серверниг маълумотлар базасидан олинган фойдаланувчининг махфий калити ёрдамида ўзи генерациялаган тасодифий сонни шифрлайди. Сўнгра сервер шифрлаш натижасини аппарат калитидан келган сон билан таққослайди. Бу сонлар мос келганида фойдаланувчи тармоқдан фойдаланишга рухсат олади. Таъкидлаш лозимки, «сўров-жавоб» аутентификациялаш схемаси ишлатишда вақт синхронизациясидан фойдаланувчи аутентификация схемасига қараганда мураккаброқ.[4,5]

Фойдаланувчини аутентификациялаш учун бир мартали паролдан фойдаланишнинг иккинчи усули фойдаланувчи ва текширувчи учун умумий бўлган тасодифий пароллар рўйхатидан ва уларнинг ишончли синхронлаш

механизмидан фойдаланишга асосланган. Бир мартали паролларнинг бўлинувчи рўйхати махфий пароллар кетма-кетлиги ёки тўплами бўлиб, хар бир парол фақат бир марта ишлатилади. Ушбу рўйхат аутентификацион алмашинув тарафлар ўртасида олдиндан тақсимланиши шарт. Ушбу усулнинг бир вариантига биноан сўров-жавоб жадвали ишлатилади. Бу жадвалда аутентификацилаш учун тарафлар томонидан ишлатилувчи сўровлар ва жавоблар мавжуд бўлиб, хар бир жуфт фақат бир марта ишлатилиши шарт. Фойдаланувчини аутентификациялаш учун бир мартали паролдан фойдаланишнинг учинчи усули фойдаланувчи ва текширувчи учун умумий бўлган бир хил дастлабки қийматли псевдотасодифий сонлар генераторидан фойдаланишга асосланган. Бу усулни амалга оширишнинг қуйидаги вариантлари мавжуд:*ўзгартирилувчи бир мартали пароллар кетма-кетлиги.* Навбатдаги аутентификациялаш сессиясида фойдаланувчи айнан шу сессия учун олдинги сессия паролидан олинган махфий калитда шифрланган паролни яратади ва узатади; [4,7]

бир томонлама функцияга асосланган пароллар кетма-кетлиги. Ушбу усулнинг мохиятини бир томонлама функциянинг кетма-кет ишлатилиши (Лампартнинг машхур схемаси) ташкил этади. Хавфсизлик нуқтаи назаридан бу усул кетма-кет узгартирилувчи пароллар усулига нисбатан афзал хисобланади. Кенг тарқалган бир мартали паролдан фойдаланишга асосланган аутентификациялаш протоколларидан бири.

Сертификатлар асосида аутентификациялаш

Тармоқдан фойдаланувчилар сони миллионлаб ўлчанганида фойдаланувчилар паролларининг тайинланиши ва сақланиши билан боглиқ фойдаланувчиларни дастлабки рўйхатга олиш муолажаси жуда катта ва амалга оширилиши қийин бўлади. Бундай шароитда рақамли сертификатлар асосидаги аутентификациялаш пароллар қўлланишига рационал альтернатива хисобланади. Рақамли сертификатлар ишлатилганида компьютер тармоғи фойдаланувчилари хусусидаги хеч қандай ахборотни сақламайди. Бундай ахборотни фойдаланувчиларнинг ўзи сўров-сертификатларида тақдим

этадилар. Бунда махфий ахборотни, хусусан махфий калитларни сақлаш вазифаси фойдаланувчиларнинг ўзига юкланади. Фойдаланувчи шахсини тасдиқловчи рақамли сертификатлар фойдаланувчилар сўрови бўйича махсус ваколатли ташкилот-сертификация маркази CA (Certificate Authority) томонидан, маълум шартлар бажарилганида берилади. Таъкидлаш лозимки, сертификат олиш муолажасининг ўзи хам фойдаланувчининг ҳақиқийлигини текшириш (яъни, аутентификациялаш) босқичини ўз ичига олади. Бунда текширувчи тараф сертификацияловчи ташкилот (сертификация маркази CA) бўлади. Сертификат олиш учун мижоз сертификация марказига шахсини тасдиқловчи маълумотни ва очиқ калитини тақдим этиши лозим. Зарурий маълумотлар рўйхати олинадиган сертификат турига боғлиқ Сертификацияловчи ташкилот фойдаланувчининг ҳақиқийлиги тасдиғини текширганидан сўнг ўзининг рақамли имзосини очиқ калит ва фойдаланувчи хусусидаги маълумот бўлган файлга жойлаштиради хамда ушбу очиқ калитнинг муайян шахсга тегишли эканлигини тасдиқлаган холда фойдаланувчига сертификат беради. Сертификат электрон шакл бўлиб, таркибида қуйидаги ахборот бўлади:[9,10]

-ушбу сертификат эгасининг очиқ калити;

-сертификат эгаси хусусидаги маълумот, масалан, исми, электрон почта адреси, ишлайдиган ташкилот номи ва х.к

-ушбу сертификатни берган ташкилот номи;

-сертификацияловчи ташкилотнинг электрон имзоси - ушбу ташкилотнинг махфий калити ёрдамида шифрланган сертификациядаги маълумотлар.

Сертификат фойдаланувчини тармоқ ресурсларига мурожаат этганида аутентификацияловчи восита хисобланади. Бунда текширувчи тараф вазифасини корпоратив тармоқнинг аутентификация сервери бажаради. Сертификатлар нафақат аутентификациялашда, балки фойдаланишнинг маълум ҳуқуқларини тақдим этишда ишлатилиши мумкин. Бунинг учун сертификатга қўшимча хошиялар киритилиб уларда сертификация эгасининг фойдаланувчиларнинг у ёки бу категориясига мансублиги кўрсатилади. Очиқ калитларнинг сертификатлар билан узвий боғлиқлигини алохида

таъқидлаш лозим. Сертификат нафақат шахсни, балки очиқ калит мансублигини тасдиқловчи ҳужжатдир. Рақамли сертификат очиқ калит ва унинг эгаси ўртасидаги мосликни ўрнатади ва кафолатлайди. Бу очиқ калитни алмаштириш хавфини бартараф этади. Агар абонент ахборот алмашинуви бўйича шеригидан сертификат таркибидаги очиқ калитни олса, у бу сертификатдаги сертификация марказининг рақамли имзосини ушбу сертификация марказининг очиқ калити ёрдамида текшириш ва очиқ калит адреси ва бошқа маълумотлари сертификатда кўрсатилган фойдаланувчига тегишли эканлигига ишонч хосил қилиши мумкин. Сертификатлардан фойдаланилганда фойдаланувчилар рўйхатини уларнинг пароллари билан корпорация серверларида сақлаш зарурияти йуқолади.[10]

Серверда сертификацияловчи ташкилотларнинг номлари ва очиқ калитларининг бўлиши етарли. Сертификатларнинг ишлатилиши сертификацияловчи ташкилотларнинг нисбатан камлигига ва уларнинг очиқ калитларидан қизиққан барча шахслар ва ташкилотлар фойдалана олиши (масалан, журналлардаги нашрлар ёрдамида) тахминига асосланган. Сертификатлар асосида аутентификациялаш жараёнини амалга оширишда сертификацияловчи ташкилот вазифасини ким бажариши хусусидаги масалани ечиш мухим хисобланади. Ходимларни сертификат билан таъминлаш масаласини корхонанинг ўзи ечиши жуда табиий хисобланади. Корхона ўзининг ходимларини яхши билади ва улар шахсини тасдиқлаш вазифасини ўзига олиши мумкин. Бу сертификат берилишидаги дастлабки аутентификациялаш муолажасини осонлаштиради. Корхоналар сертификатларни генерациялаш, бериш ва уларга хизмат кўрсатиш жараёнларини автоматлаштиришни таъминловчи мавжуд дастурий махсулотлардан фойдаланишлари мумкин. Масалан, Netscape Communications компанияси серверларини корхоналарга шахсий сертификатларини чиқариш учун таклиф этади.
Сертификацияловчи ташкилот вазифасини бажаришда тижорат асосида сертификат бериш бўйича мустақил марказлар хам жалб этилиши мумкин. Бундай хизматларни, хусусан, Verisign компаниясининг сертификацияловчи маркази таклиф этади. Бу компаниянинг сертификатлари халқаро

стандарт X.509 талабларига жавоб беради. Бу сертификатлар маълумотлар ҳимоясининг қатор махсулотларида, жумладан ҳимояланган канал SSL протоколида ишлатилади.[5,6]

Қатъий аутентификациялаш

Криптографик протоколларида амалга оширилувчи қатъий аутентификациялаш ғояси қуйидагича. Текширилувчи (исботловчи) тараф қандайдир сирни билишини намойиш этган холда текширувчига ўзининг ҳақиқий эканлигини исботлайди. Масалан, бу сир аутентификацион алмашиш тарафлари ўртасида олдиндан хавфсиз усул билан тақсимланган бўлиши мумкин. Сирни билишлик исботи криптографик усул ва воситалардан фойдаланилган холда сўров ва жавоб кетма-кетлиги ёрдамида амалга оширилади. Энг мухуми, исботловчи тараф фақат сирни билишлигини намойиш этади, сирни ўзи эса аутентификацион алмашиш мобайнида очилмайди. Бу текширувчи тарафнинг турли сўровларига исботловчи тарафнинг жавоблари ёрдами билан таъминланади. Бунда якуний сўров фақат фойдаланувчи сирига ва протокол бошланишида ихтиёрий танланган катта сондан иборат бошлангач сўровга боглиқ бўлади. Аксарият холларда қатъий аутентификациялашга биноан хар бир фойдаланувчи ўзининг махфий калитига эгалиги аломати бўйича аутентификацияланади. Бошқача айтганда фойдаланувчи унинг алоқа бўйича шеригининг тегишли махфий калитга эгалигини ва у бу калитни ахборот алмашинуви бўйича ҳақиқий шерик эканлигини исботлашга ишлата олиши мумкинлигини аниқлаш имкониятига эга.[7,8]

X.509 стандарти тавсияларига биноан қатъий аутентификациялашнинг қуйидаги муолажалари фарқланади:

бир томонлама аутентификация;
икки томонлама аутентификация;
уч томонлама аутентификация.

Бир томонлама аутентификациялаш бир томонга йуналтирилган ахборот алмашинувини кузда тутади. Аутентификациянинг бу тури қуйидагиларга имкон яратади:

-ахборот алмашинувчининг фақат бир тарафини ҳақиқийлигини тасдиқлаш;

-узатилаётган ахборот яхлитлигининг бузилишини аниқлаш;

-"узатишнинг такрори" типидаги ҳужумни аниқлаш;

-узатилаётган аутентификацион маълумотлардан фақат текширувчи тараф фойдаланишини кафолатлаш.

Икки томонлама аутентификацилаши бир томонлилигига нисбатан исботловчи тарафга текширувчи тарафнинг қўшимча жавоби бўлади. Бу жавоб текширувчи томонни алоқанинг айнан аутентификация маълумотлари мўлжалланган тараф билан ўрнатилаётганига ишонтириш лозим.

Уч томонлама аутентификациялаш таркибида исботловчи тарафдан текширувчи тарафга қўшимча маълумотлар узатиш мавжуд. Бундай ёндашиш аутентификация ўтказишда вақт белгиларидан фойдаланишдан воз кечишга имкон беради.

Таъкидлаш лозимки, ушбу туркумлаш шартлидир. Амалда ишлатилувчи усул ва воситалар тўплами аутентификация жараёнини амалга оширишдаги муайян шарт-шароитларга боғлик. Қатъий аутентификациянинг ўтказилиши ишлатиладиган криптографик алгоритмлар ва қатор қўшимча параметрларни тарафлар томонидан сўзсиз мувофиқлаштиришни талаб этади. Қатъий аутентификациялашнинг муайян вариантларини кўришдан олдин бир мартали параметрларнинг вазифалари ва имкониятларига тўхташ лозим. Бир мартали параметрлар баъзида "nonces" - бир мақсадга бир мартадан ортиқ ипшатилмайдиган катталик деб аталади. Хозирда ишлатиладиган бир мартали параметрлардан тасодифий сонлар, вақт белгилари ва кетма-кетликларнинг номерларини кўрсатиш мумкин. Бир мартали параметрлар узатишнинг такрорланишини, аутентификацион алмашинув тарафларини алмаштириб қўйишни ва очиқ матнни танлаш

билан хужум қилишни олдини олишга имкон беради. Бир мартали параметрлар ёрдамида узатиладиган хабарларнинг ноёблигини, бир маънолилигини ва вақтий кафолатларини таъминлаш мумкин. Бир мартали параметрларнинг турли хиллари алохида ишлатилиши, ёки бир-бирини тўлдириши мумкин.

Бир мартали параметрларнинг қуйидаги ишлатилиш мисолларини кўрсатиш мумкин:

-"сўров-жавоб" принципида қурилган протоколларда ўз вақтидалигини текшириш. Бундай текширишда тасодифий сонлар, соатларни синхронлаш билан вақт белгилари ёки муайян жуфт (текширувчи, исботловчи) учун кетма-кетликларнинг номерларидан фойдаланиш мумкин;

-ўз вақтидалигини ёки ноёблик кафолатини таъминлаш.

Протоколнинг бир мартали параметрларини бевосита (тасодифий сонни танлаш нули билан) ёки билвосита (бўлинувчи сирдаги ахборотни тахлиллаш ёрдамида) назоратлаш орқали амалга оширилади;

-хабарни ёки хабарлар кетма-кетлигини бир маъноли идентификациялаш. Бир охангда ўсувчи кетма-кетликнинг бир мартали қийматини (масалан, серия номерлари ёки вақт белгилари кетма-кетлиги) ёки мос узунликдаги тасодифий сонларни тузиш орқали амалга оширилади. Таъкидлаш лозимки, бир мартали параметрлар криптографик протоколларнинг бошқа вариантларида хам (масалан, калит ахборотини тақсимлаш протоколларида) кенг қўлланилади.[1,4]

Қатъий аутентификациялаш протоколларини қўлланиладиган криптографик алгоритмларига боғлиқ холда қуйидаги гурухдарга ажратиш мумкин:

-шифрлашнинг симметрик алгоритмлари асосидаги қатъий аутентификациялаш протоколлари;

-бир томонлама калитли хеш-функциялар асосидаги қатъий аутентификациялаш протоколлари;

-шифрлашнинг асимметрик алгоритмлари асосидаги қатъий аутентификациялаш алгоритмлари;

-электрон рақамли имзо асосидаги қатъий аутентификациялаш

алгоритмлари.

Маълумотлар манбаи аутентификацияси

Маълумотлар манбаи аутентификацияси (аввалари, маълумотлар аутентификацияси (message authentication) деб ҳам аталиб келинган) маълумотлар яхлитлиги билан узвий боғланган. Зеро, атайлаб ўзгартирилган ахборотни қабул қилиб олишдаги таваккалчилик (хавфи) ишончли бўлмаган манбадан ахборот қабул қилиш таваккалчилигига (хавфига) яқин. Аммо аслида маълумотлар манбаи аутентификацияси ва маълумотларни етишмаслигидан ҳимоялаш тушунчалари фарқли тушунчалардир. Чунки маълумотлар манбаи аутентификацияси албатта алоқа канали билан боғлиқ ҳолда қаралиб, манба идентификацияси (манбани унинг идентификатори (номи, символларнинг ноёб сатри) бўйича аниқлаш жараёни) ва маълумотларнинг янгилиги билан алоқадор бўлса, маълумотлар яхлитлигини ҳимоялашда айтилган белгилар асосий ҳисобланмайди.[4]

Маълумотлар манбаи аутентификацияси қуйидаги амалларни бажаришни назарда тутади.

1. Маълумот уни қабул этувчига шундай тарзда жўнатиладики, маълумотнинг ҳақиқийлигини уни қабул қилишдан аввал текшириб чиқишга имконият бўлсин.

2. Маълумот жўнатувчисини идентификациялаш.

3. Жўнатувчи юборган маълумотларнинг яхлитлигини текшириш.

4. Маълумот жўнатувчисининг кимлигини (реаллигини) текшириш.

Моҳият аутентификацияси

Моҳият аутентификацияси ахборот алмашув жараёни, яъни протоколи бўлиб, унинг давомида иштирокчи бошқа иштирокчининг ҳақиқийлигига (lively correspondence) амин бўлади.Аслида АП давомида маълумотнинг ҳақиқийлиги ёки ҳақиқий эмаслиги аён бўлади. Бундай ҳолларда маълумот ва

уни муаллифининг ҳақиқийлигига ишонч ҳосил қилиш учун маълумотлар манбаи аутентификацияси механизмларидан фойдаланиш лозим.Тармоқланган тизимларда қуйидаги моҳият аутентификацияси сценарийлари амал қилади. Улардан иккитасига тўхталамиз.

Иккита бош компьютерлараро (хост-хост типида, инглизчада - host-host type) маълумотлар алмашуви.[3,4]

Протокол иштирокчилари компьютерлар бўлиб, улар тармоқланган тизимнинг тугунлари ёки платформалари деб юритилади. Компьютерлар иши ўзаро мослашган бўлиши зарур. Масалан, агар узоқлашган платформалардан бири “қайта юкланмоқчи бўлса” (такрорий инициализацияланиш), у ҳақиқий серверни идентификация қилиши лозим ва унга керакли ахборотни жўнатиши лозим, масалан, операцион тизимнинг ҳақиқий нусхасини, таймерни ёки атроф-муҳитни тўғри ўрнатиш. Ахборот ҳақиқийлигини аниқлаш одатда АП ёрдамида амалга оширилади. Қоида тарзида, икки бош компьютерлараро маълумотлар алмашув клиент-сервер тизими сифатида бўлиб, бирига (клиент) иккинчиси (сервер) томонидан хизмат кўрсатилади.

Иштирокчи ва бош компьютерлараро (иштирокчи-хост типида, инглизчада - user-host type) маълумотлар алмашинуви. Иштирокчи бош компьютерда рўйхатдан ўтиб, компьютер тизимига киришга рухсат олади. Одатда мижоз бош компьютерда тармоққа узоқдан кириш (telnet) орқали рўйхатдан ўтади ёки ўз файлини файл узатиш протоколига (ftp-file transfer protocol) мувофиқ бош компьютерга жўнатади. Иккала ҳолда ҳам паролни аутентификациялаш протоколи ишга тушади. Айрим ҳолларда, масалан, кредит карточкалар бўйича тўловларда, ўзаро аутентификациялаш (mutual authentication) зарур бўлади. Субьект ўзининг ҳақиқийлигини тасдиқлаш учун тизимга турли маълумотларни тақдим этиши мумкин, масалан, пароль, шахсий идентификация коди, шахсий калит билан шифрланган хабар, смарткарта, биометрик белги, бармоқ изи, сўровга жавоб, рақамли сертификат, имзо ва шунга ўхшашлар.[5,4]

Протокол ёрдамидаги аутентификация

Аутентификациялашнинг кенг тарқалган схемаларидан бири оддий аутентификациялаш бўлиб, у анъанавий кўп мартали паролларни ишлатишга, яъни пароллар ва рақамли сертификатлардан фойдаланишга асосланган. Тармоқдаги иштирокчини оддий аутентификациялаш жараёнини қуйидагича тасаввур этиш мумкин. Тармоқдан фойдаланишга уринган иштирокчи компютер клавиатурасида ўзининг идентификатори ва паролини теради. Бу маълумотлар аутентификация серверига ишлаш учун тушади. Аутентификация серверида сақланаётган иштирокчи идентификатори бўйича маълумотлар базасидан мос ёзув топилади. Ундан паролни топиб иштирокчи киритган парол билан таққосланади. Агар улар мос келса, аутентификациялаш муваффақиятли бўлган ҳисобланади ва иштирокчи легал (қонуний) мақомини ва муаллифлашган тизими орқали унинг мақоми учун аниқланган ҳуқуқларни ва тармоқ ресурсларидан фойдаланишга рухсатни олади.[5]

Икки томонлама аутентификация

Ушбу юқорида номлари келтирилган усуллар қанчалик бардошли саналмасин, ушбу усуллар асосида ишлаб чиқилган тизим бардошлилиги фақат буларга боғлиқ бўлмайди. Одатда ушбу параметрлар ҳақиқий фойдаланувчи томонидан эмас, бузғунчи томонидан ҳам киритилиши мумкин. Ушбу ҳолатда ананавий аутентификациялаш усулида ўзига яраша муаммо келиб чиқади. Ушбу муамммони олдини олиш мақсадида ҳозирда кенг тарқалган *икки факторли аутентификациялаш* усулидан фойдаланилади. [6,5]

Ушбу усулда одатий аутентификациялаш усулидан ўтган фойдаланувчи юқоридаги усуллардан бири асосида иккинчи марта аутентификациядан ўтказилади. Ушбу усул парол асосида аутентификациялаш усулида иштирок этаётган ҳақиқий фойдаланувчи ёки

компьютер эканлигини аниқласа, хавфсизлик токенларига асосланган усулда эса токен эгаси ҳақиқийлигини текширади. Биометрик аутентификациялаш усулларида эса фойдаланувчини ҳақиқийлиги ва тириклигини текширишда фойдаланилади. Умумий ҳолда икки факторли аутентификациялаш усули оддий аутентификациялаш усулига қўшимча хавфсизлик параметрини қўшади. Икки факторли аутентификациялаш усули унда фойдаланилган қурилма турига қараб икки турга: уланган(connected) ва уланмаган (unconnected) бўлинади.Уланган қурилмаларга асосланган икки факторли аутентификациялаш усулида тўғридан-тўғри боғланган қурилма орқали маълумот қабул қилинади. Масалан, USB ёки Bluetooth асосида уланган қурилмалар.

Уланмаган қурилмаларга асосланган икки факторли аутентификациялаш усулида фойдаланувчи қурилма ва аутентификация тизими орасида жойлашади.[4]

Қуйида икки факторли аутентификациялаш усулари келтирилган:

-Бир мартали парол ҳосил қилиб берувчи қурилмаларга асосланган;

-Бир мартали парол ҳосил қилиб берувчи дастурий воситага асосланган;

-Терминал (компьютер, мобил телефон ва ҳ.к.) хусусиятига асосланган;

-TAN (Transaction Authentication Number) рўйхатига асосланган;

-SMS токенларга асосланган;

-Смарткарталар ва чип ўқувчи қурилмаларга асосланган;

-Махсус хотирага эга USB асосланган;

-Биометрик хусусиятларга асосланган ва ҳ.к.

Фойдаланувчиларни биометрик идентификациялаш ва аутентификациялаш

Охирги вақтда инсоннинг физиологик параметрлари ва характеристи-каларини, хулқининг хусусиятларини ўлчаш орқали фойдаланувчини

ишончли аутентификациялашга имкон берувчи биометрик аутентификация-лаш кенг тарқалмоқда.

Биометрик аутентификациялаш усуллари анъанавий усулларга нисбатан қуйидаги афзалликларга эга:

-биометрик аломатларнинг ноёблиги туфайли аутентификациялашнинг ишончлилик даражаси юқори;[5,6]

-биометрик аломатларнинг соғлом шахсдан ажратиб бўлмаслиги; биометрик аломатларни сохталаштиришнинг қийинлиги. Фойдаланувчини аутентификациялашда фаол ишлатиладиган биометрик алгоритмлар қуйидагилар:

-бармоқ излари;

-қўл панжасининг геометрик шакли;

-юзнинг шакли ва ўлчамлари;

-овоз хусусиятлари;

-кўз ёйи ва тўр пардасининг накхпи.

Аутентификациянинг биометрик қисм тизими ишлашининг намунавий схемаси қуйидагича. Тизимда рўйхатга олинишида фойдаланувчидан ўзининг ҳарактерли аломатларини бир ёки бир неча марта намойиш қилиниши талаб этилади. Бу аломатлар (ҳақиқий сифатида маълум) тизим томонидан қонуний фойдаланувчининг қиёфаси сифатида рўйхатга олинади. Фойдаланувчининг бу қиёфаси тизимда электрон шаклда сақланади ва ўзини қонуний фойдаланувчи деб даъво қилган хар бир одамни текширишда ишлатилади. Тақдим этилган аломатлар мажмуаси билан рўйхатга олинганларининг мослиги ёки мос келмаслигига қараб қарор қабул қилинади. Истеъмолчи нуқтаи назаридан биометрик аутенфикациялаш тизими қуйидаги иккита параметр орқали ҳарактерланади:[7,4]

-хатолик инкорлар коэффициенти FRR (false-reject rate);

-хатолик тасдиқлар коэффициенти FAR (false-alarm rate).

Хатолик инкор тизим қонуний фойдаланувчи шахсини тасдиқламаганда пайдо бўлади (одатда FRR қиймати тахминан 100 дан бирни ташкил этади). *Хатолик тасдиқ* тизим ноқонуний фойдаланувчи шахсини тасдиқлаганида пайдо бўлади (одатда FAP қиймати тахминан 10000 дан бирни ташкил этади). Бу иккала коэффициент бир бири билан боғлиқ: хатолик инкор коэффициентининг хар бирига маълум хатолик тасдиқ коэффициенти мос келади. Мукаммал биометрик тизимда иккала хатоликнинг иккала параметри нўлга тенг бўлиши шарт. Афсуски, биометрик тизим идеал эмас, шу сабабли ниманидур қурбон қилишга тўғри келади. Одатда тизимли параметрлар шундай созланадики, мос хатолик инкорлар коэффициентини аниқловчи хатолик тасдиқларнинг исталган коэффициентига эришилади.[7]

Биометрик аутентификациялашнинг дактилосконик тизими

Биометрик тизимларнинг аксарияти идентификациялаш параметри сифатида бармоқ изларидан фойдаланади (аутентификациянинг дактилоскопик тизими). Бундай тизимлар содда ва қулай, аутентификациялашнинг юқори ишончлилигига эга. Бундай тизимларнинг кенг тарқалишига асосий сабаб бармоқ излари бўйича катта маълумотлар баъзасининг мавжудлигидир. Бундай тизимлардан дунёда асосан полиция, турли давлат ва баъзи банк ташкилотлари фойдаланади.

Аутентификациянинг дактилоскопик тизими қуйидагича ишлайди. Аввал фойдаланувчи руйхатга олинади. Одатда, сканерда бармоқнинг турли холатларида сканерлашнинг бир неча варианти амалга оширилади. Табиий-ки, намуналар бир-биридан бироз фаркданади ва қандайдир умумлаштирил-ган намуна, «паспорт» шакллантирилиши талаб этилади. Натижалар аутен-тификациянинг маълумотлар базасида хотирланади. Аутентификациялашда сканерланган бармоқ изи маълумотлар базасидаги «паспортлар» билан таққосланади.[8,7]

Юзнинг тузилиши ва овоз бўйича аутентификацияловчи тизимлар.

Бу тизимлар арзонлиги туфайли энг фойдаланувчан хисобланадилар, чунки аксарият замонавий компьютерлар видео ва аудео воситаларига эга. Бу синф тизимлари телекоммуникация тармоқларида масофадаги фойдаланувчи субъектни идентификациялаш учун ишлатилади. *Юз тузилишини сканерлаш технологияси* бошқа биометрик технологиялар яроқсиз бўлган иловалар учун тўғри келади. Бу холда шахсни идентификациялаш ва верификациялаш учун кўз, бурун ва лаб хусусиятлари ишлатилади. Юз тузилишини аниқловчи қурилмаларни ишлаб чиқарувчилар фойдаланувчини идентификациялашда хусусий математик алгоритмлардан фойдаланадилар.

Маълум бўлишича, кўпгина ташкилотларнинг ходимлари юз тузилишини сканерловчи қурилмаларга ишонмайдилар. Уларнинг фикрича камера уларни расмга олади, сўнгра суратни монитор экранига чиқаради. Камеранинг сифати эса паст бўлиши мумкин. Ундан ташқари юз тузилишини сканерлаш - биометрик аутентификациялаш усуллари ичида ягона, текширишга рухсатни талаб қилмайдиган (яширинган камера ёрдамида амалга оширилиши мумкин) усул хисобланали.[4,5]

Таъкидлаш лозимки, юз тузилишини аниқлаш технологияси янада такомиллаштирилишни талаб этади. Юз тузилишини аниқловчи аксарият алгоритмлар қуёш ёруғлиги жадаллигининг кун бўйича тебраниши натижасидаги ёруғлик ўзгаришига таъсирчан бўладилар. Юз холатининг ўзгариши ҳам аниқлаш натижасига таъсир этади. Юз хрлатининг 45° га ўзгариши аниқлашни самарасиз бўлишига олиб келади.

Овоз буйича аутентификациялаш тизимлари

Бу тизимлар арзонлиги туфайли фойдаланувчан хисобланадилар. Хусусан уларни кўпгина шахсий компьютерлар стандарт комплектидаги

ускуна (масалан микрофонлар) билан бирга ўрнатиш мумкин. Овоз бўйича аутентификациялаш тизимлари хар бир одамга ноёб бўлган баландлиги, модуляцияси ва товуш частотаси каби овоз хусусиятларига асосланади. Овозни аниқлаш нутқни аниқлашдан фарқланади. Чунки нутқни аниқловчи технология абонент сўзини изохласа, овозни аниқлаш технологияси сўзловчининг шахсини тасдиқлайди. Сўзловчи шахсини тасдиқлаш баъзи чегараланишларга эга. Турли одамлар ўхшаш овозлар билан гапириши мумкин, хар қандай одамнинг овози вақт мобайнида кайфияти, хиссиётлик холати ва ёшига боғлиқ холда ўзгариши мумкин. Унинг устига телефон аппаратларнинг турли-туманлиги ва телефон орқали боғланишларининг сифати сўзловчи шахсини аниқлашни қийинлаштиради. Шу сабабли овоз бўйича аниқлашни юз тузилишини ёки бармоқ изларини аниқлаш каби бошқа биометриклар билан биргаликда амалга ошириш мақсадга мувофиқ хисобланади. *Куз ёйи тур пардасининг шакли бўйича аутентификациялаш тизими.* Бу тизимларни иккита синфга ажратиш мумкин: кўз ёйи расмидан фойдаланиш; кўз тўр пардаси қон томирлари расмидан фойдаланиш.[5,6]

Одам кўз пардаси аутентификация учун ноёб объект хисобланади. Кўз туби қон томирларининг расми хатто эгизакларда хам фарқланади. Идентификациялашнинг бу воситаларидан хавфсизликнинг юқори даражаси талаб этилганида (масалан харбий ва мудофаа объектларининг режимли зоналарида) фойдаланилади.

Биометрик ёндашиш "ким бу ким" эканлигини аниқлаш жараёнини соддалаштиришга имкон беради. Дактилоскопик сканерлар ва овозни аниқловчи қурилмалардан фойдаланиш ходимларни тармоққа киришларида мураккаб паролларни эслаб қолишдан халос этади. Қатор компаниялар корхона масштабидаги бир мартали аутентификация SSO (Single Sign-On) га биометрик имкониятларни интеграциялайдилар. Бундай бириктириш

тармоқ маъмурларига паролларни бир мартали аутентификациялаш хизматини биометрик технологиялар билан алмаштиришга имкон беради. Шахсни биометрик аутентификациялашнинг биринчилар қаторида кенг тарқалган соҳаларидан бири мобил тизимлари бўлди. Муаммо фақат компьютер ўғирланишидаги йўқотишларда эмас, балки ахборот тизимининг бузилиши катта зарарга олиб келиши мумкин. Ундан ташқари, ноутбуклар дастурий боғланиш (мобил компьютерларда сақланувчи пароллар ёрдамида) орқали корпоратив тармоқдан фойдаланишни тез-тез амалга оширади. Бу муаммоларни кичик, арзон ва катта энергия талаб этмайдиган бармоқ излари датчиклари ечишга имкон беради. Бу қурилмалар мос дастурий таъминот ёрдамида ахборотдан фойдаланишнинг мобил компьютерда сақланаётган тўртта сатхи - руйхатга олиш, экранни сақлаш режимидан чиқиш, юклаш ва файлларни дешифрациялаш учуй аутентификацияни бажаришга имкон беради. Фойдаланувчини биометрик аутентификациялаш махфий калитдан фойдаланишни модул куринишида шифрлашда жиддий ахамиятга эга бўлиши мумкин. Бу модул ахборотдан фақат ҳақиқий хусусий калит эгасининг фойдаланишига имкон беради. Сўнгра калит эгаси ўзининг махфий калитини ишлатиб хусусий тармоқлар ёки Internet орқали узатилаётган ахборотни шифрлаши мумкин.[7,6]

1.3.Аутентификациялашда электрон ракамли имзодан фойдаланиш

X.509 стандартининг тавсияларида рақамли имзо, вақт белгиси ва тасодифий сонлардан фойдаланиш асосидаги аутентификациялаш схемаси спецификацияланган. Ушбу схемани тавсифлаш учун куйидаги белгилашларни киритамиз:

- t_A, r_A ва $r_в$ — мос ҳолда вақт белгиси ва тасодифий сонлар;
- S_A - қатнашувчи A генерациялаган имзо;
- $cert_A$ — қатнашувчи A очиқ калитининг сертификати;
- $cert_B$ - қатнашувчи B очиқ калитининг сертификати;

Мисол тариқасида аутентификациялашнинг қуйидаги протоколларини келтирамиз:1. В акт белгисидан фойдаланиб бир томонлама аутентфикациялаш: $A\text{^}B{:}cert_A,t_A,B,S_A(f_A,B)$[4,5]

қатнашувчи *B* ушбу хабарни олганидан сўнг вақт белгиси t_A нинг туғрилигини, олинган идентификатор *B* ни ва сертификат $cert_A$ даги очиқ калитдан фойдаланиб рақамли имзо $S_A(t_A,B)$ нинг корректлигини текширади.

2. Тасодифий сонлардан фойдаланиб бир томонлама аутентификациялаш:

A <- B : $г_в$

$A\text{^}B{:}cert_A,r_A,B,S_A(r_A,r_B,B)$

Қатнашувчи *B* қатнашувчи *A* дан хабарни олиб айнан у хабарнинг адресати эканлигига ишонч хосил қилади; сертификат $cert_A$ дан олинган қатнашувчи *A* очиқ калитидан фойдаланиб очиқ куринишда олинган $г_A$ сони, биринчи хабарда жўнатилган $г_в$ сони ва ўзининг идентификатори *B* остидаги [6,5]имзо $S_A(r_A,r_B,B)$ нинг корректлигини текширади. Имзо чекилган тасодифий сон $г_A$ очиқ матнни танлаш билан хужумни олдини олиш учун ишлатилади.

3. Тасодифий сонлардан фойдаланиб икки томонлама аутентификациялаш:

A <- B : $г_в$

$A\text{^}B{:}cert_A,r_A,B,S_A(r_A,r_B,B)$

A<$г$- B: $cert_B, A, S_B(r_A, r_B, A)$

Ушбу протоколдаги хабарларни ишлаш олдинги протоколдагидек бажарилади.

1.4.Аутентификациялашда Хеш -функциялардан фойдаланиш

Хэшлаш функцияси (хэш-функцияси) шундай ўзгартиришки, кириш йулига узунлиги ўзгарувчан хабар М берилганида чиқиш йулида белгиланган узунликдаги қатор *h(M)* хосил булади. Бошқача айтганда, хеш-функция *h(.)* аргумент сифатида узунлиги ихтиёрий хабар (хужжат) М ни қабул қилади ва белгиланган узунликдаги хеш-қиймат (хеш) /7=/г(М)ни қайтаради (5.14-расм). ***Хэш-киймат h(M) хабар М нинг дайджести,*** яъни ихтиёрий узунликдаги асосий хабар М нинг хичлантирилган иккилик

ифодаси. Хэш-лаш функцияси ўлчами мегабайт ва ундан катта бўлган имзо чекилувчи ҳужжат М ни 128 ва ундан катта битга (хусусан, 128 ёки 256 бит) зичлаштиришга имкон беради. Таъкидлаш лозимки, хеш-функция *h(M)* қийматининг хужжат Мга богликдиги мураккаб ва ҳужжат Мнинг узини тиклашга имкон бермайди.[9,8]

Хэшлаш функцияси қуйидаги хусусиятларга эга бўлиши лозим:

1.Хэш-функция ихтиёрий ўлчамли аргументга қўлланиши мумкин.

2.Хэш-функция чиқиш йулининг қиймати белгиланган ўлчамга эга.

3.Хэш-функция *h(x)* ни ихтиёрий *"x"* учун етарлича осон хисобланади. Хэш-функцияни хисоблаш тезлиги шундай бўлиши керакки, хэш-функция ишлатилганида электрон рақамли имзони тузиш ва текшириш тезлиги хабарнинг ўзидан фойдаланилганига қараганда анчагина катта бўлсин.

4.Хэш-функция матн М даги орасига қуйишлар (вставки), чиқариб ташлашлар (выбросы), жойини ўзгартиришлар ва ҳ каби ўзгаришларга сезгир бўлиши лозим.

5.Хэш-функция қайтарилмаслик хусусиятига эга бўлиши лозим.

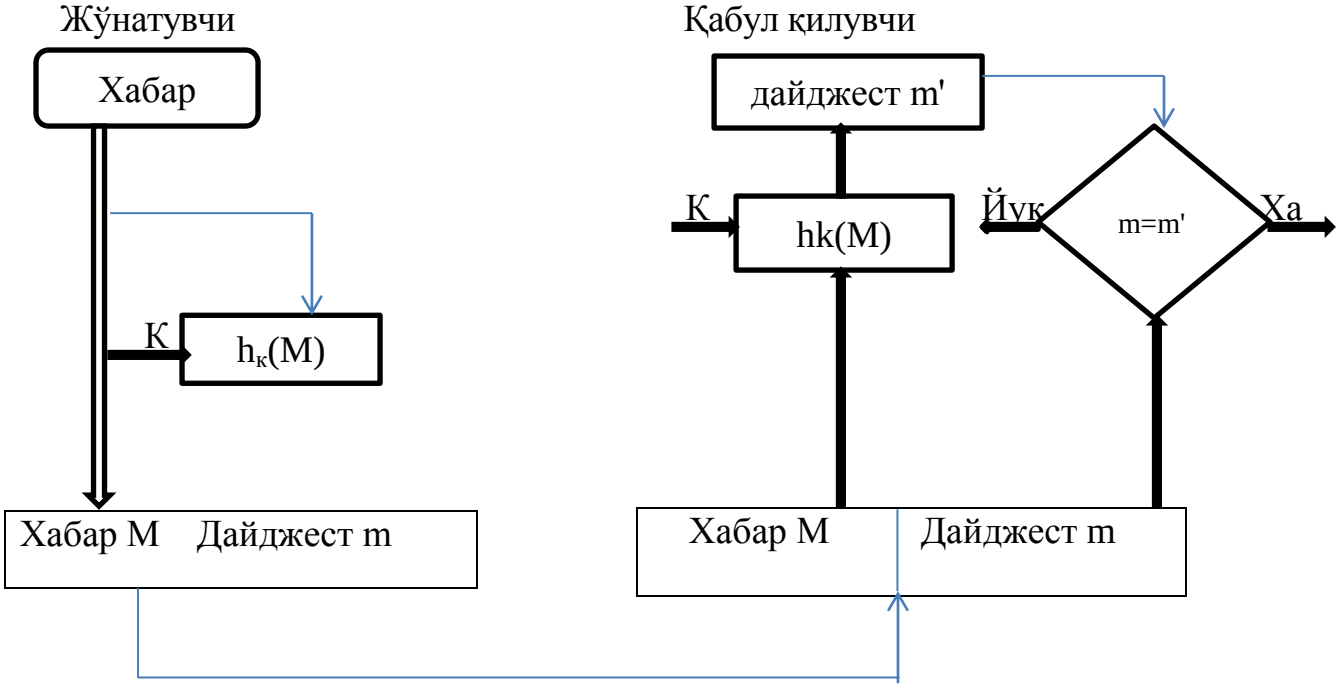
6. Иккита турли ҳужжатлар (уларнинг узунлигига боғлиқ бўлмаган холда) хэш-функциялари қийматларининг мос келиши эхтимоллиги жуда кичкина бўлиши шарт, яъни хисоблаш нуқтаи назаридан *h(x')=h(x)* бўладиган мумкин эмас. Иккита турли хабар бита тугунчага (свертка) зичлаштириш назарий жихатдан мумкин. Бу коллизия ёки тўқнашиш деб аталади. Шунинг учун хэшлаш функциясининг бардошлигини таъминлаш мақсадида тўқнашишларга йул қўймасликни кўзда тутиш лозим. Тўқнашишларга бутунлай йўл қўймаслик мумкин эмас, чунки умумий холда мумкин бўлган хабарлар сони хэшлаш функциялари чиқиш йуллари қийматларининг мумкин бўлган сонидан ортиқ. Аммо, тўқнашишлар эхтимоллиги паст бўлиши лозим.5-хусусият *h(.)* бир томонлама эканлигини билдирса, 6 хусусият бир хил тугунчани берувчи иккита ахборотни топиш мумкин эмаслигини кафолатлайди. Бу сохталаштиришни олдини олади. Шундай

қилиб, хэшлаш функциясидан хабар ўзгаришини пайқашда фойдаланиш мумкин, яъни у *криптографии назорат uuFunducunu* (ўзгаришларни пайқаш коди ёки *хабарни аутентификациялаш коди* деб хам юритилади) шакллантиришга хизмат қилиши мумкин. Бу сифатда хэш-функция хабарнинг яхлитлигини назоратлашда, электрон рақамли имзони шакллантаришда ва текширишда ишлатилади. Хэш-функция фойдаланувчини аутентифкациялашда хам кенг қўлланилади. Ахборот хавфсизлигининг қатор технологияларида шифрлашнинг ўзига хос усули *бир томонлама хеш-функция ёрдамида шифрлаш* ишлатилади. Бу шифрлашнинг ўзига хослиги шундан иборатки, у мохияти бўйича, бир томонламадир, яъни тескари муолажа қабул қилувчи томонда расшифровка қилиш билан бирга олиб борилмайди. Иккала тараф (жўнатувчи ва қабул қилувчи) хэш-функция асосидаги бир томонлама шифрлаш муолажасидан фойдаланади. Энг оммабоп хэш-функциялар MD2, MD4, MD5 ва SHA.MD2, MD4 ва MD5 Р.Райвест томонидан ишлаб чиқилган ахборот дайджестини хисобловчи алгоритм. Уларнинг хар бири 128 битли хэш-кодни тузади. MD2 алгоритми энг секин ишласа, MD4 алгоритми тезкор ишлайди. MD5 алгоритми MD4 алгоритмининг модификацияси бўлиб, MD4 алгоритмида хавфсизликнинг оширилиши эвазига тезликдан ютказилган. SHA(Secure Hash Algorithm) 160 битли *хэш-кодни* тузувчи ахборот дайджестини хисобловчи алгоритм. [3,4] Бу алгоритм MD4 ва MD5 алгоритмларига нисбатан ишончлироқ.

Бир томонлама калитли хэш-функциялардан фойдаланишга асосланган протоколлар

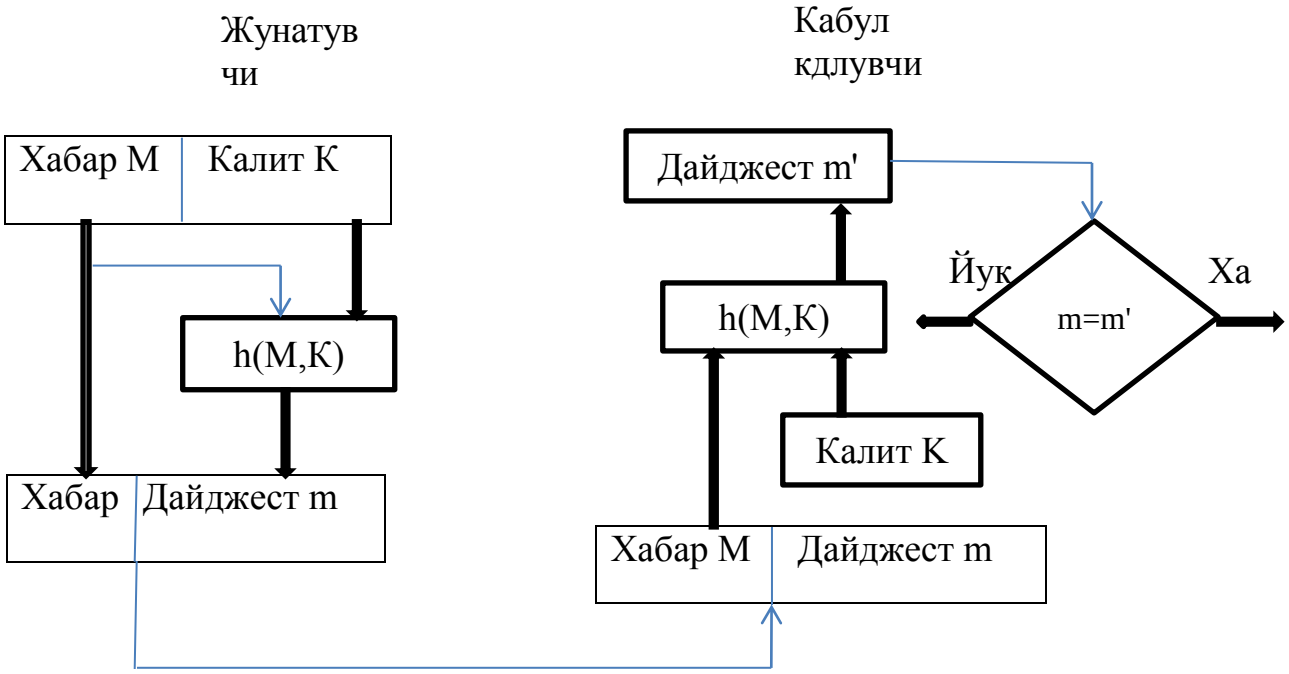
Бир томонлама хэш-функция ёрдамида шифрлашнинг ўзига хос хусусияти шундаки, у мохияти бўйича бир томонламадир, яъни тескари ўзгартириш-қабул қилувчи тарафда расшифровка қилиш билан бирга олиб борилмайди. Иккала тараф (жўнатувчи ва қабул қилувчи) бир томонлама шифрлаш муолажасидан фойдаланади. Шифрланаётган маълумот *M* га

қулланилган *K* параметр-калитли бир томонлама хэш-функция $h_k(.)$ натижада байтларнинг белгиланган катта бўлмагани сонидан иборат хэш-қиймат (дайджест) *"m"* ни беради.



Дайджест "т" қабул қилувчига дастлабки хабар *M* билан бирга узатилади. Хабарни қабул қилувчи, дайджест олинишида қандай бир томонлама хэш-функция ишлатилганлигини билган холда, расшифровка қилинган хабар *M* дан фойдаланиб, дайджестни бошқатдан хисоблайди. Агар олинган дайджест билан хисобланган дайджест мос келса, хабар *M* нинг таркиби хеч қандай ўзгаришга дучор бўлмаганини билдиради. Дайджестни билиш дастлабки хабарни тиклашга имкон бермайди, аммо маълумотлар яхлитлигини текширишга имкон беради. Дайджестга дастлабки хабар учун ўзига хос назорат йиғиндиси сифатида қараш мумкин. Аммо, дайджест ва оддий назорат йиғиндиси орасида жиддий фарқ хам мавжуд. Назорат йиғиндисидан алоқанинг ишончсиз линияси буйича узатиладиган [5,6]

Хабарларнинг яхлитлигини текшириш воситаси сифатида фойдаланилади. Текширишнинг бу воситаси нияти бузуқ одамлар билан кўрашишга мўлжалланмаган. Чунки, бу холда назорат йиғиндисининг янги қийматини қўшиб хабарни алмаштириб қуйишга уларга хеч ким ҳалақит бермайди. Қабул қилувчи бунда хеч нарсани сезмайди. Дайджестни хисоблашда, оддий назорат йигиндисидан фаркли равишда, махфий калитлар ишлатилади. Агар дайджест олинишида фақат жўнатувчи ва қабул қилувчига маълум бўлган параметр-калитли бир томонлама хэш-функция ишлатилса, дастлабки хабарнинг хар қандай модификацияси дархол маълум бўлади.



Бу холда бир томонлама хэш-функция *h(.)* параметр калитга эга эмас, аммо у махфий калит билан тўлдирилган хабарга қўлланилади,яъни жўнатувчи дайджест m=h(M, К)ни хисоблайди. Қабул қилувчи дастлабки хабарни чиқариб олиб, уни ўша маълум махфий калит билан тўлдиради.[5]Сўнгра олинган маълумотларга бир томонлама хэш-функция п(.)қўллайди. Хисоблаш натижаси дайджест "т" тармоқ орқали олинган дайджест "т" билан таққосланади. Хэш қиймат бошқа номлар билан: “хэш код”, “свертка”, “дайджест”, “бармоқ излари” деб ҳам аталади.

Хэш функцияга қуйидаги талаблар қўйилади:

1.Ихтиёрий узунликдаги матнга қўллаб бўлади.

2.Чиқишда тайинланган узунликдаги қийматни беради.

3.Ихтиёрий берилган x бўйича $h(x)$ осон ҳисобланади.

4.Ихтиёрий берилган H бўйича $h(x)= H$ тенгликдан x ни ҳисоблаб топиб бўлмайди. (Бир томонлилик хоссаси)

5.Олинган x ва $y \neq x$ матнлар учун $h(x) \neq h(y)$ бўлади. (Коллизияга бардошлилик хоссаси)[7]

Одатда мумкин бўлган маълумотларнинг сони мумкин бўлган хэш қийматлар сонидан кўп бўлади, шунинг учун ҳар бир хэш қийматга бир нечта матнлар тўплами, яъни бир хил хэш қийматли маълумотлар тўплами мос келади.Хэш функциялар иккита муҳим турга, *калитли* ва *калитсиз* хэш функцияларга ажратилади. Калитли хэш функциялар симметрик калитли тизимларда ишлатилади. Уларга маълумотни аутентификация қилиш кодлари (message authentication code (MAC))ҳам дейилади. Улар бир-бирига ишонувчи фойдаланувчилар тизимида қўшимча воситаларсиз манбанинг ҳақиқийлигини, маълумотнинг тўлалигини кафолатлайди.

Аутентификациялаш усули асосида ҳужжатларни қалбакилаштиришдан ҳимоялаш

2.1.Электрон рақамли имзодан фойдаланган холда ҳужжатни қалбакилаштиришдан ҳимоялаш

ЭРИ алгоритмлари-Қабул қилиб олинган маълумотларнинг ҳақиқий ёки ҳақиқий эмаслигини аниқлаш масаласини, яъни маълумотлар аутентификацияси масаласининг моҳияти ҳақида тўҳталамиз. Ҳар қандай ёзма хат ёки ҳужжатнинг охирида шу ҳужжатни тузувчиси ёки тузиш учун жавобгар бўлган шахснинг имзоси бўлиши табиий ҳолдир. Бундай ҳолат одатда қуйидаги иккита мақсаддан келиб чиқади. Биринчидан, маълумотни олган томон ўзида мавжуд имзо наъмунасига олинган маълумотдаги имзони солиштирган ҳолда шу маълумотнинг ҳақиқийлигига ишонч ҳосил қилади. Иккинчидан, шахсий имзо маълумот ҳужжатига юридик жиҳатдан муаллифликни кафолатлайди. Бундай кафолат эса савдо-сотиқ ишончнома, мажбурият ва шу каби битимларда алоҳида муҳимдир. Ҳужжатлардаги қўйилган шахсий имзоларни соҳталаштириш нисбатан мураккаб бўлиб, шахсий имзоларнинг муаллифларини ҳозирги замонавий илғор криминалистика услубларидан фойдаланиш орқали аниқлаш мумкин. Аммо электрон рақамли имзо хусусиятлари бундан фарқли бўлиб, иккилик саноқ системаси хусусиятлари билан белгиланадиган хотира регистрлари битларига боғлиқ. Хотира битларининг маълум бир кетмакетлигидан иборат бўлган электрон имзони кўчириб бирор жойга қўйиш ёки ўзгартириш компьютерлар асосидаги алоқа тизимларида мураккаблик туғдирмайди. Бугунги юқори даражада ривожланган бутун дунё цивилизациясида ҳужжатлар, жумладан маҳфий ҳужжатларнинг ҳам, электрон кўринишда ишлатилиши ва алоқа тизимларида узатилиши кенг қўлланилиб борилаётганлиги электрон ҳужжатлар ва электрон имзоларнинг ҳақиқийлигини аниқлаш масалаларининг муҳимлигини келтириб чиқармоқда. Очиқ калитли криптографик тизимлар қанчалик қулай ва криптобардошли бўлмасин, аутентификация масаласининг тўла ечилишига

жавоб бера олмайди. Шунинг учун аутентификация услуби ва воситалари криптографик алгоритмлар билан биргаликда комплекс ҳолда қўлланилиши талаб этилади. Қуйида иккита (А) ва (Б) фойдаланувчиларнинг алоқа муносабатларида аутентификация тизими рақиб томоннинг ўз мақсади йўлидаги қандай хатти-ҳаракатларидан ва криптотизим фойдаланувчиларининг фойдаланиш протоколини ўзаро бузилишлардан сақлаши кераклигини кўрсатувчи ҳолатлар кўриб чиқилади.[7,6]

Рад этиш (ренегатство)

Фойдаланувчи (А) фойдаланувчи (Б) га ҳақиқатан ҳам маълумот жўнатган бўлиб, узатилган маълумотни рад этиши мумкин.

Бундай қоида бузилишининг (тартибсизликнинг) олдини олиш мақсадида электрон (рақамли) имзодан фойдаланилади.

Модификациялаш (ўзгартириш)

Фойдаланувчи (Б) қабул қилиб олинган маълумотни ўзгартириб, шу ўзгартирилган маълумотни фойдаланувчи (А) юборди, деб таъкидлайди (даъво қилади).

Соҳталаштириш

Фойдаланувчи (Б)нинг ўзи маълумот тайёрлаб, бу соҳта маълумотни фойдаланувчи (А) юборди деб даъво қилади.

Фаол модификациялаш (ўзгартириш)

(А) ва (Б) фойдаланувчиларнинг ўзаро алоқа тармоғига учинчи бир (В) фойдаланувчи ноқонуний тарзда боғланиб, уларнинг ўзаро узатаётган маълумотларини ўзгартирган ҳолда деярли узлуксиз узатиб туради.

Ниқоблаш (имитациялаш)

Учинчи фодаланувчи (В) фойдаланувчи (Б)га фойдаланувчи (А) номидан маълумот жўнатади.

Юқорида санаб ўтилган: модификациялаш, сохталаштириш, фаол модификациялаш, ниқоблаш каби алоқа тизими қоидаларининг бузилишини олдини олиш мақсадида рақамли сигнатурадан рақамли имзо ва узатиладиган

маълумотнинг бирор қисмини тўла ўз ичига олувчи рақамли шифрматндан иборат бўлган маълумотдан фойдаланилади.[8,7]

Такрорлаш

Фойдаланувчи (В) фойдаланувчи (А) томонидан фойдаланувчи (Б)га жўнатилган маълумотни такроран (Б)га жўнатади. Бундай ноқонуний хатти–ҳаракат алоқа усулидан банклар тармоқларида электирон ҳисоб-китоб тизимидан фойдаланишда ноқонунийлик билан ўзгалар пулларини талон-тарож қилишда фойдаланилади. Ана шундай ноқонуний усуллардан муҳофазаланиш учун қуйидаги чора-тадбирлари кўрилади.

- имитациялашга бардошлилик – имитабардошлилик;

- криптотизимга кираётган маълумотларни муҳофаза мақсадларидан келиб чиқиб тартиблаш.

Электрон рақамли имзо алоқа тизимларида бир неча тур қоида бузилишларидан муҳофаза қилинишни таъминлайди, яъни:

- махфий калит фақат фойдаланувчи (А)нинг ўзигагина маълум бўлса, у ҳолда фойдаланувчи (Б) томонидан қабул қилиб олинган маълумотни фақат (А) томонидан жўнатилганлигини рад этиб бўлмайди;

- қонун бузар (рақиб томон) махфий калитни билмаган ҳолда мадификациялаш, сохталаштириш, фаол модификациялаш, ниқоблаш ва бошқа шу каби алоқа тизими қоидаларининг бузилишига имконият туғдирмайди; [5,4]

алоқа тизимидан фойдаланувчиларнинг ўзаро боғлиқ ҳолда иш юритиши муносабатидаги кўплаб келишмовчиликларни бартараф этади ва бундай келишмовчиликлар келиб чиққанда воситачисиз аниқлик киритиш имконияти туғилади.

Кўп ҳолларда узтилаётган маълумотларни шифрлашга ҳожат бўлмай, уни электрон рақамли имзо билан тасдиқлаш керак бўлади. Бундай ҳолатларда очиқ матн жўнатувчининг ёпиқ калити билан шифрланиб, олинган шифрматн очиқ матн билан бирга жўнатилади. Маълумотни қабул

қилиб олган томон жўнатувчининг очиқ калити ёрдамида шифрматнни дешифрлаб, очиқ матн билан солиштириши мумкин.

1991 йилда АҚШ даги Стандартлар ва Технологиялар Миллий Институти DSA (Digital Signature Algorithm) рақамли имзо алгоритмининг стандартини DSS (Digital Signature Standard) биз юқорида келтирган Эл-Гамал ва RSA алгоритмлари асосида яратиб, фойдаланувчиларга таклиф этган.[4,7]

Дастлаб таъкидланганидек, имзо хужжатнинг юридик мақомини кафолатлайди. Хозирги ривожланган жамиятда ахборот коммуникация тармоқларида электрон маълумот алмашинувининг кенгайиб бориши маълумотларнинг маҳфийлигини, ҳақиқийлигини ва муаллифликни ўрнатиш масалаларини ечишни талаб этади. Масалан, алмашилган электрон маълумотлар асосида у ёки бу ҳолатнинг ўзгариши, бу маълумотлар муаллифи манфатларига зид келиб, у электрон маълумот муаллифлигидан бош тортиши мумкин. Шундай ҳолатларнинг олдини олиш механизми маълумот муаллифини ўзигагина маълум бўлган бирор сонли параметр (махфий калит) билан боғлиқ ҳолда ҳосил қилинадиган сонлар кетма-кетлигида иборат бўлган электрон рақамли имзо (ЭРИ) ҳисобланади.

ЭРИ ахборот коммуникация тармоғида электрон ҳужжат алмашинуви жараёнида қуйидаги учта масалани ечиш имконини беради:

- электрон ҳужжат манбаининг ҳақиқийлигини аниқлаш;

- электрон ҳужжат яхлитлигини (ўзгармаганлигини) текшириш;

- электрон ҳужжатга рақамли имзо қўйган субъектни муаллифликдан бош тортмаслигини таъминлайди.

Ҳар қандай ЭРИ алгоритми иккита:

– имзо қўйиш;

– имзони текшириш;

қисмдан иборат бўлади. Имзо қўйиш муаллиф томонидан, фақат унга маълум бўлган махфий калит билан амалга оширилади. Имзонинг

ҳақиқийлигини текшириш эса исталган шахс томонидан, имзо муаллифининг очиқ калити билан амалга оширилиши мумкин.[9,6]

Электрон коммуникациялар ва электрон хужжат алмашинуви ҳозирги кунда иш юзасидан бўладиган муносабатларнинг ажралмас қисми ҳисобланиб, ҳар қандай замонавий ташкилотни электрон хужжатлар алмашинуви ва Интернетсиз тасаввур қилиш қийин. Интернет тармоғидан электрон хужжатлар алмашинуви асосида молиявий фаолият олиб боришда маълумотлар алмашинувини ҳимоя қилиш ва электрон хужжатнинг юридик мақомини таъминлаш биринчи даражали аҳамият касб этади. Электрон хужжатли маълумот алмашинуви жараёнида ЭРИни қўллаш ҳар хил турдаги тўлов тизимлари (пластик карточкалар), банк тизимлари ва савдо соҳаларининг молиявий фаолиятини бошқаришда электрон хужжат алмашинуви тизимларининг ривожланиб бориши билан кенг тарқала бошлади.

Ҳозирда ЭРИ тизимини яратишнинг бир нечта йўналишлари мавжуд. Бу йўналишларни учта гуруҳга бўлиш мумкин:

1) очиқ калитли шифрлаш алгоритмларига асосланган;

2) симметрик шифрлаш алгоритмларига асосланган;

3) имзони ҳисоблаш ва уни текширишнинг махсус алгоритмларига асосланган рақамли имзо тизимларидир.

Очиқ калитли шифрлаш алгоритмларига асосланган ЭРИ тизимлари қуйидагича ташкил қилинади. Агар ахборот коммуникация тармоғининг i- фойдаланувчиси j- фойдаланувчисига имзоланган электрон ҳужжат жўнатмоқчи бўлса, i- фойдаланувчи ўзининг маҳфий калити $k_i^м$ билан имзоланиши керак бўлган ҳужжатни ўзини шифрлаб ёки унинг хэш қийматини шифрлаб, шу ҳужжат билан биргаликда жўнатади. Бу электрон ҳужжатни қабул қилиб олган j- фойдаланувчи, шифрланган маълумотни i- фойдаланувчининг очиқ калити $k_i^о$ билан дешифрлаб, хосил бўлган матнни хужжат матнига ёки унинг хэш қийматига солиштиради. Агар матнлар билан

хэш қийматлар бир хил бўлса имзо ҳақиқий, акс ҳолда ҳақиқий эмас деб қабул қилинади.[7,9]

Симметрик шифрлаш алгоритмларига асосланган ЭРИ тизимлари қуйидагича ташкил этилади. i- фойдаланувчи бир вақтнинг ўзида i-фойдаланувчига ҳам j- фойдаланувчига ҳам маълум бўлиб, бошқа фойдаланувчиларга маълум бўлмаган $k_{ij}^{м}$ - калит билан имзоланиши керак бўлган электрон ҳужжатни ёки унинг хэш қийматини шифрлаб, шу хужжат билан биргаликда жўнатади. Электрон ҳужжатни қабул қилиб олган j-фойдаланувчи, шифрланган маълумотни $k_{ij}^{м}$- калит билан дешифрлаб, ҳосил бўлган матнни ҳужжат матнига ёки унинг хэш қийматига солиштиради. Агар матнлар билан хэш қийматлар бир хил бўлса имзо ҳақиқий, акс ҳолда ҳақиқий эмас деб қабул қилинади. Бундай ЭРИ тизими бир марталик ҳисобланади, чунки $k_{ij}^{м}$ - калитдан иккинчи марта фойдаланиш имконияти электрон хужжатларни қалбакилаштириш имкониятини яратади. Бундай ҳолатга чек қўйиш учун электрон ҳужжат алмашинуви ишончли учинчи томон орқали амалга оширилиши мумкин: i- фойдаланувчи ўзига ва фақат ишончли учинчи томонга маълум бўлган калит $k_{i3}^{м}$ билан рақамли имзони амалга ошириб, имзоланган электрон ҳужжатни учинчи ишончли томонга жўнатади, учинчи томон имзони хақиқийлигини $k_{i3}^{м}$ - калит билан текшириб, агар ҳақиқий бўлса, j- фойдаланувчининг ўзига ва фақат ишончли учинчи томонга маълум бўлган калит $k_{j3}^{м}$ билан рақамли имзони амалга ошириб, имзоланган электрон хужжатни j- фойдаланувчига жўнатади. Бундай ЭРИ тизими фойдаланувчилар учун ноқулай бўлиб, кўплаб келишмовчиликларни келтириб чиқаради.Амалда, учинчи турдаги имзони ҳисоблаш ва уни текширишнинг махсус алгоритмларига асосланган рақамли имзо тизимларидан кенг фойдаланилади.

Махсус ЭРИ алгоритмлари рақамли имзони ҳисоблаш ва имзони текшириш қисмларидан иборат. Рақамли имзони ҳисоблаш қисми имзо

қўйувчининг маҳфий калити ва имзоланиши керак бўлган ҳужжатнинг хэш қийматига боғлиқ бўлади. Имзони текшириш қисми имзо эгасининг очиқ калитига ва қабул қилиб олинган ҳужжатнинг хэш қийматига боғлиқ ҳолда амалга оширилади. [5,6]

Махсус ЭРИ стандартлари туркумига:

1. Россия ЭРИ стандарти: ГОСТ Р 34.10-94 ва унинг эллиптик эгри чизиқда такомиллаштирилган варианти ***ГОСТ Р 34.10-2001;***

2. ***Америка ЭРИ стандарти:*** ***DSA*** ва унинг эллиптик эгри чизиқда

такомиллаштирилган варианти ***ECDSA -2000;***

3. ***Ўзбекистон Республикаси стандарти: O'zDSt 1092:2005;***

алгоритмлари мисол бўла олади

Рақамли имзо битлар кетма-кетлигида ифодаланган бирор сондан иборат. Шунинг учун уни бошқа электрон хужжатларга кўчириш ёки ўзгартириш киритиш катта қийинчилик туғдирмайди. Шунинг учун электрон хужжат алмашинуви тизимида ЭРИ ни қалбакилаштиришнинг олдини олиш чора - тадбирлари ЭРИ алгоритмининг электрон хужжатларни қалбакилаштиришга бардошлилиги масаласини ечиш талаб этилади.

ЭРИ алгоритмининг бардошлилиги қуйдаги учта масаланинг мураккаблиги билан аниқланади:

- *имзони қалбакилаштириш*, берилган ҳужжатга, маҳфий калитга эга бўлмаган ҳолда тўғри имзо ҳисоблаш;

- *имзоланган маълумотни ташкил этиш*, маҳфий калитга эга бўлмаган ҳолда тўғри имзоланган маълумотни топиш;

- *маълумотни алмаштириш*, бир хил имзога эга бўлган иккита ҳар хил маълумотни топиш.[4,8]

Келтирилган ЭРИ алгоритмлари стандартлари бардошлиликлари дискрет логарифимлаш ва эллиптик эгри чизиқ рационал нуқталари устида амаллар бажариш масалаларининг мураккаблигига асосланган.Қуйида

ахборт-коммуникация тармоғининг маҳфий электрон хужжат алмашиш тизими асимметрик шифрлаш алгоритмидан иборат бўлганда ЭРИни очиқ калитли шифрлаш алгоритми асосида амалга ошириш мисол тариқасида кўриб ўтилади.Шудай қилиб, i - фойдаланувчи M - махфий маълумотни j - фойдаланувчига имзо қўйган ҳолда жўнатмоқчи бўлса, у ҳолда $\boldsymbol{i}$ - фойдаланувчи қуйдагиларни амалга ошириши керак:

1. Маълумот M тизим фойдаланувчиларининг барчасига маълум бўлган хэш-функция $h: X \to Y$ (бу ерда X - очиқ матнлар тўплами, Y - хэшлаш натижасида хосил бўлган қиймат) билан қайд қилинган бит узунлигидаги ифодага сиқилади;

2. Маълумотни хеш қиймати $h(M) = H$ фақат $\boldsymbol{i}$ - фойдаланувчининг ўзига маълум бўлган махфий калитга $k_i^м$ боғлиқ бўлган бир томонлама функция E, орқали шифрланади, яъни $E_{k_i^м}(h(M)) = S$.

3. Сўнгра, j - фойдаланувчининг очиқ калити $k_j^о$ билан маълумот M ва S бирлаштириланган кенгайтирилган маълумот шифрланади, яъни $E_{k_j^о}(M \cup S) = E_{k_j^о}(M) \cup E_{k_j^о}(S) = E_{k_j^о}(M) \cup E_{k_j^о}\left(E_{k_i^м}(h(M))\right) = C_1 \cup C_2 = C$;

4. Шифрланган маълумот C очиқ алоқа тармоғи орқали j - фойдаланувчига жўнатилади.

Шифрланган маълумотни олган j - фойдаланувчи, фақат унинг ўзига маълум бўлган махфий калит $k_j^м$ билан дешифрлашни амалга оширади, яъни

$$D_{k_j^з}(C) = D_{k_j^з}(C_1 \cup C_2) = D_{k_j^з}(C_1) \cup D_{k_j^з}(C_2) = D_{k_j^з}\left(E_{k_j^о}(M)\right) \cup D_{k_j^з}\left(E_{k_j^о}\left(E_{k_i^з}(h(M))\right)\right) =$$
$$= M \cup E_{k_i^з}(h(M)),$$

бу ерда ЭРИ ифодаси $E_{k_i^м}(h(M))$ хали дешифрланмаган.

5. Маълумот эгасини ва маълумотнинг ўзини ҳақиқийлигига ишоч хосил қилиш учун j -фойдаланувчи $\boldsymbol{i}$ -фойдаланувчининг очиқ калити $k_i^о$ билан ЭРИ қисмини $E_{k_i^м}(h(M))$ дешифрлаб $h(M)$-ифодани олади, яъни

$$D_{k_i^о}\left(E_{k_i^м}(h(M))\right) = h(M).$$

6. Сўнгра, j -фойдаланувчи дешифрлаш натижасида олган $D_{k_j^м}(C_1)$ очиқ маълумотни калитсиз хэш фунция билан хэшлайди $h\left(D_{k_j^э}(C_1)\right)$ ва ушбу $D_{k_i^о}\left(E_{k_i^м}(h(M))\right)=h(M)$ таққослаш билан имзонинг тўғрилигига ишонч ҳосил қилиши мумкин, агарда $h\left(D_{k_j^м}(C_1)\right)=D_{k_i^о}\left(E_{k_i^э}(h(M))\right)=h(M)$ бўлса, акс ҳолда имзо нотўғри, ҳамда, электрон ҳужжат ҳақиқий бўлмайди.[9,8]

ЭРИ имзонинг тўғрилиги маълумотни ўзини, унинг авторини ва манбасининг ҳақиқийлигини кафолатлайди.

Таъкидлаш жоизки, 1 - 6 - бандлар, асимметрик криптотизимларда маълумот алмашинувчи томонларнинг ЭРИ протоколини ифодалайди. Криптографик протокол деб, икки ва ундан ортиқ томонлар қатнашган ҳолда маҳфий маълумот алмашинуви жарёнида томонларнинг ўз вазифаларини бажариши кетма-кетлиги тушунилади.

RSA очиқ калитли шифрлаш алгоритми асосидаги ЭРИ

Тизимнинг ҳар бир i- фойдаланувчиси (e_i, d_i) - калитлар жуфтлигини яратади. Бунинг учун етарли катта бўлган p ва q - туб сонлари олиниб (бу сонлар маҳфий тутилади), $n=pq$- сони ва Эйлер функциясининг қиймати $\varphi(n)=(p-1)(q-1)$ ҳисобланади (бу сон ҳам махфий тутилади). Сўнгра, $(e_i, \varphi(n))=1$ шартни қаноатлантирувчи, яъни $\varphi(n)$ -сони билан ўзаро туб бўлган e_i -сон бўйича d_i-сони ушбу $e_i d_i = 1 \bmod \varphi(n)$ формула орқали ҳисобланади. Бу (e_i; d_i) –жуфтликда e_i - очиқ калит ва d_i- маҳфий калит деб эълон қилинади.

Шундан сўнг i- фойдаланувчидан j- фойдаланувчига шифрланган маълумотни имзолаган ҳолда жўнатиши қуйидагича амалга оширилади:

1. *Шифрлаш қоидаси:* $M^{e_j} \bmod n = C$, бу ерда M- очиқ маълумот, C – шифрланган маълумот;

2. *Дешифрлаш қоидаси:* $C^{d_j} \bmod n = M^{e_j d_j} \bmod n = M$;

3. *ЭРИ ни ҳисоблаш:* $H(M)^{d_i} \bmod n = P_i$,

бу ерда i - фойдаланувчининг P_i - имзоси M - маълумотнинг $H(M)$ - хеш функция қиймати бўйича ҳисобланган;[7,4]

4. *ЭРИ ни текшириш:* $(P_i)^{e_i} \bmod n = H(M)^{e_i d_i} \bmod n = H(M)$, агар $H(M) = H(M_1)$ бўлса (бу ерда M_1 -дешифрланган маълумот), у ҳолда электрон хужжат ҳақиқий, акс ҳолда ҳақиқий эмас, чунки хэш функция хоссасига кўра $M = M_1$ бўлса уларнинг хэш қийматлари ҳам тенг бўлади.

5. *Маълумотни махфий узатиш протоколи:*

$\left[M \cup H(M)^{d_i}\right]^{e_j} \bmod n = \left[M \cup P_i\right]^{e_j} \bmod n = C$;

6. *Махфий узатилган маълумотни қабул қилиш протоколи:*

$C^{d_j} \bmod n = \left[M \cup P_i\right]^{e_j d_j} \bmod n = M \cup P_i$, умуман қараганда дастлабки маълумот ўзгартирилган бўлиши мумкин, шунинг учун $C^{d_j} \bmod n = M_1 \cup P_i$ бўлиб, натижада, хеш қиймат имзо бўйича ушбу ифода $(P_i)^{e_i} \bmod n = H(M)^{e_i d_i} \bmod n = H(M)$ билан ҳисобланади ва қабул қилиб олинган маълумотнинг хеш қиймати $H(M_1)$ бўлса, у ҳолда $H(M) = H(M_1)$ бўлганда электрон ҳужжат ҳақиқий, аксинча бўлса қалбаки ҳисобланади.

Эл-Гамал очиқ калитли шифрлаш алгоритми асосидаги ЭРИ

Эл-Гамал очиқ калитли шифрлаш алгоритмига асосланган криптотизимнинг ҳар бир i - фойдаланувчиси учун очиқ ва маҳфий калитлар генерацияси қуйидагича амалга оширилади, очиқ эълон қлинадиган p_i - туб сон (ёки фойдаланувчилар гуруҳи учун умумий бўлган p - туб сон) танланади, ушбу $g_i < p_i$ (ёки фойдаланувчилар гуруҳи учун $g < p$) шартни қаноатлантирувчи g_i (ёки фойдаланувчилар гуруҳ учун g) сони танланади, ушбу $y_i = g^{x_i} \bmod p_i$ (p -умумий бўлганда $y_i = g^{x_i} \bmod p$, $x_i < p$) формула билан x_i - махфий калит бўйича y_i сони ҳисобланади. Шундай қилиб, (p_i, g_i, y_i)- параметрлар бирикмаси (умумий p ва g учун (p, g, y_i)- параметрлар бирикмаси очиқ калитни ташкил этади, маҳфий калит x_i ҳисобланади.

Тизимда i- фойдаланувчидан j- фойдаланувчига шифрланган маълумотнинг имзоланган ҳолда жўнатилиши қуйидагича амалга оширилади: [8,6]

1.*Шифрлаш қоидаси*: $a_j = g_j^k \bmod p_j$, $b_j = y_j^k M \bmod p_j$ (умумий p и g лар учун $a = g^k \bmod p$, $b_j = y_j^k M \bmod p$), бу ерда k-тасодифий сон бўлиб маълумотни имзоловчи томонидан танланади, бу сон $(p_j - 1)$ сони билан ўзаро туб ЭКУБ$(k, p_j - 1) = 1$ (p ва g умумий бўлганда ЭКУБ(k, $p-1$) =1), M -очиқ маълумот, шифрланган маълумот $(a_j, b_j) = C$ (p ва g умумий бўлганда, $(a, b_j) = C$).

2.*Дешифрлаш қоидаси:* $b_j \Big/ a_j^{x_j} \bmod p_j = M$ (p ва g умумий бўлганда $b \Big/ a^{x_j} \bmod p = M$), ҳақиқатан ҳам $b_j \Big/ a_j^{x_j} \bmod p_j \equiv g_j^{x_i k} M \Big/ g_j^{k x_i} \bmod p_j \equiv M$ (p ва g умумий бўлганда $b \Big/ a^{x_j} \bmod p \equiv y_j^k M \Big/ a^{x_j} \bmod p \equiv g^{x_j k} M \Big/ g^{k x_j} \bmod p = M \bmod p = M$, так как $M < p$);

3.*ЭРИ ни ҳисоблаш қоидаси:* $a_i = g_i{}^k \bmod p_i$, b_i сони эса $M = (x_i a_i + k b_i) \bmod (p_i - 1)$ ёки $H(M) = (x_i a_i + k b_i) \bmod (p_i - 1)$ тенгламадан топилади, яъни $b_i = (M - a_i x_i) k^{-1} \bmod (p_i - 1)$ ёки $b_i = (H(M) - a_i x_i) k^{-1} \bmod (p_i - 1)$ (p ва g умумий бўлганда $a = g^k \bmod p$, b сони эса $M = (x_i a + k b) \bmod (p - 1)$ ёки $H(M) = (xa + kb) \bmod (p - 1)$ тенгламадан топилади, яъни $b = (M - a x_i) k^{-1} \bmod (p - 1)$ ёки $b = (H(M) - a x_i) k^{-1} \bmod (p - 1)$, ЭКУБ$(k, p - 1) = 1$) $H(M)$-маълумотнинг хэш қиймати, x_i-махфий калит, имзо сифатида a_i ва b_i жуфтлик, яъни $(a_i, b_i) = P_i$, (p ва g умумий бўлганда (a, b)) имзо деб қабул қилинади.

4. *Имзони текшириш қоидаси:*

Агар $y_i^{a_i} a_i^{b_i} \bmod p_i = g_i^M \bmod p_i$ ёки $y_i^{a_i} a_i^{b_i} \bmod p_i = g_i^{H(M)} \bmod p_i$ бўлса, у ҳолда электрон хужжат ҳақиқий, акс ҳолда қалбаки ҳисобланади. Чунки,

$y_i = g_i^{x_i} \bmod p_i$ ва $a_i = g_i^{\,k} \bmod p_i$

тенгликлар ўринли бўлиб, Ферма теоремасига кўра ушбу айният ўринли:

5. *Маълумотни махфий узатиш протоколи:*

$a_j = g_j^k \bmod p_j$, $b_j = y_j^k M' \bmod p_j =, (a_j, b_j) = C$ -шиффрмаълумот;

Махфий узатилган маълумотни қабул қилиш протоколи:

$$b_j \Big/ a_j^{x_j} \bmod p_j = M' = M \cup P_i,$$

умуман қараганда, дастлабки маълумот ўзгартирилган бўлиши мумкин, шунинг учун

$$b_j \Big/ a_j^{x_j} \bmod p_j = M' = M_1 \cup P_i,$$

бўлиб, $H(M_1)$ хэш қиймат ҳисобланади. Агар $y_i^{a_i} a_i^{b_i} \bmod p_i = g_i^{M_1} \bmod p_i$ ёки $y_i^{a_i} a_i^{b_i} \bmod p_i = g_i^{H(M_1)} \bmod p_i$ бўлса, у ҳолда электрон хужжат ҳақиқий, акс ҳолда қалбаки ҳисобланади.

Энди имзони ҳисоблаш ва уни текширишга асосланган ЭРИ алгоритмлари DSA ва ГОСТ Р 34.10-94 стандарлари билан танишилади. Бу алгоритмларнинг асосини Эл-Гамал шифрлаш алгоритми ташкил этади.[6,7]

DSA ЭРИ стандарти

1991 йилда NIST (National Institute of Standard and Technology) томонидан DSA (Digital Signature Algorithm) алгоритмига асосланган DSS (Digital Signature Standard) ЭРИ стандартининг лойиҳаси муҳокамага қўйилди. Ушбу алгоритм бардошлилиги етарли катта туб характеристикага эга бўлган чекли майдонда дискрет логарифмлаш масаласининг мураккаблигига асосланган. Қуйида алгоритм қадамлари кетма-кетлиги келтирилган.

Имзони шакллантириш

1. Маълумот жўнатувчи M -маълумотни ва қуйидаги параметрларни кенг доирадаги тизим фойдаланувчиларига очиқ эълон қилади:

p – туб сон, $2^{512} < p < 2^{1024}$, бит узунлиги 64 га каррали;

q - туб сон, $2^{159} < q < 2^{160}$, $p-1$ нинг бўлувчиси;

$g = h^{(p-1)/q} \bmod p$, бу ерда h ушбу $0 < h < p$ ва $h^{(p-1)/q} \bmod p > 1$ шартларни қаноатлантирувчи бутун сон;

y – очиқ калит бўлиб, $y = q^x \bmod p$ формула орқали аниқланади. Бу ерда x – махфий калит бўлиб, $0<x<q$ ораликдан олинган ва фақат имозоловчининг ўзигагина маълум;[6,4]

$H(M)$ – M маълумотдан $[1;q]$ ораликдаги бутун сонни генерация қилувчи хеш-функция.

2. Маълумот жўнатувчи $0 < k < q$ ораликдан тасодифий k сонни танлайди, уни махфий тутади ва имзо генерациясидан кейин дарҳол йўқотади.

3. Маълумот жўнатувчи r ва s қийматларни қуйидаги қонуният орқали ҳисоблайди:

$r = g^k \bmod p \bmod q,$

$s = k^{-1}(xr + H(M)) \bmod q.$

M - маълумотга қўйилган имзо (r, s) сонлар жуфтлигидан иборат.

Имзони текшириш. Қабул қилувчи M' маълумотни ва (r', s') имзони қабул қилиб олади. У M ва M' маълумотларнинг мос келишини текшириши лозим. Бунинг учун у қуйидаги қадамлар кетма-кетлигини бажаради:

1. $0 < s' < q$ ёки $0 < r' < q$ шартлардан бирортаси бажарилмаса, имзо қалбаки деб ҳисобланади ва имзони текшириш тугатилади.
2. $v = (s')^{-1} (\bmod q)$ топилади.
3. $z_1 = H(M') v \bmod q$, $z_2 = r' v \bmod q$ ҳисобланади.
4. Кейин $u = g^{z_1} y^{z_2} \bmod p \bmod q$ ҳисобланади.

5. Агар $r' = u$ тенглик ўринли бўлса, у ҳолда имзо ҳақиқий ва $M = M'$ тенглик тўғри.

Алгоритмнинг тўғрилиги. $M = M'$, $s' = s$ ва $r' = r$ бўлсин. У ҳолда $r = u$ тенглик ўринли бўлиши кўрсатилади.

Демак, $v = (s')^{-1} \bmod q$, $z_1 = H(M')\, v \bmod q$, $z_2 = r'\, v \bmod q$ эканлигидан, қуйидагини ёзиш мумкин:

$$u = g^{z1}\, y^{z1} \bmod p \bmod q = g^{H(M)s-1}\, g^{xrs-1} \bmod p \bmod q =$$

$$= g^{k(xr+H(M))-1(xr+H(M))} \bmod p \bmod q = g^{k} \bmod p \bmod q = r.$$

Бундан кўриш мумкинки, $r = u$ тенглик ўринли. Шундай қилиб, алгоритм тўғрилиги исботланди.[8,7]

ГОСТ Р 34.10-94 электрон рақамли имзоси

Ушбу параграфда 2000 йилгача Россия стандарти ҳисобланган ГОСТ Р 34.10–94 ЭРИ алгоритми қараб чиқилади. Бу алгоритм DSA алгоритмига ўхшаш ва қуйидаги бошланғич очиқ параметрлардан фойдаланади:

1) Узунлиги L бўлган катта p туб сон танланади, бу ерда L сон 509 битдан 512 битгача ёки 1020 битдан 1024 битгача оралиқдан танланади, яъни $2^{509} < p < 2^{512}$ ёки $2^{1020} < p < 2^{1024}$.

2) Узунлиги L_1 бўлган катта q туб сон танланади, бу ерда L_1 сон 254 битдан 256 битгача оралиқдан танланади, яъни $2^{254} < p < 2^{256}$.

3) $g^q \bmod p = 1$ шартни қаноатлантирувчи $0 < g < p-1$ оралиқдаги g сон танланади.

4) $y = g^x \bmod p$ дан y- очиқ калит ҳисобланади, бу ерда $0 < x < q$ оралиқдан олинган x -махфий калит.

5) $H(M)$ - хэш-функция берилган M - маълумот бўйича ҳисобланган бутун сон бўлиб, *1* дан q гача оралиқдаги қийматларни қабул қилади, яъни $1 < H(M) < q$.

Имзони генерация қилиш алгоритми. Бошланғич маълумотлар: M - маълумот, берилган параметрлар ва махфий калит. Натижа: имзо - (r,s).

1) $1 \le k \le q$ интервалдан тасодифий k сони олинади, у махфий сақланади ва имзо қўйилгандан кейин дарҳол йўқотилади.

2) $r = (g^k \bmod p)(\bmod q)$ ҳисобланади.[4,5]

3) Жўнатилаётган M - маълумотнинг $e := H(M)$ - хэш қиймати ҳисобланади.

4) Агар $r = 0$ ёки $H(M) \bmod q = 0$ бўлса, у ҳолда 1- қадамга ўтилиб, бошқа k танланади.

5) $s = (xr + kH(M)) \bmod q$ ҳисобланади, бу ерда махфий калит x фақат имзо қўювчининг ўзигагина маълум.

6) Агар $s = 0$ бўлса, у ҳолда 1-қадамга борилади.

7) M маълумот имзоси - (r,s) жуфтлигидан иборат.

Имзони текшириш алгоритми. Бошланғич маълумотлар: M маълумот, берилган параметрлар, имзони текшириш калити ва M маълумот имзоси. Натижа: имзо ҳақиқийлиги ёки қалбакилиги ҳақидаги тасдиқ.

1) Агар $1 \le r, s \le n-1$ шарт бажарилмаса, у ҳолда имзо қалбаки ва имзони текшириш алгоритми тугатилади. Бу шартлар бажарилса кейинги қадамга ўтилади.

2) $e := h(m)$ ҳисобланади.

3) $w := H(M)^{(q-2)} \bmod q$ ҳисобланади.

4) $u_1 := sw \bmod q$ ҳисобланади.

5) $u_2 := (q-r)w \bmod q$ ҳисобланади.

6) $u := (g^{u_1} y^{u_2} \bmod p)(\bmod q)$ ҳисобланади.

7) Агар $u = r$ шарт бажарилса, у ҳолда имзо ҳақиқий, акс ҳолда имзо қалбаки ва имзони текшириш алгоритми тугатилади.[6,7]

ГОСТ Р 34.10-94 имзо алгоритмининг тўғрилиги

ГОСТ Р 34.10-94 электрон рақамли имзо генерацияси алгоритмидан олинган r параметрнинг қцийматини имзони текшириш алгоритмидаги u параметр қиймати билан тенглигини кўрсатишимиз керак.

Ҳақиқатан, $u = (g^{u_1} y^{u_2} \bmod p)(\bmod q) = g^{sw \bmod q} \cdot g^{x(q-r)w \bmod q} \bmod p \bmod q$

$= g^{(s+xq-xr)w \bmod q} \bmod p \bmod q = g^{(xr+kH(M)+xq-xr)w \bmod q} \bmod p \bmod q =$

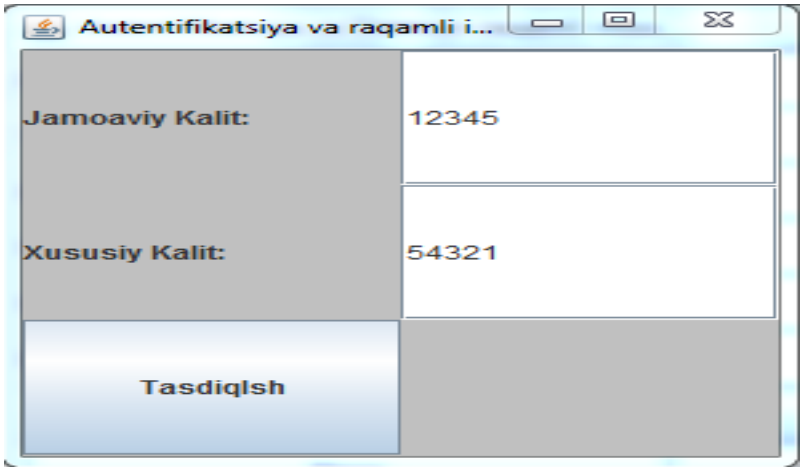
$= g^{(kH(M)+xq)w \bmod q} \bmod p \bmod q =$

$= g^{kH(M)w \bmod q} \bmod p \cdot (g^q \bmod p)^{xw \bmod q} (\bmod q) =$

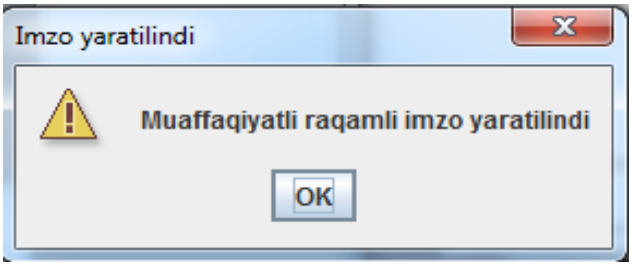
$= / (g^q \bmod p)=1$ шартга кўра, $(g^q \bmod p)^{xw \bmod q} (\bmod q)=1$ тенглик ўринли/$= g^{kH(M)w \bmod q} \bmod p (\bmod q) = / w=H(M)^{(q-2)} \bmod q$, $0<H(M)<q$ (q –туб) шартга ва Эйлера – Ферма теоремасига кўра $H(M)^{(q-2)} \bmod q= H(M)^{-1}$ эканлиги келиб чиқади, шунга кўра g нинг даражасини $kH(M)w=kH(M)H(M)^{q-2} \bmod q= kH(M)H(M)^{-1}=k$ каби ифодалаш мумкин $/ = g^k \bmod p (\bmod q) = r$. Шундай қилиб талаб қилинган шарт кўрсатилди. [5,8]Электрон рақамли имзони қўллашдан мақсад, биринчидан электрон ҳужжатдаги ахборот асл нусха эканлигини тасдиқлаш, иккинчидан учинчи тарафга (арбитр, судга ва бошқаларга) ҳужжатни муаллифи ушбу шахс эканлигини исботлаш. Ушбу мақсадга эришиш учун муаллиф ўзининг махфий индивидуал рақами (индивидуал калит,пароль) билан ҳужжатга ўрнатилган тартибда «электрон имзо қўйиш» жараёнини бажариши лозим. Бундай имзо қўйишда, ҳар гал индивидуал калит электрон ҳужжатдаги маълумотлар билан маълум қоидага мувофиқ аралашиб кетади. Электрон имзо ғояси биринчи марта Диффи ва Хеллман асарида ҳужжатнинг асл нусха эканлигини ва муаллиф томонидан имзоланганлигини аниқлаш учун таклиф этилган. Ҳозирги пайтда рақамли имзо кенг қўлланилмоқда (узатиладиган ёки сақланадиган шифрланган матнга бириктирилган рақам, бу ахборотнинг бутунлигини ва муаллифни ҳақиқийлигини текшириш имкониятини кафолатлайди). Симметрик шифрлаш алгоритмларига асосланган рақамли имзо моделлари ҳам мавжуд.

2.2.Ҳужжатни қалбакилаштиришдан ҳимоялаш дастурий модулини ишлаб чиқиш

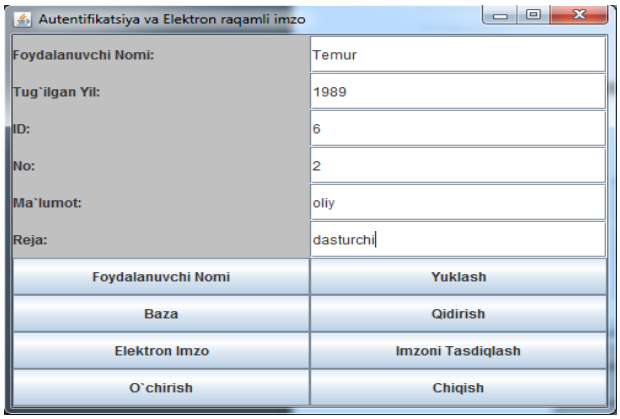
Биринчи навбатда электрон рақамли имзони яратиб оламиз ва шундан сўнг қуйидаги ойна хосил бўлади ва бу ерга бирон та бир калит сўз киритамиз



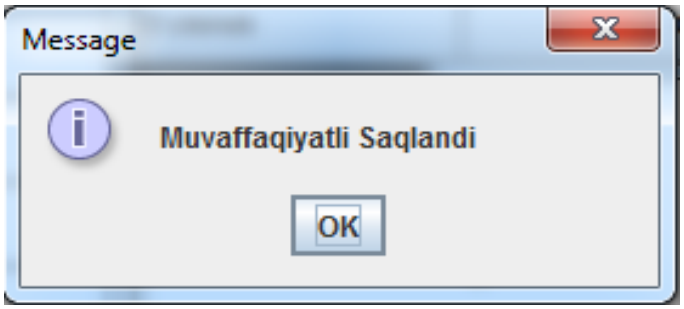
Ва шундан сўнг тасдиқлаш тугмасини босамиз ва бу ерда рақамли имзо яратилинди ва шундан сўнг ок тугмасини босамиз



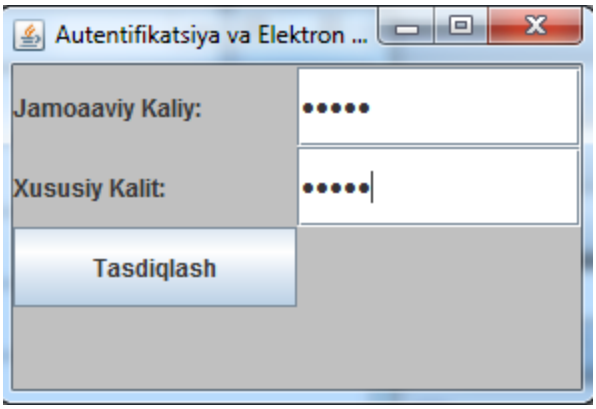
Рақамли имзо яратилиб бўлингандан сўнг фойдаланувчи аутентификация жараёнидан ўтади



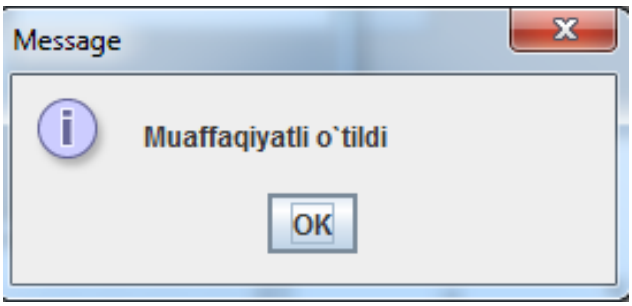
Ва шундан сўнг фойдаланувчи тугмасини босамиз ва муваффақиятли сақланди деб жавоб келади ва шундан сўнг ок тугмаси босилади



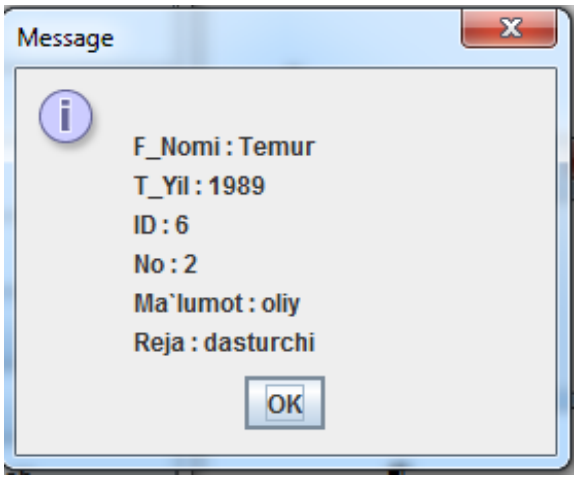
Ва бу ерда қуйидаги ойна хосил бўлади ундан сўнг жамоавий ва хусусий калит чиқади бу ерда иккаласига хам сўз ёзиб чиқамиз



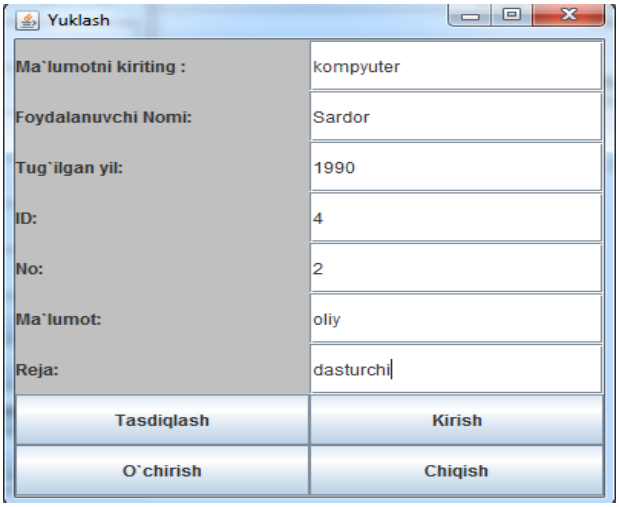
Шундан сўнг тасдиқлаш тугмасини босамиз ва муаффакийатли ўтилди деган жавоб келади ва ок тугмаси босилади



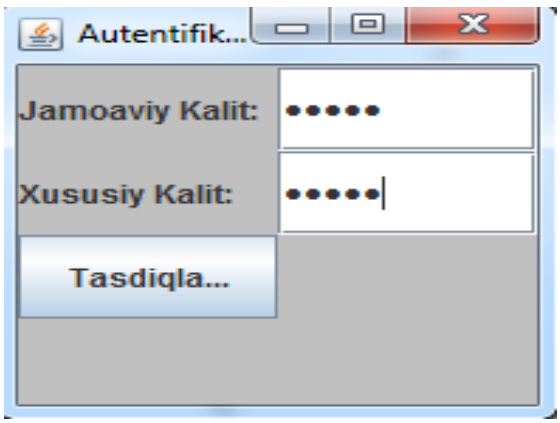
Ва хар бир одам регистратциядан ўтгандан сўнг хар бирини базага сақлаб қолади



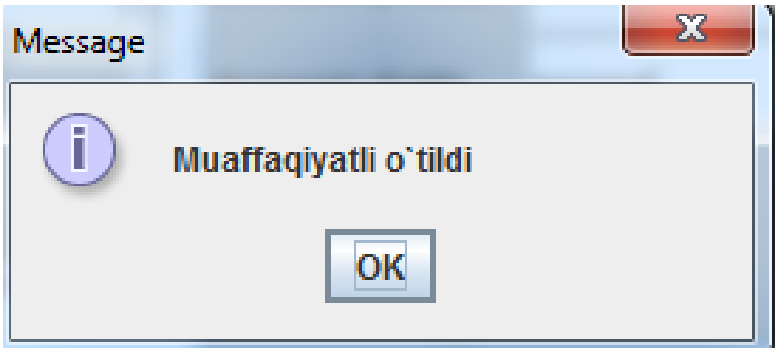
Яна кимдир киркоқчи бўлса яна ушандай регистратсиядан ўтади



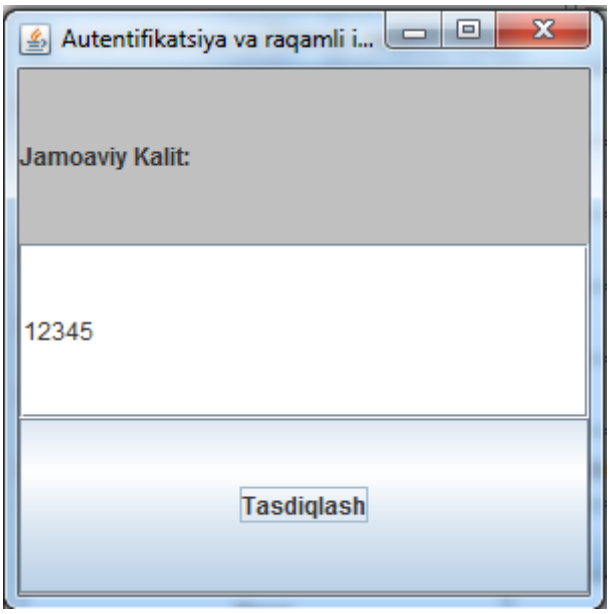
Ва шундан сўнг кириш тугмасини босамиз бизарга қуйидаги ойна хосил бўлади ва жамоавий калит ва хусусий калитни киритади



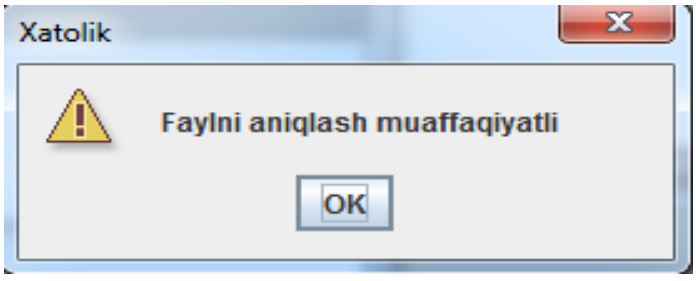
Ва шундан сунг бу хам муаффакиятли ўтилди деган жавоб келади



Бу имзо туғрилигини текшириш учун жамоавий калит киритилади



Шундан сўнг тасдиқлаш тугмасини босамиз ва бу имзонинг туғрилигини кўрсатади



3БОБ.Ҳаёт фаолияти хавфсизлиги

3.1.Ишлаб чиқаришда ходимлар саломатлигига зарар етиши ва иш берувчи масулияти

Хўжалик юритишнинг бозор шароитларига ўтиш корхоналар фаолияти амалиётида катта ўзгаришларни юзага келтирди.

Кўпчилик корхоналарда бошқарув структураси қатор мутахассислар лавозимлари, шу жумладан Меҳнат мухофазаси бўйича мутахассисликларнинг қисқартириш томонга ўзгарди, давлат органлари ва назорат касаба уюшмалари, идоралар томонидан хавфсиз иш шароитларига риояэтиш устидан назорат савияси сустлашди.

Натижада сўнгги йилларда ишлаб чиқариш травматизми мухим даражада ўсди. Шундан келиб чиқиб, жабрланганлар ва уларнинг оилалари учун бўлгани каби иш берувчи учун хам мухим ахамият касб этиб, хуқуқий базага эга саналади.

Ўзбекистонда хар бир ходим иши билан боғлиқ тарзда саломатлигига етказиладиган зарарни қоплаш хуқуқига эга.

Иш берувчи вақтида ва тўғри ишлаб чиқаришда бахтсиз ходисаларни терговини ўтқазиш ва хисобини олиш, шунингдек ходимларга етказилган зарар учун моддий жавобгарликни зиммасига олиши шарт.

Хар қандай шикаст етказувчи воқеа бахтсиз воқеа саналади.

1. Механик (санчилган, кесилган,лат еган ва х.к.).
2. Термик (куйиш, музлаш, совқотиб қолиш, иссиқлик зарбаси ва х.к.).
3. Электрик.
4. Кимёвий.
5. Психик ва бошқа.

Уларнинг оқибатида инсон қисқа муддатга ёки узоқ даврга меҳнатга лаёқатини юқотади.[10]

Бахтсиз ходиса деб касбий касалликлар, касбий захарланишлар ва айрим холатларда умумий касалликлар тушунилади.

Тиббий муассаса хулосаси меҳнат мажбуриятлари билан боғлиқ саломатликка путур етишлар сонига умумий касаллик учун зарур шарт хисобланади. Саломаликка путур етказадиган бахтсиз ходисалар ишлаб чиқариш ходисалари ёки маиший хисобланади.

Иш берувчи фақат ишлаб чиқариш бахтсиз ходисалари учун жавобгардир.

Ишлаб чиқариш билан боғлиқ бахтсиз ходисалар қуйидагилардан иборат:

-улар томонидан меҳнат вазифалари (шу жумладан хизмат сафарлари хам) ни бажариш, шунингдек иш берувчи топшириғисиз хам корхона манфаатлари доирасида бирор бир халокатларни амалга ошираётганда;

-корхона транспортида ишга йўл олаётганда ёки ишдан қайтаётганда;

-белгиланган танаффуслардан тортиб бутун иш вақти мобайнида корхона худуди ёки бошқа иш жойида;

-ўтқазилиш жойидан қатъий назар шанбалик ўтқазилаётган вақтда;

-ишлаб чиқаришда юз берган авариялярда;

-иш вақтида хизмат объектлари ўртасидаги харакат билан фаолияти боғлиқ ходим билан жамоат транспортида ёки пиёда, шунингдек иш берувчининг топшириғига кўра, иш жойига кетаётганида;

-иш вақтида хизмат сафарлари ёки иш берувчининг топшириғига кўра, шахсий енгил транспортда;[11]

-иш вақтида бошқа шахс томонидан танага шикаст етказиш, ёки меҳнат вазифасини бажараётганида ходимнинг қасддан ўлдирилиши.

Фақат ўз ўлими, табиий жон бериў ходисалари, шунингдек, жиноятлар қилаётганда ўша жабрланувчилар томонидан жарохатлар инобатга олинмайди. Иш берувчининг жавобгарлиги қандай вазиятларда бахтсиз ходиса рўй бергани ва етказилган зарарга боғлиқ.

1. Агар зарар юқори хавфсизлик манбаи томонидан етказилган бўлса, иш берувчи воқеа табиий офат оқибатида, ёки жарбланувчи ғарази ёки унинг қўпол эхтиёткорсизлиги туфайли, бўлганини исботлай олмаса,у етказилган зарарни тўлиқ миқдорда қоплаши керак.

Масалан, металл қирқувчи ускунада ишчи қўлига шикаст етди. Иш берувчи томонидан Меҳнат мухофазаси ва Техника Хавфсизлиги бузилмади. Жарохат ишчининг оддийгина эхтиёткорсизлиги натижасида келиб чиқди. Бахтсиз ходиса юқори хавфлилик манбаи (ускуна) таъсирида юз бергани боис иш берувчи ўз айби бўлмасада, зарарни тўлиқ қоплаши зарур.

Ишчининг қўпол эхтиёткорсизлиги холатида иш берувчи ва ишчи аралаш жавобгар бўлади. Мазкур холатда қоплаш хажми камайтирилади.

Эхтиёткорсизликнинг қандайлиги (қўпол ва ёки оддий) вазиятлар инобатга олиниб, хар бир аниқ ходисада хал қилинади. Бунда жабрланувчининг ёши, малакаси, жисмоний ахволи ва хоказолар, хамда бахтсиз ходисанинг аниқ вазияти хисобга олинади.

Масалан, агар иш бўйича катта хамкасабалари мисолида, ёш ишчи химоя кўзойнакларини кўзидан олиб қўйди, у эхтиёткорсизлик бўлади. Бироқ қўпол эхтиёткорсизликка йўл қўймади. Унинг техника хавфсизлиги бўйича талаблари ва уста танбехларига қарши борган тажрибали хамкасабалари қаттиқ харакатларини қўпол эхтиёткорсизлик деб хисоблаш мумкин.

Иш берувчи доимо жабрланувчига кўра, бахтсиз ходисани олдини олишда катта имкониятларга эга. Айнан, у ходимлар хавфсизлигини таъминлашга жавобгардир.[12]

2. Агар зарар юқори хавфлилик манбаи томонидан етказилмаган бўлса, иш берувчи фақат айби бўлсагина жавоб беради. Масалан, дўкон сотувчиси ёрдамчи хоналар ўртасида тўкилган ўсимлик ёоғидан тойиб кетди ва йиқилишида жарохат олди, дейлик. Бахтсиз ходиса юқори хавфлилик манбаи билан боғлиқ эмас. Демак, иш берувчига зарар учун жавобгарликни юқлашдан аввал унинг айбини аниқлаб олиш зарур. Айб эса шундаки, иш

хавфсиз ахволда эмас эди. Агар иш мувофиқ ахволда бўлганида эди, иш берувчининг бунда айби хам бўлмасди ва у зарарни қоплашга мажбур хам бошлмасди.

Касбий касаллик, одатда, юқори хавфлилик манбаи таъсирида юзага келади, бу холатда иш берувчининг айбини исботлашнинг хожати юқ, фақат бу хасталикнинг меҳнат мажбуриятлари ижроси билан боғлиқлик жихатини аниқлаш зарур.

3.2.Техноген ҳусусиятли фавқулодда вазиятлар ва улардан мухофазаланиш

Техноген тусдаги фавқулодда вазиятларга 7 хил турдаги вазиятлар киради:

1.Транспортлардаги авариялар ва халокатлар

-экипаж аъзолари ва йўловчиларнинг ўлимига, хаво кемаларининг тўлиқ парчаланишига ёки қаттиқ шикастланишига ҳамда қидирув ва авария-қидирув ишларини талаб қиладиган авиа халокатлар;

-ёнғинга, портлашга, харакатланувчи таркибининг бузилишига сабаб бўлган ва темир йўл ходимларининг халокат худудидаги темир йўл платформаларида, вокзал биноларида ва шахар иморатларида бўлган одамлар ўлимига, шунингдек, ташиланган кучли таъсир кўрсатувчи захарли модда (КТЗМ)лар билан халокат жойига туташ худуднинг захарланишига олиб келган темир йўл транспортидаги халокат ва фалокатлар[12,10]

-портлашларга, ёнғинларга, транспорт восигаларининг парчаланишига, ташилаётган КТЗМларнинг зарарли хоссалари намоён бўлишига ва одамлар ўлими (жарохатланиши, захарланиши)га сабаб бўладиган автомобил транспортининг халокати ва авариялари, шу жумладан, йўл транспорт ходисалари;

-одамларнинг ўлимига, шикастланишига ва захарланишига, метрополитен поеъздлари парчаланишига олиб келадиган метрополитен бекатларидаги ва тунелларидаги халокатлар, авариялар, ёнғинлар;

-газ, нефт махсулотларининг отилиб чиқишига, очиқ нефт ва газ фавваларининг ёниб кетишига сабаб бўладиган магистрал қувурлардаги авариялар.

2. Кимёвий хавфли объектлардаги авариялар:

Теварак-атроф табиий мухитга таъсир қилувчи захарли моддаларнинг (авария ҳолатида) одамлар, хайвонлар ва ўсимликларнинг кўплаб шикастланишига олиб келиши мумкин бўлган ёки олиб келган тақдирда, йўл қўйиладиган чегаравий концентрациялардан анча ортиқ миқдорда санитария-химоя худудидан четга чиқишига сабаб бўладиган кимёвий хавфли объектлардаги авариялар, ёнғин ва портлашлар.[10]

3. Ёнғин, портлаш хавфи мавжуд бўлган объектлардаги авариялар:

-технологик жараёнда портлайдиган, осон ёниб кетадиган ҳамда бошқа ёнғин учун хавфли моддалар ва материаллар ишлатиладиган ёки сақланадиган объектлардаги одамларнинг механик ва термик шикастланишларига, захарланишларига ва ўлимига, асосий ишлаб чиқариш захираларининг нобуд бўлишига, фавқулодда вазиятлар худудларида ишлаб чиқариш марокининг ва одамлар ҳаёт фаолиятининг бузилишига олиб келадиган ёнғинлар ва портлашлар;

-одамларнинг шикастланишига, захарланишига ва ўлимига олиб келадиган ҳамда қидирув-қутқариш ишларини ўтказишни, нафас олиш органларини мухофаза қилишнинг махсус анжомларини ва воситаларини қўллашни талаб қилувчи кўмир шахта паридаги ҳамда кон-руда саноатидаги газ ва чанг портлаши билан боғлиқ авариялар, ёнғинлар ва жинсларнинг қўпорилиши.

4. Энергетика ва коммунал тизимлардаги авариялар:

-саноат ва қишлоқ хўжалиги махсулотлари истеъмолчиларининг авария туфайли энергия таъминотисиз қолишига ҳамда аҳоли ҳаёт фаолиятининг бузилишига олиб келадиган ГЭС, ГРЭС, ИЭСлардаги, туман иссиқлик марказларидаги электр тармоқларидаги буғқозон қурилмаларидаги,

копрессор, газ тақсимлаш шахобчаларидаги ва бошқа энергия таъминоти объектларидаги авариялар, ёнғинлар, аҳоли ҳаёт фаолиятининг бузилишига ва саломатлигига хавф туғилишига олиб келадиган газ қувурларидаги, сув чиқариш иншоотларидаги, сув қувурларидаги, канализация ва бошқа коммунал объектлардаги авариялар;[11,10]

-атмосфера, тупроқ, ер ости ва ер усти сувларининг одамлар саломатлигига хавф туғдирувчи даражада концентрациядаги зарарли моддалар билан ифлосланишига сабаб бўладиган газ тозалаш қурилмаларидаги, биологик ва бошқа тозалаш иншоотларидаги авариялар.

5. Бино ва иншоотларнинг бирдан қулаб тушиши билан боғлиқ авариялар:

Одамлар ўлими билан боғлиқ бўлган ва зудлик билан авария қутқарув утказилишини ҳамда зарар кўрганларга шошилинч тиббий ёрдам кўрсатилишини талаб қиладиган мактаблар, касалхоналар, кинотеатрлар ва бошқа ижтимоий йўналишдаги объектлар, шунингдек, уй-жой сектори бинолари конструкцияларининг тўсатдан бузилиши, ёнғинлар, газ портлаши ва бошқа ходисалар.

6. Радиоактив ва бошқа хавфли ҳамда экологик жихатдан зарарли моддалардан фойдаланши ёки уларни сақлаш билан боғлиқ авариялар:

-санитария химоя худуди ташқарига чиқариб ташланиши натижасида пайдо бўладиган юқори даражадаги радиоактивлик одамларнинг йўл қўйиладиган кўп миқдорда нурланишини келтириб чиқарадиган технологик жараёнда радиоактив моддалардан фойдаланадиган объектлардаги авариялар;

-радиоактив материалларни ташиш вақтидаги авариялар;

-радиоизотоп буюмларнинг йўқотилиши;

-биологик воситаларни ва улардан олинадиган препаратларни тайёрлаш, сақлаш ва ташишни амалга оширувчи илмий тадқиқот ва бошқа

муассасаларда биологик воситаларнинг атроф-мухитга чиқиб кетиши ёки йўқотилиши билан боғлиў вазиятлар. [12,11]

7. Гидротехник иншоотлардаги халокатлар ва авариялар:

Сув омборларида, дарё ва каналлардаги бузилишлар, баланд тоғлардаги йўллардан сув уриб кетиши натижасида вужудга келадиган ҳамда сув босган худудларда одамлар ўлимига, саноат ва қишлоқ хўжалиги объектлари ишининг, ахоли ҳаёт фаолиятинингбузилишига олиб келадиган ва шошилинч кўчириш тадбирларини талаб қиладиган халокатли сув босишлари.

Фуқаро мухофазаси тадбирларини режалаштириш. Ҳарбий даврда ҳам, тинчлик даврида ҳам юзага келадиган хавфлардан аҳолини, худудларни, моддий бойликларни мухофаза қилишда мухим вазифаларни бажаради. Бу борада Ўзбекистон Республикасининг 2000 йил 26 майда қабул қилган «Фуқаро мухофазаси тўғрисида» ги қонунида ўз аксини топган.

Ушбу қонун фуқаро мухофазаси сохасидаги асосий вазифаларни, уларни амалга оширишнинг хуқуқий асосларини, давлат органларининг, корхоналар, муассасалар ва ташкилотларнинг ваколатларини хамда фукаро мухофазаси кучлари ва воситаларини хам белгилаб берган.

1. Ахоли ва объектларни ҳарбий харакатлар олиб бориш пайтида ёки шу харакатлар оқибатида юзага келадиган хавфлардан ҳимоялаш харакатлари ва усулларига тайёрлаш.

2. Бошқарув, хабар бериш ва алоқа тизимларини ташкил қилиш, ривожлантириш ва доимий шай холатда сақлаб туриш.

3. Халқ хўжалиги объектларининг барқарор ишлашини таъминлаш юзасидан тадбирлар комплексини ўтказиш.

4. Ахолини, моддий ва маданий бойликларини хавфсиз жойларга эвакуация қилиш.

5. Фуқаро мухофазаси ҳарбий тизимлари шайлигини таъминлаш.

6. Ахолини умумий ва шахсий сақловчи воситалари билан таъминлаш тадбирларини ўтказиш.[10]

7. Ахолининг ҳарбий даврдаги ҳаёт фаолиятини таъминлаш .

8. Радиациявий, кимёвий ва биологик вазият устидан кузатиш ва лаборатория назорати олиб бориш.

9. Қугқарув ва бошқа кечиктириб бўлмайдиган ишларни ўтказиш.

10. Ҳарбий даврларда хам зарар кўрган худудларда жамоат тартибини йўлга қўйиш ва сақлаб туриш.

11. Ахолини ва худудларни мухофаза қилиш юзасидан бошқа тадбирларни амалга ошириш.

Мана шу вазифаларни муваффақиятли олиб бормай туриб, зарарланган худудларда, объектларда муътадил ҳаёт фаолиятини яратиб бўлмайди. Бу ишларни давлат органлари орқали, фуқаро мухофазаси бошчилигида бутун халқ ёрдамида амалга оширилади.[11]

3.3. Ўзбекистонда экологик хавфсизликни таъминлаш

Экологик хавфсизликни таъминлаш эндиликда биринчи ражали ва кечиктириб бўлмайдиган вазифага айланди. Чунки, ичимлик сувларининг ифлосланганлиги, жойларда атмосфера хавосини чиқиндилар билан жиддий туйинганлиги, бунинг натижасида аҳоли орасида турли касалликлар тарқалганлиги, форма ерларни шурланиб, яйловларнинг махсулдорлигини пасайиб бораётганлиги қишлоқ хўжалик ишлаб чиқаришига салбий таъсир этаётганлиги мамлакат миқёсида туб ўзгаришларни амалга ошириш зарурлигини ўқтиради.

Экологик хавфсизликни таъминлаш борасида бир қатор бир-бирлари билан боғлик бўлган тутунли масалаларни амал қилиш зим бўлади. Биринчи галда экологик (биоэкологик, геосистели, биосферали) мониторингни амалга ошириш устувор ахамиятга эга. Ўзбекистонда бу турдаги мониторинг ҳозирда турли массасалар ва ташкилотлар томонидан амалга ошириб келинмокда, лекин уларнинг кўлами ва эгаллаган худуди ҳозирги талабга мутлақо жавоб бермайди. Чунончи, тупроқнинг саноат ва кимёвий ашёлар

билан ифлосланиши (Республика Бош Гидромет хизматига юклатилган) фақат айрим қишлоқ жамоалари худуди буйича назорат қилинади. Бунда барча вилоятларнинг суғориладиган ерлари назарда тутилмаган, хеч бўлмаганда хар бир вилоят бўйича танлаб олинган тестли жамоа хужаликларини маълум участкалари назарда тутилганда мақсадга мувофиқ бўлар эди. Фақат шундагина республика худуди бўйича суқорма ерларни техноген ифлосланиши бўйича тегишли хулоса чиқариш мумкин бўлади. Худди шундай ахвол сув хавзаларининг ифлосланиши, атмосфера хавосининг чиқиндилар билан туйиниши ва бошқа соҳаларда хам мавжуд, уларнинг белгиланган меъёрда бўлиши табиий муҳит буйича зарур бўлган мониторинг ахборотларини олиш ва мавжуд экологик вазият тўғрисида аниқ хулоса чиқаришга имкон беради. [12,10]

Экологик экспертиза янги кўриладиган саноат корхоналари учун хос. Лекин мантиқан қараганда ишлаб турган барча саноат корхоналари, гидротехник иншоотлар ва бошка мухандислик объектлар учун мунтазам экспертиза ўтказиш зарур. Атроф-муҳитни аслида эскидан ишлаб келаёгган саноат корхоналари ифлослаб келмоқда. Бинобарин, экологик экспертиза барча корхоналарни назоратга олиши шарт. Шундагина табиий мухитда тозаланиш бошланиши мумкин.

Экологик вазиятни бошқариш ва тегишли тадбирлар мажмуасини қўллаш учун негиз сифатида турли масштабларда экологик ва табиатни муҳофаза қилиш хариталарини яратиш жоиз. Бу хариталар республика худудида мавжуд экологик вазиятларни назорат қилиш, уларнинг тадрижий ўзгаришларини ўрганиш, тегишли чора - тадбирларни режалаштириш имконини беради. Мавжуд хариталар муваккат бўлиб, уларнинг хар йили янги маълумотлар билан янгилаб турилиши амалий ахамият касб этади. Хар бир вилоят маълум масштабда экологик ва табиатни мухофаза қилиш хариталарига эга бўлиши ва дискетларга тушириш компьютерлар орқали мутахассислар хамда рахбарият (шахар, вилоят хокимлари, Республика

Вазирлар Махкамаси)га фойдаланиш учун топширилиши даркор. Компъютерлар оркали алоқа барча вилоятлардан олишан тасвирлар ёрдамида Тошкентда республика буйича жамланма мониторингли ахборот олиниш имкони бўлади.

Табиатни муҳофаза қилиш буйича чиқарилган барча Олий Мажлис қонунлари ва Вазирлар Махкамасининг қарорлари, кўрсатмалари ва бошқа меъёрий хужжатлари ўз вақтида бажарилиши ва уларга амал қилиниши лозим. Қонунга хурмат табиатга хам хурматни билдиради.

Экологик хавфсизликни таъминлаш шунингдек, меъёрий кўрсаткичлар, РЭМ ва бошқа қабул қилинган маълум андозаларга риоя қилишга хам боғликдир. Саноат, автотранспорт чиқиндилари энг кам хавфсиз кўрсаткичларга қадар камайган бўлиши, иккиламчи ресурслар тўлиқ, қайта ишланиб улардан фойдали элементлар ажратиб олиниши зарур. Энг мухими, исрофгарчиликка чек қўйилиб, табиатдан эхтиёжга яраша бойликларни ажратиб олиб, чикиндиларни чиқармаслик тамойилида иш тутишга ўтишдан иборат. Табиатдан бойликларни олишда “ким ошди” тамойилидан воз кечиб уни бойитиш, ресурсларни қайта тиклаш, камайиб бораётганларидан эхтиёткорлик билан фойдаланиш, бу борада муқобил вариантлар, яъни урнини босадиган бошқа ресурслардан фойдаланишга ўтиш каби тамойилларни барча жойларда, хамма ишлаб чиқариш корхоналарида-қуллашга ўтиш табиатни асраш, уни эъзозлаш ўз навбатида экологик хавфсизликни таъминлашни кафолатлайди. [10,11]

Хулоса

Битирув малакавий иши бўйича қуйидагиларни хулоса сифатида кўрсатиш мумкин.

1.Аутентификациялаш усули асосида ҳужжатларни қалбакилаштиришдан ҳимоялашда электрон рақамли имзодан ва хеш-функциялардан фойдаланиш мақсадга мувофиқ хисобланади.

2.Маьлумотларнинг сони мумкин бўлган хеш-қийматлар сонидан кўп бўлади.Демак хар бир хеш-қийматга бир нечта матнлар тўплами мос келади.

3.Электрон рақамлм имзо,яьни узатиладиган ва сақланадиган шифрланган матнга бириктирилган рақам ҳужжатларнинг ва муаллифнинг ҳақиқийлигини кафолатлайди.

4.Ҳужжатни қалбакилаштиришдан ҳимоялаш дастурий модули ишлаб чиқилди. Бу дастурда аутентификациялаш учун электрон рақамли имзодан фойдаланилди.

5.Хаёт фаолияти хавфсизлиги бўлимида ишлаб чиқаришда ходимлар саломатлигига зарар етиши ва иш берувчиниг маьсулияти масалалари ёритилган. Техноген хусусиятли фавқулотда вазиятлар ва улардан ҳимояланиш масалалари хам кўрилган.

Фойдаланилган адабийотлар

1.*Каримов И.А.* Мамлакатимизда демократик ислоҳотларни янадачуқурлаштириш ва фуқаролик жамиятини ривожлантириш Концепцияси. – Т.,2010.

2. Ўзбекистон Республикасининг «Ахборотлаштириш тўғрисида»ги қонуни Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси. – 2004. №12.10-м.

3. *Каримов И.А*. Мамлакатимизда демократик ислоҳотларни янада чуқур лаштириш ва фуқаролик жамиятини ривожлантириш концепцияси. – Т.,2010.

4. Ўзбекистон Республикасининг «Ахборот эркинлиги принциплари ва кафолатлари тўғрисида»ги қонуни // Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси. – 2003. – №1. – 2-м.

5. С.К.Ганиев, М.М. Каримов. Хисоблаш системалари ва тармокларида информация химояси. Олий ўқув юрт.талаб. учун ўқув қўлланма.Тошкент Давлат техника ўниверситети, 2008.

6 .www.Google.ru

7. Вэк Дж., Карнахан Л. Безопасность корпоративной сети при работе с Интернетом. Введение в межсетевые экраны //Конфидент.-2000.-№4-5.

8.Ziyonet.uz

9. Экология и безопасность жизнедеятельности: Учебное пособие для студентов ВУЗов/ ред. Л. А. Муравий, 2002.

10. Белов С.В. Безопасность жизнедеятельности М.: Высшая школа. 2003

11. ЁрматовҒ.Ё., Исамухамедов Ё.У. Меҳнатни мухофаза қилиш. Дарслик. Ўзбекистан нашриёти. Тошкент 2002.

Иловалар

```
package Fahim;
import javax.swing.JFrame;
import java.awt.event.*;
import java.awt.*;
import javax.swing.*;
import java.util.*;
import javax.xml.*;
import javax.xml.transform.*;
import javax.xml.transform.stream.*;
import javax.xml.transform.dom.*;
import org.w3c.dom.*;
import javax.xml.parsers.*;
import org.xml.sax.*;
import Fahim.XMLWork.Update.sign1;
import java.io.*;
import java.io.*;
import java.security.*;
import java.security.spec.*;
import java.util.*;
class XMLWork extends JFrame {
private JPanel buttonPanel;
private JLabel l1;
private JLabel l2;
private JLabel l3;
private JLabel l4;
private JLabel l5;
private JLabel l6;
private JTextField t1;
private JTextField t2;
private JTextField t3;
private JTextField t4;
private JTextField t5;
private JTextField t6;
private JButton StoreButt;
private JButton ReadButt;
private JButton SearchButt;
private JButton UpdateButt;
private JButton GenSigButt;
private JButton VerSigButt;
```

```
private JButton ResetButt;
private JButton ExitButt;
public XMLWork() {
l1 = new JLabel("Foydalanuvchi Nomi: ", SwingConstants.LEFT);
l2 = new JLabel("Tug`ilgan Yil: ", SwingConstants.LEFT);
l3 = new JLabel("ID: ", SwingConstants.LEFT);
l4 = new JLabel("No: ", SwingConstants.LEFT);
l5 = new JLabel("Ma`lumot: ", SwingConstants.LEFT);
l6 = new JLabel("Reja: ", SwingConstants.LEFT);
t1 = new JTextField(5);
t2 = new JTextField(5);
t3 = new JTextField(5);
t4 = new JTextField(5);
t5 = new JTextField(5);
t6 = new JTextField(5);
StoreButt = new JButton("Foydalanuvchi Nomi");
StoreButtonHandler StoreB = new StoreButtonHandler();
StoreButt.addActionListener(StoreB);
ReadButt = new JButton("Baza");
ReadButtonHandler ReadB = new ReadButtonHandler();
ReadButt.addActionListener(ReadB);
SearchButt = new JButton("Qidirish");
SearchButtonHandler SearchB = new SearchButtonHandler();
SearchButt.addActionListener(SearchB);
UpdateButt = new JButton("Yuklash");
UpdateButtonHandler UpdateB = new UpdateButton
UpdateButt.addActionListener(UpdateB);
GenSigButt = new JButton("Elektron Imzo");
GenSigButtonHandler GenSigB = new GenSigButtonHandler();
GenSigButt.addActionListener(GenSigB);
VerSigButt = new JButton("Imzoni Tasdiqlash");
VerSigButtonHandler VerSigB = new VerSigButtonHandler();
VerSigButt.addActionListener(VerSigB);
ResetButt = new JButton("O`chirish");
ResetButtonHandler Refresh = new ResetButtonHandler();
ResetButt.addActionListener(Refresh);
ExitButt = new JButton("Chiqish");
ExitButtonHandler CloseOut = new ExitButtonHandler();
ExitButt.addActionListener(CloseOut);
setTitle("Autentifikatsiya va Elektron raqamli imzo");
Container pane = getContentPane();
```

```
pane.setLayout(new GridLayout(10, 2));
pane.add(l1);
pane.add(t1);
pane.add(l2);
pane.add(t2);
pane.add(l3);
pane.add(t3);
pane.add(l4);
pane.add(t4);
pane.add(l5);
pane.add(t5);
pane.add(l6);
pane.add(t6);
pane.add(StoreButt);
pane.add(UpdateButt);
pane.add(ReadButt);
pane.add(SearchButt);
pane.add(GenSigButt);
pane.add(VerSigButt);
pane.add(ResetButt);
pane.add(ExitButt);
setDefaultCloseOperation(EXIT_ON_CLOSE);
}
private class StoreButtonHandler implements ActionLi
public void actionPerformed(ActionEvent e) {
String i1, i2, i3, i4, i5, i6;
i1 = (t1.getText());
i2 = (t2.getText());
i3 = (t3.getText());
i4 = (t4.getText());
i5 = (t5.getText());
i6 = (t6.getText());
if ((i1.length() != 0) && (i2.length() != 0) && (i3.length() != 0)
&& (i4.length() != 0) && (i5.length() != 0)
&& (i6.length() != 0)) {
Element rootElement;
DocumentBuilderFactory builderFactory = DocumentBuilderFactory
.newInstance();
DocumentBuilder docBuilder = null;
try {
docBuilder = builderFactory.newDocumentBuilder();
```

```
} catch (ParserConfigurationException e1) {
// TODO Auto-generated catch block
e1.printStackTrace();
}
Document document = docBuilder.newDocument();
File file1 = new File("file.xml");
if (file1.exists()) {
DocumentBuilderFactory fact = DocumentBuilderFac
.newInstance();
try {
DocumentBuilder builder = fact.newDocumentBuilder();
} catch (ParserConfigurationException e1) {
// TODO Auto-generated catch block
e1.printStackTrace();
}
try {
document = docBuilder.parse(file1);
} catch (SAXException e1) {
// TODO Auto-generated catch block
e1.printStackTrace();
} catch (IOException e1) {
// TODO Auto-generated catch block
e1.printStackTrace();
}
rootElement = document.getDocumentElement();
// root = node.getNodeName();
} else {
rootElement = document.createElement("Syllabus");
document.appendChild(rootElement);
}
Element root = document.getDocumentElement();
// Element rootElement = document.getDocumentElement();
Element subject = document.createElement("subject");
rootElement.appendChild(subject);
Element name = document.createElement("name");
name.appendChild(document.createTextNode(i1));
subject.appendChild(name);
Element year = document.createElement("year");
year.appendChild(document.createTextNode(i2));
subject.appendChild(year);
Element sem = document.createElement("semester");
```

```
sem.appendChild(document.createTextNode(i3));
subject.appendChild(sem);
Element courseno = document.createElement("course
courseno.appendChild(document.createTextNode(i4));
subject.appendChild(courseno);
Element credit = document.createElement("credit");
credit.appendChild(document.createTextNode(i5));
subject.appendChild(credit);
Element syllabus = document.createElement("syllabus");
syllabus.appendChild(document.createTextNode(i6));
subject.appendChild(syllabus);
root.appendChild(subject);
try {
DOMSource source = new DOMSource(document);
TransformerFactory transformerFactory = TransformerFactory
.newInstance();
Transformer transformer = transformerFactory
.newTransformer();
StreamResult result = new StreamResult("file.xml");
transformer.transform(source, result);
JOptionPane.showMessageDialog(null, "Muvaffaqiyatli Saqlandi");
}
catch (Exception ex) {
}
sign1 ac = new sign1();
ac.getContentPane().setBackground(Color.LIGHT_GRAY);
ac.setCursor(Cursor.getPredefinedCursor(Cursor.HAND_CURSOR));
ac.setBounds(400, 200, 300, 200);
ac.setVisible(true);
} else {
JOptionPane.showMessageDialog(null,
"Kechirasiz !! Iltimos barcha maydonlarni to'ldiring", "Xatolik",
JOptionPane.WARNING_MESSAGE);
}
}
class sign1 extends JFrame {
private JPanel buttonPanel;
private JLabel l2;
private JLabel l3;
JPasswordField t2;
JPasswordField t3;
```

```
private JButton OkButt;
public sign1() {
l2 = new JLabel("Jamoaaviy Kaliy: ", SwingConstants.LEFT);
l3 = new JLabel("Xususiy Kalit: ", SwingConstants.LEFT);
t2 = new JPasswordField(10);
t3 = new JPasswordField(10);
OkButt = new JButton("Tasdiqlash");
OkButtonHandler OkB = new OkButtonHandler();
OkButt.addActionListener(OkB);
setTitle("Autentifikatsiya va Elektron raqamli imzo");
Container pane = getContentPane();
pane.setLayout(new GridLayout(4, 2));
pane.add(l2);
pane.add(t2);
pane.add(l3);
pane.add(t3);
pane.add(OkButt);
}
private class OkButtonHandler implements ActionListener {
public void actionPerformed(ActionEvent e) {
String i1, i2, i3, i4, i5, i6;
i1 = (t1.getText());
i2 = new String(t2.getPassword());
i3 = new String(t3.getPassword());
String xmlFilePath1 = "file.xml";
String signedXmlFilePath1 = "digitallysignedfile.xml";
String privateKeyFilePath1 = i3 + ".key";
String publicKeyFilePath1 = i2 + ".key";
XmlDigitalSignatureGenerator xmlSig1 = new XmlDigitalSignatureGenerator();
xmlSig1.generateXMLDigitalSignature(xmlFilePath1,
signedXmlFilePath1, privateKeyFilePath1,
publicKeyFilePath1);
JOptionPane.showMessageDialog(null, "Muaffaqiyatli o`tildi");
}
}
}
}
private class ReadButtonHandler implements ActionListener {
public void actionPerformed(ActionEvent e) {
String s = " ";
try {
```

```
File fXmlFile = new File("file.xml");
DocumentBuilderFactory dbFactory = DocumentBuilderFactory
.newInstance();
DocumentBuilder dBuilder = dbFactory.newDocumentBuilder();
Document doc = dBuilder.parse(fXmlFile);
doc.getDocumentElement().normalize();
NodeList nList = doc.getElementsByTagName("subject");
for (int temp = 0; temp < nList.getLength(); temp++) {
Node nNode = nList.item(temp);
if (nNode.getNodeType() == Node.ELEMENT_NODE) {
Element eElement = (Element) nNode;
s = s
+ "\nF_Nomi : "
+ eElement.getElementsByTagName("name").item(0)
.getTextContent()
+ "\nT_Yil : "
+ eElement.getElementsByTagName("year").item(0)
.getTextContent()
+ "\nID : "
+ eElement.getElementsByTagName("semester")
.item(0).getTextContent()
+ "\nNo : "
+ eElement.getElementsByTagName("courseno")
.item(0).getTextContent()
+ "\nMa`lumot : "
+ eElement.getElementsByTagName("credit")
.item(0).getTextContent()
+ "\nReja : "
+ eElement.getElementsByTagName("syllabus")
.item(0).getTextContent();
}
s = s + "\n";
}
JOptionPane.showMessageDialog(null, s);
} catch (Exception e1) {
e1.printStackTrace();
}
}
}
private class SearchButtonHandler implements ActionListener {
public void actionPerformed(ActionEvent e) {
```

```
String s = " ";
try {
String i1 = (t1.getText());
File fXmlFile = new File("file.xml");
DocumentBuilderFactory dbFactory = DocumentBuilderFactory
.newInstance();
DocumentBuilder dBuilder = dbFactory.newDocumentBuilder();
Document doc = dBuilder.parse(fXmlFile);
doc.getDocumentElement().normalize();
NodeList nList = doc.getElementsByTagName("subject");
for (int temp = 0; temp < nList.getLength(); temp++) {
Node nNode = nList.item(temp);
if (nNode.getNodeType() == Node.ELEMENT_NODE) {
Element eElement = (Element) nNode;
if (i1.equals(eElement.getElementsByTagName("na
.item(0).getTextContent())) {
s = s
+ "\nF_Nomi : "
+ eElement.getElementsByTagName("name")
.item(0).getTextContent()
+ "\nT_Yil : "
+ eElement.getElementsByTagName("year")
.item(0).getTextContent()
+ "\nID : "
+ eElement.getElementsByTagName("semester")
.item(0).getTextContent()
+ "\nNo : "
+ eElement.getElementsByTagName("courseno")
.item(0).getTextContent()
+ "\nMa`lumot : "
+ eElement.getElementsByTagName("credit")
.item(0).getTextContent()
+ "\nReja : "
+ eElement.getElementsByTagName("syllabus")
.item(0).getTextContent();
}
s = s + "\n";
}
}
JOptionPane.showMessageDialog(null, s);
} catch (Exception e1) {
```

```
e1.printStackTrace();
}
}
}
private class UpdateButtonHandler implements ActionListener {
public void actionPerformed(ActionEvent e) {
Update ac1 = new Update();
ac1.getContentPane().setBackground(Color.LIGHT_GRAY);
ac1.setCursor(Cursor.getPredefinedCursor(Cursor.HAND_CURSOR));
ac1.setBounds(400, 200, 400, 400);
ac1.setVisible(true);
}
}
private class GenSigButtonHandler implements ActionListener {
public void actionPerformed(ActionEvent e) {
try_pass ac = new try_pass();
ac.getContentPane().setBackground(Color.LIGHT_GRAY);
ac.setCursor(Cursor.getPredefinedCursor(Cursor.HAND_CURSOR));
ac.setBounds(400, 200, 300, 300);
ac.setVisible(true);
}
}
private class VerSigButtonHandler implements ActionListener {
public void actionPerformed(ActionEvent e) {
Verify ac = new Verify();
ac.getContentPane().setBackground(Color.LIGHT_GRAY);
ac.setCursor(Cursor.getPredefinedCursor(Cursor.HAND_CURSOR));
ac.setBounds(400, 200, 300, 300);
ac.setVisible(true);
}
}
private class ResetButtonHandler implements ActionListener {
public void actionPerformed(ActionEvent e) {
t1.setText("");
t2.setText("");
t3.setText("");
t4.setText("");
t5.setText("");
t6.setText("");
}
}
```

```
private class ExitButtonHandler implements ActionListener {
public void actionPerformed(ActionEvent e) {
System.exit(0);
}
}
public class Update extends JFrame {
private JPanel buttonPanel;
private JLabel l1;
private JLabel l2;
private JLabel l3;
private JLabel l4;
private JLabel l5;
private JLabel l6;
private JLabel l7;
private JTextField t1;
private JTextField t2;
private JTextField t3;
private JTextField t4;
private JTextField t5;
private JTextField t6;
private JTextField t7;
private JButton ConfirmButt;
private JButton SignButt;
private JButton Reset1Butt;
private JButton Exit1Butt;
public Update() {
l1 = new JLabel("Foydalanuvchi Nomi: ", SwingConstants.LEFT);
l2 = new JLabel("Tug`ilgan yil: ", SwingConstants.LEFT);
l3 = new JLabel("ID: ", SwingConstants.LEFT);
l4 = new JLabel("No: ", SwingConstants.LEFT);
l5 = new JLabel("Ma`lumot: ", SwingConstants.LEFT);
l6 = new JLabel("Reja: ", SwingConstants.LEFT);
l7 = new JLabel(
"Ma`lumotni kiriting : ",
SwingConstants.LEFT);
t1 = new JTextField(5);
t2 = new JTextField(5);
t3 = new JTextField(5);
t4 = new JTextField(5);
t5 = new JTextField(5);
t6 = new JTextField(5);
```

```
t7 = new JTextField(5);
ConfirmButt = new JButton("Tasdiqlash");
ConfirmButtonHandler ConfirmB = new ConfirmButtonHandler();
ConfirmButt.addActionListener(ConfirmB);
SignButt = new JButton("Kirish");
SignButtonHandler SignB = new SignButtonHandler();
SignButt.addActionListener(SignB);
Reset1Butt = new JButton("O`chirish");
Reset1ButtonHandler Refresh = new Reset1ButtonH
Reset1Butt.addActionListener(Refresh);
Exit1Butt = new JButton("Chiqish");
Exit1ButtonHandler CloseOut = new Exit1ButtonHa
Exit1Butt.addActionListener(CloseOut);
setTitle("Yuklash");
Container pane1 = getContentPane();
pane1.setLayout(new GridLayout(9, 2));
pane1.add(l7);
pane1.add(t7);
pane1.add(l1);
pane1.add(t1);
pane1.add(l2);
pane1.add(t2);
pane1.add(l3);
pane1.add(t3);
pane1.add(l4);
pane1.add(t4);
pane1.add(l5);
pane1.add(t5);
pane1.add(l6);
pane1.add(t6);
pane1.add(ConfirmButt);
pane1.add(SignButt);
pane1.add(Reset1Butt);
pane1.add(Exit1Butt);
}
private class ConfirmButtonHandler implements ActionListener {
public void actionPerformed(ActionEvent e) {
String i1, i2, i3, i4, i5, i6, i7;
i7 = (t7.getText());
i1 = (t1.getText());
i2 = (t2.getText());
```

```
i3 = (t3.getText());
i4 = (t4.getText());
i5 = (t5.getText());
i6 = (t6.getText());
System.out.println(i1);
try {
File fXmlFile = new File("file.xml");
DocumentBuilderFactory dbFactory = DocumentBuilderFactory
.newInstance();
DocumentBuilder dBuilder = dbFactory.newDocumentBuilder();
Document doc = dBuilder.parse(fXmlFile);
NodeList nList = doc.getElementsByTagName("subject");
String s = " ";
for (int temp = 0; temp < nList.getLength(); temp++) {
Node nNode = nList.item(temp);
if (nNode.getNodeType() == Node.ELEMENT_NODE) {
Element eElement = (Element) nNode;
if (i7.equals(eElement.getElementsByTagName("name")
.item(0).getTextContent())) {
if (i1.length() > 0) {
eElement.getElementsByTagName("name")
.item(0).setTextContent(i1);
}
if (i2.length() > 0) {
eElement.getElementsByTagName("year")
.item(0).setTextContent(i2);
}
if (i3.length() > 0) {
eElement.getElementsByTagName("semester")
.item(0).setTextContent(i3);
}
if (i4.length() > 0) {
eElement.getElementsByTagName("courseno")
.item(0).setTextContent(i4);
}
if (i5.length() > 0) {
eElement.getElementsByTagName("credit")
.item(0).setTextContent(i5);
}
if (i6.length() > 0) {
eElement.getElementsByTagName("syllabus")
```

```
.item(0).setTextContent(i6);
}
JOptionPane
.showMessageDialog(null, "Confirmed");
}
}
TransformerFactory transformerFactory = TransformerFactory
.newInstance();
Transformer transformer = transformerFactory
.newTransformer();
DOMSource source = new DOMSource(doc);
StreamResult result = new StreamResult(new File(
"file.xml"));
transformer.transform(source, result);
try {
KeyPairGenerator keyGen = KeyPairGenerator
.getInstance("DSA", "SUN");
SecureRandom random = SecureRandom.getInstance(
"SHA1PRNG", "SUN");
keyGen.initialize(1024, random);
KeyPair pair = keyGen.generateKeyPair();
PrivateKey priv = pair.getPrivate();
PublicKey pub = pair.getPublic();
Signature dsa = Signature.getInstance(
"SHA1withDSA", "SUN");
dsa.initSign(priv);
FileInputStream fis = new FileInputStream(
"file.xml");
BufferedInputStream bufin = new BufferedInputStream(
fis);
byte[] buffer = new byte[2048];
int len;
while (bufin.available() != 0) {
len = bufin.read(buffer);
dsa.update(buffer, 0, len);
}
;
bufin.close();
byte[] realSig = dsa.sign();
FileOutputStream sigfos = new FileOutputStream(
"rafi");
```

```
sigfos.write(realSig);
sigfos.close();
byte[] key = pub.getEncoded();
FileOutputStream keyfos = new FileOutputStream(
"fahim");
keyfos.write(key);
keyfos.close();
} catch (Exception e1) {
System.err.println("Caught exception "
+ e1.toString());
}
}
} catch (Exception e1) {
e1.printStackTrace();
}
}
}
private class SignButtonHandler implements ActionListener {
public void actionPerformed(ActionEvent e) {
sign1 ac = new sign1();
ac.getContentPane().setBackground(Color.LIGHT_GRAY);
ac.setCursor(Cursor.getPredefinedCursor(Cursor.HAND_CURSOR));
ac.setBounds(400, 200, 200, 200);
ac.setVisible(true);
}
}
class sign1 extends JFrame {
private JPanel buttonPanel;
private JLabel l2;
private JLabel l3;
JPasswordField t2;
JPasswordField t3;
private JButton OkButt;
public sign1() {
l2 = new JLabel("Jamoaviy Kalit: ", SwingConstants.LEFT);
l3 = new JLabel("Xususiy Kalit: ", SwingConstants.LEFT);
t2 = new JPasswordField(10);
t3 = new JPasswordField(10);
OkButt = new JButton("Tasdiqlash");
OkButtonHandler OkB = new OkButtonHandler();
OkButt.addActionListener(OkB);
```

```
setTitle("Autentifikatsiya va raqamli imzo");
Container pane = getContentPane();
pane.setLayout(new GridLayout(4, 2));
pane.add(l2);
pane.add(t2);
pane.add(l3);
pane.add(t3);
pane.add(OkButt);
}
private class OkButtonHandler implements ActionL
public void actionPerformed(ActionEvent e) {
String i1, i2, i3, i4, i5, i6;
i1 = (t1.getText());
i2 = new String(t2.getPassword());
i3 = new String(t3.getPassword());
String xmlFilePath1 = "file.xml";
String signedXmlFilePath1 = "digitallysignedfile.xml";
String privateKeyFilePath1 = i3 + ".key";
String publicKeyFilePath1 = i2 + ".key";
XmlDigitalSignatureGenerator xmlSig1 = new XmlDigitalSignatureGenerator();
xmlSig1.generateXMLDigitalSignature(xmlFilePath1,
signedXmlFilePath1, privateKeyFilePath1,
publicKeyFilePath1);
JOptionPane.showMessageDialog(null, "Muaffaqiyatli o`tildi");
}
}
}
private class Reset1ButtonHandler implements ActionListener {
public void actionPerformed(ActionEvent e) {
t1.setText("");
t2.setText("");
t3.setText("");
t4.setText("");
t5.setText("");
t6.setText("");
}
}
private class Exit1ButtonHandler implements ActionListener {
public void actionPerformed(ActionEvent e) {
setVisible(false);
}
```

```
}
}
class try_pass extends JFrame {
private JPanel buttonPanel;
private JLabel l1;
private JLabel l2;
JTextField p1;
JTextField p2;
private JButton OkButt;
public try_pass() {
l1 = new JLabel("Jamoaviy Kalit: ", SwingConstants.LEFT);
l2 = new JLabel("Xususiy Kalit: ", SwingConstants.LEFT);
p1 = new JTextField(10);
p2 = new JTextField(10);
OkButt = new JButton("Tasdiqlsh");
OkButtonHandler OkB = new OkButtonHandler();
OkButt.addActionListener(OkB);
setTitle("Autentifikatsiya va raqamli imzo");
Container pane = getContentPane();
pane.setLayout(new GridLayout(3, 2));
pane.add(l1);
pane.add(p1);
pane.add(l2);
pane.add(p2);
pane.add(OkButt);
}
private class OkButtonHandler implements ActionLi
public void actionPerformed(ActionEvent e) {
String PrivateKey = p2.getText();
String PublicKey = p1.getText();
String keysDirPath = ".";
KryptoUtil util = new KryptoUtil();
String result = util.storeKeyPairs(keysDirPath, PrivateKey,
PublicKey);
if (result.equals("success")) {
JOptionPane.showMessageDialog(null,
"Muaffaqiyatli raqamli imzo yaratilindi",
"Imzo yaratilindi", JOptionPane.WARNING_MESSAGE);
}
}
}
```

```
}
class Verify extends JFrame {
private JPanel buttonPanel;
private JLabel l1;
JTextField p1;
private JButton OkButt;
public Verify() {
l1 = new JLabel("Jamoaviy Kalit: ", SwingConstants.LEFT);
p1 = new JTextField(10);
OkButt = new JButton("Tasdiqlash");
OkButtonHandler OkB = new OkButtonHandler();
OkButt.addActionListener(OkB);
setTitle("Autentifikatsiya va raqamli imzo");
Container pane = getContentPane();
pane.setLayout(new GridLayout(3, 2));
pane.add(l1);
pane.add(p1);
pane.add(OkButt);
}
private class OkButtonHandler implements ActionListener {
public void actionPerformed(ActionEvent e) {
String PublicKey = p1.getText();
String keysDirPath = ".";
String signedXmlFilePath = "digitallysignedfile.xml";
String publicKeyFilePath = PublicKey+".key";
try {
boolean validFlag = XmlDigitalSignatureVerifier.
isXmlDigitalSignatureValid(signedXmlFilePath, publicKeyFilePath);
System.out.println("Raqamli Imzo amal qilish muddati : " + validFlag);
if(validFlag==true)
{
JOptionPane.showMessageDialog(null,
"Faylni aniqlash muaffaqiyatli", "Xatolik",
JOptionPane.WARNING_MESSAGE);
}
else
{
JOptionPane.showMessageDialog(null,
"Kechirasiz !! Aniqlash muvaffaqiyatsiz", "Xatolik",
JOptionPane.WARNING_MESSAGE);
}
```

```
} catch (Exception ex) {
ex.printStackTrace();
}
}
}
}
static class XML_SIGN_UPDATE {
public static void main(String[] args) throws Exception {
XMLWork ac = new XMLWork();
ac.getContentPane().setBackground(Color.LIGHT_GRAY);
ac.setCursor(Cursor.getPredefinedCursor(Cursor.HAND_CURSOR));
ac.setBounds(400, 200, 500, 400);
ac.setVisible(true);
}
}
}
```

KryptoUtil.java

```
package Fahim;
import java.io.File;
import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.FileOutputStream;
import java.io.IOException;
import java.io.OutputStream;
import java.security.Key;
import java.security.KeyFactory;
import java.security.KeyPair;
import java.security.KeyPairGenerator;
import java.security.NoSuchAlgorithmException;
import java.security.PrivateKey;
import java.security.PublicKey;
import java.security.spec.InvalidKeySpecException;
import java.security.spec.PKCS8EncodedKeySpec;
import java.security.spec.X509EncodedKeySpec;
public class KryptoUtil {
private static final String ALGORITHM = "RSA";
private KeyPair generateKeyPairs() {
KeyPair keyPair = null;
KeyPairGenerator keyGen;
try {
```

```
keyGen = KeyPairGenerator.getInstance(ALGORITHM);
keyGen.initialize(1024);
keyPair = keyGen.genKeyPair();
} catch (NoSuchAlgorithmException e) {
e.printStackTrace();
}
return keyPair;
}
public String storeKeyPairs(String dirPath,String PrivateKey,String PublicKey) {
KeyPair keyPair = generateKeyPairs();
PrivateKey privateKey = keyPair.getPrivate();
PublicKey publicKey = keyPair.getPublic();
storeKeys(dirPath + File.separator + PublicKey+".key", publicKey);
storeKeys(dirPath + File.separator + PrivateKey+".key", privateKey);
return "success";
}
private void storeKeys(String filePath, Key key) {
byte[] keyBytes = key.getEncoded();
OutputStream outStream = null;
try {
outStream = new FileOutputStream(filePath);
outStream.write(keyBytes);
} catch (Exception e) {
e.printStackTrace();
} finally {
 if (outStream != null) {
 try {
outStream.close();
} catch (IOException e) {
e.printStackTrace();
}
}
}
}
private byte[] getKeyData(String filePath) {
File file = new File(filePath);
byte[] buffer = new byte[(int) file.length()];
FileInputStream fis = null;
try {
fis = new FileInputStream(file);
fis.read(buffer);
```

```
} catch (FileNotFoundException e) {
e.printStackTrace();
} catch (IOException e) {
e.printStackTrace();
} finally {
 if (fis != null) {
 try {
fis.close();
} catch (IOException e) {
e.printStackTrace();
}
}
}
return buffer;
}
 public PrivateKey getStoredPrivateKey(String filePath) {
PrivateKey privateKey = null;
byte[] keydata = getKeyData(filePath);
PKCS8EncodedKeySpec encodedPrivateKey = new PKCS8EncodedKeySpec(keydata);
KeyFactory keyFactory = null;
 try {
keyFactory = KeyFactory.getInstance("RSA");
} catch (NoSuchAlgorithmException e) {
e.printStackTrace();
}
try {
privateKey = keyFactory.generatePrivate(encodedPrivateKey);
} catch (InvalidKeySpecException e) {
e.printStackTrace();
}
return privateKey;
}
public PublicKey getStoredPublicKey(String filePath) {
PublicKey publicKey = null;
byte[] keydata = getKeyData(filePath);
KeyFactory keyFactory = null;
try {
keyFactory = KeyFactory.getInstance("RSA");
} catch (NoSuchAlgorithmException e) {
e.printStackTrace();
}
```

```
X509EncodedKeySpec encodedPublicKey = new X509EncodedKeySpec(keydata);
try {
publicKey = keyFactory.generatePublic(encodedPublicKey);
} catch (NullPointerException npe) {
npe.printStackTrace();
} catch (InvalidKeySpecException e) {
e.printStackTrace();
}
return publicKey;
}
}
```

Elektron Raqamli Imzo yaratish

```
package Fahim;
import Fahim.KryptoUtil;
import java.io.File;
import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.IOException;
import java.security.InvalidAlgorithmParameterException;
import java.security.KeyException;
import java.security.NoSuchAlgorithmException;
import java.security.PrivateKey;
import java.security.PublicKey;
import java.util.Collections;
import javax.xml.crypto.MarshalException;
import javax.xml.crypto.dsig.CanonicalizationMethod;
import javax.xml.crypto.dsig.DigestMethod;
import javax.xml.crypto.dsig.Reference;
import javax.xml.crypto.dsig.SignatureMethod;
import javax.xml.crypto.dsig.SignedInfo;
import javax.xml.crypto.dsig.Transform;
import javax.xml.crypto.dsig.XMLSignature;
import javax.xml.crypto.dsig.XMLSignatureException;
import javax.xml.crypto.dsig.XMLSignatureFactory;
import javax.xml.crypto.dsig.dom.DOMSignContext;
import javax.xml.crypto.dsig.keyinfo.KeyInfo;
import javax.xml.crypto.dsig.keyinfo.KeyInfoFactory;
import javax.xml.crypto.dsig.keyinfo.KeyValue;
import javax.xml.crypto.dsig.spec.C14NMethodParameterSpec;
import javax.xml.crypto.dsig.spec.TransformParameterSpec;
import javax.xml.parsers.DocumentBuilderFactory;
```

```
import javax.xml.parsers.ParserConfigurationException;
import javax.xml.transform.Transformer;
import javax.xml.transform.TransformerConfigurationException;
import javax.xml.transform.TransformerException;
import javax.xml.transform.TransformerFactory;
import javax.xml.transform.dom.DOMSource;
import javax.xml.transform.stream.StreamResult;
import org.w3c.dom.Document;
import org.xml.sax.SAXException;
public class XmlDigitalSignatureGenerator {
private Document getXmlDocument(String xmlFileI
Document doc = null;
DocumentBuilderFactory dbf = DocumentBuilderFactory.newInstance();
dbf.setNamespaceAware(true);
try {
doc = dbf.newDocumentBuilder().parse(new FileInputStream(xmlFilePath));
} catch (ParserConfigurationException ex) {
ex.printStackTrace();
} catch (FileNotFoundException ex) {
ex.printStackTrace();
} catch (SAXException ex) {
ex.printStackTrace();
} catch (IOException ex) {
ex.printStackTrace();
}
return doc;
}
private KeyInfo getKeyInfo(XMLSignatureFactory xmlSigFactory, String publicKeyPath) {
KeyInfo keyInfo = null;
KeyValue keyValue = null;
PublicKey publicKey = new KryptoUtil().getStoredPublicKey(publicKeyPath);
KeyInfoFactory keyInfoFact = xmlSigFactory.getKeyInfoFactory();

try {
keyValue = keyInfoFact.newKeyValue(publicKey);
} catch (KeyException ex) {
ex.printStackTrace();
}
keyInfo = keyInfoFact.newKeyInfo(Collections.singletonList(keyValue));
 return keyInfo;
}
```

```
 private void storeSignedDoc(Document doc, String destnSignedXmlFilePath) {
TransformerFactory transFactory = TransformerFactory.newInstance();
Transformer trans = null;
try {
trans = transFactory.newTransformer();
} catch (TransformerConfigurationException ex) {
ex.printStackTrace();
}
 try {
StreamResult streamRes = new StreamResult(new File(destnSignedXmlFilePath));
 trans.transform(new DOMSource(doc), streamRes);
} catch (TransformerException ex) {
ex.printStackTrace();
}
System.out.println("XML file with attached digital signature generated successfully ...");
}
public void generateXMLDigitalSignature(String originalXmlFilePath,
String destnSignedXmlFilePath, String privateKeyFilePath, String publicKeyFilePath) {
Document doc = getXmlDocument(originalXmlFilePath);
XMLSignatureFactory xmlSigFactory = XMLSignatureFactory.getInstance("DOM");
PrivateKey privateKey = new KryptoUtil().getStoredPrivateKey(privateKeyFilePath);
DOMSignContext domSignCtx = new DOMSignContext(privateKey, doc.getDocumentElement());
Reference ref = null;
SignedInfo signedInfo = null;
try {
ref = xmlSigFactory.newReference("", xmlSigFactory.newDigestMethod(DigestMethod.SHA1, null),
Collections.singletonList(xmlSigFactory.newTransform(Transform.ENVELOPED,
(TransformParameterSpec) null)), null, null);
signedInfo = xmlSigFactory.newSignedInfo(
xmlSigFactory.newCanonicalizationMethod(CanonicalizationMethod.INCLUSIVE,
(C14NMethodParameterSpec) null),
 xmlSigFactory.newSignatureMethod(SignatureMethod.RSA_SHA1, null),
Collections.singletonList(ref));
} catch (NoSuchAlgorithmException ex) {
ex.printStackTrace();
} catch (InvalidAlgorithmParameterException ex) {
ex.printStackTrace();
}
KeyInfo keyInfo = getKeyInfo(xmlSigFactory, publicKeyFilePath);
XMLSignature xmlSignature = xmlSigFactory.newXMLSignature(signedInfo, keyInfo);
 try {
```

```
xmlSignature.sign(domSignCtx);
} catch (MarshalException ex) {
ex.printStackTrace();
} catch (XMLSignatureException ex) {
ex.printStackTrace();
}
storeSignedDoc(doc, destnSignedXmlFilePath);
}
}
```

Elektron raqamli imzoni tasdiqlash

```
package Fahim;
import Fahim.KryptoUtil;
import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.IOException;
import java.security.PublicKey;
import javax.xml.crypto.dsig.XMLSignature;
import javax.xml.crypto.dsig.XMLSignatureFactory;
import javax.xml.crypto.dsig.dom.DOMValidateContext;
import javax.xml.parsers.DocumentBuilderFactory;
import javax.xml.parsers.ParserConfigurationException;
import org.w3c.dom.Document;
import org.w3c.dom.NodeList;
import org.xml.sax.SAXException;
public class XmlDigitalSignatureVerifier {
private static Document getXmlDocument(String xmlFilePath) {
Document doc = null;
DocumentBuilderFactory dbf = DocumentBuilderFactory.newInstance();
dbf.setNamespaceAware(true);
try {
doc = dbf.newDocumentBuilder().parse(new FileInputStream(xmlFilePath));
} catch (ParserConfigurationException ex) {
ex.printStackTrace();
} catch (FileNotFoundException ex) {
ex.printStackTrace();
} catch (SAXException ex) {
ex.printStackTrace();
} catch (IOException ex) {
ex.printStackTrace();
}
return doc;
```

```
}
public static boolean isXmlDigitalSignatureValid(String signedXmlFilePath,
String pubicKeyFilePath) throws Exception {
boolean validFlag = false;
Document doc = getXmlDocument(signedXmlFilePath);
NodeList nl = doc.getElementsByTagNameNS(XMLSignature.XMLNS, "Signature");
if (nl.getLength() == 0) {
throw new Exception("No XML Digital Signature Found, document is discarded");
}
PublicKey publicKey = new KryptoUtil().getStoredPublicKey(pubicKeyFilePath);
DOMValidateContext valContext = new DOMValidateContext(publicKey, nl.item(0));
XMLSignatureFactory fac = XMLSignatureFactory.getInstance("DOM");
XMLSignature signature = fac.unmarshalXMLSignature(valContext);
validFlag = signature.validate(valContext);
return validFlag;
}
}
```