O’ZBEKISTON RESPIBLIKASI OLIY VA O’RTA MAXSUS TA’LIM VAZIRLIGI

NAMANGAN DAVLAT UNIVERSITETI

FIZIKA MATEMATIKA FAKULTETI

5130200-AMALIY MATEMATIKA VA INFORMATIKA YO’NALISHI

4-BOSQICH 405-GURUH TALABASI

AHMEDOVA G. Q. NING

“Kriptografik masalalarni yechishda bir tomonlama funksiyalarni qo’llanilishi”

MAVZUSIDAGI

BITIRUV MALAKAVIY ISHI

NAMANGAN – 2015

O’ZBEKISTON RESPUBLIKASI OLIY VA O’RTA MAXSUS TA’LIM VAZIRLIGI

NAMANGAN DAVLAT UNIVERSITETI

FIZIKA-MATEMATIKA FAKULTETI

AMALIY MATEMATIKA KAFEDRASI

“DAK ga tavsiya etaman”
Fizika-matematika
fakulteti dekani_____
f-m.f.n. A.Mirzamov
“___”_____2015 yil

“Kriptografik masalalarni yechishda bir tomonlama funksiyalarni qo’llanilishi”

BITIRUV MALAKAVIY ISH

Bajardi:«**Amaliy matematika va informatika**»
ta’lim yo’nalishi bitiruvchi 4-kurs talabasi
Ahmedova G.Q _____
Rahbar: Q.G’oziyev
_____

Bitiruv malakaviy ishi kafedradan dastlabki himoyadan o’tdi. Kafedraning__ sonli bayonnomasi.
«____» _____2015 yil.

Namangan – 2015

NAMANGAN DAVLAT UNIVERSITETI

FIZIKA MATEMATIKA FAKULTETI
513200 – AMALIY MATEMATIKA VA INFORMATIKA YO'NALISHI

BITIRUV MALAKAVIY ISH BO'YICHA TOPSHIRIQ

Talaba: _____

1. Bitiruv malakaviy ishining mavzusi: _____
_____
_____

Bitiruv malakaviy ishining mavzusi universitet rektorining 2014 yil «2» dekabrdagi 183 A/C-sonli buyrug'i bilan tasdiqlangan.

2. Bitiruv malakaviy ishni dastlabki himoyaga topshirish muddati "____" _____ 2015 yil.

3. Tavsiya etilayotgan asosiy adabiyotlar:
_____
_____
_____
_____
_____

4. Ishning dolzarbligi:
_____
_____
_____
_____
_____
_____
_____

5. Ishning maqsadi:
_____
_____
_____
_____
_____
_____
_____
_____

6. Bitiruv malakaviy ishi bo'yicha maslahatlar:

№	Bo'lim mavzusi	Maslahatchi o'qituvchilarning F.I.SH.	Topshiriq berildi		Topshiriq bajarildi	
			Sana	Imzo	Sana	Imzo

7. Bitiruv malakaviy ishni bajarish rejasi:

№	Bitiruv malakaviy ishning bosqichlari	Bajarish muddati	Bajarilganlik belgisi

Bitiruv malakaviy ishi rahbari: ______________________________ ________________

(F.I.Sh.) (imzo)

Kafedra mudiri: ______________________________ ________________

(F.I.Sh.) (imzo)

Topshiriqni bajarish uchun oldim,

Talaba: ______________________________ ________________

(F.I.Sh.) (imzo)

Topshiriq berilgan sana ______________________

Namangan Davlat universiteti

Fizika - matematika fakulteti Amaliy matematika va informatika yo‘nalishi 4 kurs 405- guruh talabasi Ahmedova Gavharning “Kriptografik masalani yechishda bir tomonlama funksiyadan foydalanish” mavzusidagi bitiruv malakaviy ishiga ilmiy rahbar Q.G’oziyevning

X U L O S A S I

Ilmiy raxbar: **Q.G’oziyev**

Amaliy matematika kafedrasining 2015yil ___ iyunda bo‘lib o‘tgan

№ ___ - sonli yig‘ilishi bayonnomasidan

KO‘CHIRMA

Kun tartibi: Bitiruv malakaviy ishlarni himoyaga tavsiya etish.

1. Kafedra mudiri N.Otaxanov talaba Ahmedova Gavharning “Kriptografik masalani yechishda bir tomonlama funksiyadan foydalanish” mavzusidagi bitiruv malakaviy ishini taqdim etdi.

2. Ahmedova Gavhar bitiruv malakaviy ishining mohiyatini qisqacha bayon etdi. (Bitiruv malakaviy ishning mavzusi va unda ko‘rilgan ilmiy muammolar hamda ularning yechimi haqida).

1.Savollar:

3. Talabaning ilmiy rahbari Q.G’oziyev talaba Ahmedova Gavhar haqida ko‘pgina ijobiy fikrlar bildirdi. Bitiruv malakaviy ishning amaldagi Nizomga mos kelishini va Davlat attestatsiya komissiyasi huzurida himoya qilish uchun tavsiya etishlarini so‘radi.

Kafedra yig‘ilishi qaror qiladi:

1. “ Kriptografik masalani yechishda bir tomonlama funksiyadan foydalanish ” bajarilgan Bitiruv malakaviy ishini DAK da himoya etish uchun tavsiya etilsin.

2. Bitiruv malakaviy ishi ichki taqriz uchun amaliy matematika kafedrasi_____, tashqi taqriz uchun NamMTIning Oliy matematika kafedrasi dotsenti _____larga yo‘llansin.

Kafedra mudiri: N.Otaxanov

O‘ZBEKISTON RESPUBLIKASI

OLIY VA O‘RTA MAXSUS TA’LIM VAZIRLIGI

NAMANGAN DAVLAT UNIVERSITETI

FIZIKA-MATEMATIKA FAKULTETI

5130200 – Amaliy matematika va informatika yo‘nalishi

405-guruh bitiruvchisi AHMEDOVA GAVHAROY QAHRAMON QIZI ning

«Kriptografik masalalarni yechishda bir tomonlama funksiyalarni qo’llanilishi»

mavzusidagi

BITIRUV MALAKAVIY ISHI

Ilmiy raxbar: Q.G’oziyev

Namangan 2015

Mavzu: Kriptografik masalalarni yechishda bir tomonli funksiyalarni qo’llash.

Reja:

I.Kirish.

1.1 Mavzuni dolzarbligi va ahamiyati.

1.2 BMIni maqsadi va vazifalari.

1.3 Ishdagi ilmiy yangiliklar va erishilgan natijalar.

1.4 BMIni tuzilishi haqida umumiy ma’lumotlar.

II.Asosiy qism.

2.1 Kriptografiyaga asoslari.

2.2 Simmetrik kriptosistemalar.

2.3 Nosimmetrik kriptosistemalar.

2.4 Bir tomonli funksiyalar.

2.5 Elektron raqamli imzo.

2.6 Kriptosistemalar muammolari va kelajakdagi vazifalari.

III. Xulosa.

IV. Ilovalar.

V. Foydalanilgan adabiyot va internet resurslari.

VI. Mundarija.

I.Kirish.

O‘zbekiston Respublikasi mustaqillik yillari axborotlashtirish sohasida inqilobiy o‘zgarishlar davrini boshdan kechirmoqda. Zamonaviy axborot-kommunikatsiya texnologiyalari qulayliklar yaratish bilan bir qatorda yangi muammolarni ham o‘rtaga qo‘ymoqda. Axborot bazalarida saqlanadigan va telekommunikatsiya tizimlarida aylanayotgan axborot xavfsizligiga tahdid keskin oshmoqda. Keyingi vaqtlarda, ayniqsa, Internet paydo bo‘lgandan boshlab, axborot o‘girlash, axborot mazmunini egasidan ruxsatsiz o‘zgartirib qo‘yish, tarmoq va serverlardan beruxsat foydalanish, tarmoqqa tajovuz qilish hollari dunyo miqyosida ko‘paydi.

Ko‘pgina rivojlangan davlatlar axborot–telekommunikatsiya tarmoqlarida maxfiy axborotlarni xavfsiz uzatish va elektron raqamli imzo yaratishda o‘z milliy standartlaridan foydalanmoqdalar. Bunday standartlar AQSH, Rossiya, Koreya, Germaniya va bir qancha davlatlarda ishlab chiqilgan. Alohida ta’kidlash lozimki, horijga eksport qilinadigan dasturiy mahsulotlarda milliy standartlar qo‘llanilmaydi, yetarli darajada bardoshlilikka ega bo‘lmagan kriptografik vositalar qatnashadi. Ana shu sabablar O‘zbekiston Respublikasida ham milliy kriptografik algoritmlarni yaratish va ularni takomillashtirish muammolarini dolzarb qilib qo‘ydi. Bu muammoni hal etish uchun axborot xavfsizligini ta’minlashning ilmiy asosi bo‘lgan kriptologiyani rivojlantirish zaruriyati paydo bo‘ldi.

Aloqa kanallari orqali axborot xavfsizligini ta’minlab saqlash va uzatish tizimlarini yaratish hamda tahlil qilish bilan kriptologiya fani shug‘ullanadi. Kriptologiya grekchada kryptos –“sirli” va logos -“xabar” (axborot) degan ma’noni anglatadi.

O‘zbekiston Respublikasida kriptografiya sohasida ilmiy tadqiqotlar boshlanganiga hali ko‘p bo‘lgani yo‘q. Respublikada O‘zbekiston aloqa va axborotlashtirish agentligining Fan-texnika va marketing tadqiqotlari markazi olimlari birinchilardan bo‘lib kriptografiya yo‘nalishi bo‘yicha ilmiy tadqiqotlarni boshlab yubordilar. 1974 yilda o‘zbek olimi O‘zbekistonda xizmat ko‘rsatgan fan

arbobi professor Xasanov Po‘lat Fattoxovich tomonidan taklif etilgan diamatritsalar algebrasini Xasanov Xislat Po‘latovich tomonidan kriptografiya masalalarini yechish uchun takomillashtirilib topilgan parametrli algebra ishlab chiqildi. Buning natijasida Fan-texnika va marketing tadqiqotlari markazining bosh ilmiy xodimi Xasanov P.F. rahbarligida 2002 yilda kriptografiya bo‘yicha birinchi patentga talabnoma berildi. Bu patent 2006 yilda O‘zbekiston Respublikasi davlat patent idorasi tomonidan registratsiya qilindi va «Raqamli imzoni shakllantirish va autentifikatsiya usuli» ixtirosi uchun 03070-sonli patent berildi.

03070-sonli «Raqamli imzoni shakllantirish va autentifikatsiya usuli» patenti g‘oyalari Fan-texnika va marketing tadqiqotlari markazi xodimlari tomonidan ishlab chiqilgan O‘zbekiston Respublikasining kriptografiya sohasidagi dastlabki davlat standartlariga asos bo‘ldi. O’z DSt 1092:2005 «Axborot texnologiyasi. Axborotning kriptografik muxofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari», DSt 1105:2006 «Axborot texnologiyasi. Axborotning kriptografik muxofazasi. Ma’lumotlarni shifrlash algoritmi», DSt 1106:2006 «Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Xeshlash funksiyasi» shular jumlasidandir.

Kriptografiya yo‘nalishini rivojlantirishga davlatimiz tomonidan ham katta ahamiyat berilmoqda. Bunga keyingi yillarda qabul qilingan bir nechta qonun va meyoriy hujjatlar, jumladan, «Axborotlashtirish», «Elektron raqamli imzo», «Elektron hujjat aylanishi» to‘grisidagi qonunlar, Prezidentimizning 2007 yil 3 aprelda qabul qilgan «O‘zbekiston Respublikasida axborotning kriptografik himoyasini tashkil etish chora-tadbirlari» to‘grisidagi qarori misol bo‘lishi mumkin.

1.1 Mavzuni dolzarbligi va ahamiyati.

Sir emas, internet va yuqori texnologiyalardan foydalanish bugungi kun odamining odatiy ehtiyojlaridan biriga aylangan. Hozir dunyo bo`ylabaylanayotgan axborot miqdorining oshib, borayotgani hisobiga uning foydali va zararli tomonlari ham ko`rinib qolmoqda. Ayni paytda bunda xavfsizlikka egabo`lish, uni ta`minlash chora – tadbirlarini ham e`tibordan chetda qoldirmaslik zarur. Negaki, so`nggi o`n yillikda dunyodagi kiberxavfsizlik tushunchasi batomom o`zgardi, qachonlardir bir xakerning nojuya hatti – harakatlari sifatida e`tirof etilgan kiberxurujlar bugungi kunga kelib kompleks shaklga ega bo`ldi va chinakam tahdid ko`rinishini oldi. Shu bois o`z muhim axborotlarini kiberxurujlardan himoya qilishni istagan davlatda bu boradagi dasturlar keng ko`lamda tadbiq etilmoqdaki, buning natijasi o`laroq, kibermakon xavflariga ongli ravishda qarshi ko`rashishga erishish maqsad qilinmoqda. Tabiiyki, bunday sharoitda axborot xavfsizligi masalasi dolzarb ahamiyatga ega. Shuning uchun, axborot xavfsizligi masalasiga jiddiy qarashimiz, uning tarixi, qo`llanilgan usullari va erishgan yutuqlari bilan tanishib borishimiz muhim hisoblanar ekan.

1.2 BMIni maqsadi va vazifalari.

Ushbu bitiruv malakaviy ishi mavzusi orqali axborotlar xavfsizligi muammolari, axborotlashgan jamiyatda elektron axborotlardan foydalanish va uni himoya qilish qanchalik muhim va ahamiyatga ekanligini yoritish,kriptografiyaning axborotlarni himoyalashning usullaridan biri “Simmetrik, Nosimmetrik” usulida matnlarni shifrlash va deshifrlash dasturini yaratish’ mavzusini tahlil qilgan holda, ushbu himoyalash usulini batafsil bayon etish va ta`limiy xarakterdagi dasturiy mahsulotni yaratish asosiy maqsadimizdir.

Ishning vazifasi. Mavzu doirasida axborotlashgan jamiyatda elektron axborotlar xavfsizligini ta`minlash muhimligi va uning asosiy tushunchalarini tavsiflagach, matnlarni RSA usuli orqali shifrlash va deshifrlash tizimi hamda u orqali matnlarni himoyalashga doir tahlillarimizni hamda dasturiy ta`minotni yaratishga doir tadqiqotlarimizni bayon qilamiz.

1.3 Ishdagi ilmiy yangiliklar va erishilgan natijalar.

Biz o`z bitiruv malakaviy ishimizda axborotlarni Bir tomonlama funksiyalardan usuli orqali shifrlash va deshifrlashni tahlil qilib, ta`limiy xarakterdagi dasturiy mahsulotni yaratishga e`tiborni qaratishni maqsad qilib oldik. Bu orqali, axborot xavfsizligini ta`minlash bo`yicha ta`limiy xarakterdagi ma`lumot va dasturiy mahsulot yuzaga keladi. Chunki, har qanday kriptotizim uslubi bayoni va matnlarni kompyuter texnikasidan foydalangan holda shifrlash va deshifrlash dasturi, kriptografiyani rivojlanishi uchun amaliy ahamiyatga ega hisoblanadi.

Ishning ilmiy yangiligi. Axborot xavfsizlini ta`minlash bo`yicha ta`limiy xarakterdagi har qanday kriptotizim uslubining batafsil tavsifi va dasturiy tadbigi ilmiy ahamiyatga ega hisoblanadi.

**Tadqiqot ob`ekti va predmeti.** Kompyuter muhitida saqlanayotgan axborotlar va ularning xavfsizligini ta`minlashning kriptografik usullari.

1.4 BMIni tuzilishi haqida umumiy ma’lumotlar.

Bitiruv malakaviy ishi mavzusi: “ Kriptografik masalalarni yechishda bir tomonlama funksiyalardan foydalanish ” . Bitiruv malakaviy ishining umumiy tuzilishi quyidagicha:

KIRISH, ASOSIY QISM , XULOSA , ADABIYOTLAR , MUNDARIJA o’z navdatida KIRISH - Mavzuni dolzarbligi va ahamiyati, BMIni maqsadi va vazifalari, Ishdagi ilmiy yangiliklar va erishilgan natijalar, BMIni tuzilishi haqida umumiy ma’lumotlar sahifalaridan tashkil topgan. ASOSIY QISM – Kriptografiyaga asoslari, Simmetrik kriptosistemalar, Nosimmetrik kriptosistemalar, Bir tomonli funksiyalar, Elektron raqamli imzo, Kriptosistemalar muammolari va kelajakdagi vazifalari lardan iborat paragraflardan tashkil topgan. Bitiruv malakaviy ishini interaktivligini oshirish maqsadida ELEKTRON DARSLIK ham ishlab chiqildi. Bunda Diplom ish prezintatsiyasi, Dasturlar o’rin olgan. Bu dastur ishlashi uchun Kompyuterdan 256 mbayt tashqi xotira, 13 mbayt tezkor xotira internet explorer dasturlari talab qilinadi.

ASOSIY QISM

2.1 Kriptografiyaga asoslari.

Axborotlarni boshqalar o‘qishidan saqlash maqsadida maxsus kalit yordamida kodlashtirish *kriptografiya* deb ataladi. Kriptografiya uzoq yillar davomida xarbiy maqsadlarda qo’llanilib kelingan. ANB (Agenstvo natsionalnoy bezopastnosti (AQSH) 4 noyabr 1952yil tashkil topgan) AQSH prezidentining maxsus buyrug’iga binoan barcha chet davlatlardan kelayotgan xatlar va axborotlarni tekshiradi.

1995 yil 3 aprelda Rossiya prezidenti №334 qaroriga muvofiq turli xil litsenziyaga ega bo‘lmagan vositalar yordamida axborotlarni kodlashtirishni taqiqladi. Shundan keyin axborotlarni kodlashtirish bo‘yicha davlat standarti kiritildi.

Ochiq tekstni R xarfi bilan belgilaymiz. Bu tekst fayli, tasvir, maxsus tovush yoki h.k. bo’lishi mumkin. Bu axborotlar komp’yuterda ikkilik kod ko’rinishida ifodalanadi. Shifrlangan tekst S xarfi bilan belgilanadi.

SHifrtekstning xajmi ba’zan ochik tekst xajmiga teng bo’lishi mumkin. Shifrlangan tekst komp’yuter tarmog‘i kanallari bo’ylab uzatilishi yoki xotirada saqlanishi mumkin. Shifrlash funksiyasi E ni quyidagicha yozish mumkin.

$E(R)=S$

Shifrni ochish funksiyasini D harfi bilan belgilasak,

$D(S)=R$

$D(E(R))=R$

Kriptografiya quyidagi masalalarni yechilishini ta’minlashi kerak.

Autentifikatsiya - kabul qiluvchi shunga ishonch hosil kilishi kerakki ma’lumot aniq bir yuboruvchidan bo’lishi shart. Boshqa bir nom bilan yolg’on ma’lumot yuborilmasligi kerak;

Butunlik - uzatish paytida axborot o‘zgarmasligi;

Inkor qilmaslik (neosporimost) -ma’lumotni yuboruvchi o‘zi ekanini tasdiqlashi.

XX asrning oxiri va XXI asrning boshlarida kishilik jamiyatida axborotning ahamiyati keskin ravishda ortib ketdi. Insonning har bir sohadagi faoliyatini takomillashtirish va osonlashtirishga qaratilgan zamonaviy jamiyatda axborot mahsulot yoki xom ashyo sifatida borgan sari katta qiymatga ega bo‘lib bormoqda.

Keyingi yillarda kompyuter sanoatining rivojlanishi va inson hayotiga tobora chuqurroq kirib borishi natijasida axborotni ishlab chiqarish, saqlash, qayta ishlash, tahlil qilish, uzatishga bo‘lgan ehtiyoj ortib bormoqda. Oqibatda ana shu axborotlarning xavfsizligini ta’minlash informatikaning eng dolzarb muammolaridan biriga aylanib ulgurdi. Kompyuterning tarmoq texnologiyalarining jadal rivojlanishi esa bu muammoning ahamiyatini yanada oshirib yubordi.

Axborotlarni kriptografik usulda himoya qilish yuzaga kelgan muammmolarni hal qilishda muhim o‘rin tutadi.

Axborotlarni kriptografik himoya qilishda ularning mazmunini yashirish yoki begonalar tomonidan foydalanishning oldini olish maqsadida axborot maxsus funksional akslantirish yordamida bir ko‘rinishda boshqa ko‘rinishga o‘tkaziladi. Bu amalning turli usullarini ishlab chiqish uchun amaliy matematikaning yangi bir yo‘nalishi-kriptografiya yuzaga keldi va rivojlanib bormoqda.

Kriptografiya — bu axborotlarni kriptografik himoya qilishning turli model va metodlari, algoritmlari, dasturiy va texnik vositalarini ishlab chiqish hamda bunday himoya samarasini baholashni o‘rganuvchi fan hisoblanadi.

Rivojlangan davlatlarda talabalarga kriptografiya fani bo‘yicha XX asrning 80-yillaridan boshlab nazariy va amaliy mashg‘ulotlar olib boriladi.Yangidan-yangi mutaxassisliklar joriy qilinmoqda. Masalan, Rossiyada ikkita yo‘nalishda - 013200 — Kriptografiya ("matematik" kvalifikatsiyasi bilan) hamda 220600 — axborotlarni himoya qilishni tashkil qilish va uning texnologiyalari bo‘yicha mutaxassislarni tayyorlash yo‘lga qo‘yildi. Belorussiyada banklar, moliya va sug‘urta korxonalari, katta firmalar, davlat va nodavlat tashkilotlarida axborotni himoyalashga bo‘lgan ehtiyoj tufayli II.08.01.14 — Kriptografiyani matematik va

dasturiy ta’minlash hamda axborotlarni tahlil qilish ("matematik-programmist" kvalifikatsiyasi bilan) mutaxassislarni tayyorlash boshlandi. “Axborotlarni himoya qilishni tashkil etish” nomli davriy jurnalini chop qilish yo‘lga qo‘yildi.

1995 yildan boshlab, Bizning Respublikamizda ham informatsion jarayonlar bilan bog‘liq bo‘lgan barcha mutaxassislar uchun kriptografiya faniga Davlat ta’lim standartlari va Namunaviy dasturlarda alohida e’tibor berilmoqda. Bu borada, Amaliy matematika, Informatika va axborot texnologiyalari, huquqshunoslik kabi yo‘nalishlardan bu fan alohida o‘rin tutadi. Toshkent axborot texnologiyalari universitetida shu yo‘nalishda bakalavr va magistrlarni tayyorlash boshlandi.

Kriptografik algoritmlar, algoritmlarning murakkabligi, ularning matematik asoslarini o‘rganish va amaliyotga tatbiq etish masalasi o‘z echimini kutib turgan muammolardan biri hisoblangan. Ularni to‘g‘ri hal qilish axborotlarni himoya qilish jarayonini mukammalashtiribgina qolmay, Oliy ta’lim muassasalarida bo‘lajak mutaxassislarning tayyorgarlik darajasini oshirishda muhim asos bo‘lib xizmat qilishi mumkin.

Bizning bitiruv malakaviy ishimiz xam ana shu muammolarning bir qismini imkoniyat darajasida o‘rganishga qaratilganligi uchun ham dolzarb hisoblanadi.

Mazkur bitiruv malakaviy ishi kirish, asosiy qism, amaliyotga tatbiq etish va hulosalar kabi 6 ta bobni o‘z ichiga olgan bo‘lib, jami .... sahifadan iborat.

2.1.1 Kriptografiya bo‘yicha boshlang‘ich ma’lumotlar

Kriptografiya haqidagi ma’lumotlarni uning atamashunosligiga oid ayrim terminlar mazmunini ochib berishdan boshlaymiz.

Axborotlarni himoya qilish — bu tarmoqdagi aloqa hamda axborotlarning uzluksizligi, yaxlitligi va mahfiyligini ta’minlovchi barcha vosita va amallar mamuasi bo‘lib, nosozliklardan asrovchi vosita va funksiyalarni o‘z ichiga olmaydi. Axborotlarni himoya qilish kriptografiya, kriptoanaliz (kriptotahlil) va kompyuterlarga ruhsatsiz kirishdan saqlash kabi bo‘limlarni o‘z ichiga oladi.

Kriptografiya – amaliy matematikaning bir bo‘limi bo‘lib, axborotlarni mazmunini yashirish yoki ruxsatsiz foydalanishdan asrash maqsadida axborotlarni bir ko‘rinishdan boshqa ko‘rinishga o‘tkazish uchun mo‘ljallangan modellar, metodlar, algoritm, dasturiy va texnik vositalarni o‘rganadi.

Kriptosistema — bu axborotlarni kriptografik almashtirilishini dasturiy, texnik yoki dasturiy-texnik usullar yodamida amalga oshiruvchi tizimdir.

Kriptoanaliz (kriptotahlil) — bu amaliy matematikaning bitta bo‘limi bo‘lib, kiruvchi yoki chiquvchi signallardan foydalanib maxfiy parametrlarni aniqlab olish (yashirin matnni ochish) maqsadida kriptosistemalarni tahlil qilishga qaratilgan usul, model, algoritm, dasturiy va texnik vositalarni o‘rganadi.

Yuqoridagi ma’lumotlardan ko‘rinib turibdiki, kriptoanaliz matematik ma’noda kriptografiyaga teskari bo‘lgan masalalar bilan shug‘ullanadi. Kriptografiya va kriptoanaliz birgalikda yangi fan — ***kriptologiyani*** tashkil qiladi.Kriptologiya tarixini uch bosqichdan iborat deb hisoblash mumkin.

Birinchi bosqich - (eng qadimgi davrlardan to 1949 yilgacha) tor doiradagi, hususiy xamda sodda hisoblashlardan iborat kriptografik va kriptotahlil algoritmlari bilan harakterlanadi va tabiiyki, kompyuterlardan foydalanishni nazarda tutmaydi. Bu bosqichni ko‘pincha kompyuterlargacha bo‘lgan davr deb ataladi.

Ikkinchi bosqich - (1949-1976) amaliyotchi matematik K. Shennonning “Mahfiy tizimlarda bog‘lanish nazariyasi” nomli ilmiy ishining chop etilishi bilan

boshlanadi. Bu davrda EHM lardan foydalangan holda kriptologik izlanishlar keng miqyosda olib borildi. Kriptologiya matematik fanga aylandi. Ammo, bu fan mevalaridan faqat diplomatik va harbiy tashkilotlarning aloqa xizmati foydalangani uchun, kriptologiya "yopiq" (mahfiy) fan bo‘lib qoldi.

Uchinchi bosqich - (1976 yildan hozirgi davrgacha) kriptologiya ochiq fanga aylandi. Bu jarayon amerikalik matematik U. Diffi, M. Xellmanlarning "Kriptografiyadagi yangi yo‘nalishlar" ilmiy ishining chop etilishidan boshlandi. Bu ishda “mahfiy” ma’lumotlarni “yopiq kalitlarsiz”, ya’ni ochiq usulda uzatish mumkinligi (K. Shennon ishlaridan aynan shu jihati bilan farqlanadi) ko‘rsatildi. Bu bosqichda kriptografik usullar amaliyotda ommaviy ravishda qo‘llana boshlandi. Bu holatni bank ishida, kompyuter tarmoqlarida (masalan, Internet da) va boshqa bir qator sohalarda kuzatish mumkin bo‘ldi. Masalan, AQSH da bir yilda kriptologiyaga 15 mlrd. dollargacha mablag‘ sarf qilinadi.

Kriptologiya informatikaning fanining rivojlanishiga ham katta ta’sir ko‘rsata boshladi.

Zamonaviy kriptologiya matematikaning ehtimollar nazariyasi, matematik statistika, algebra, sonlar nazariyasi, algoritmlar nazariyasi, hisoblashlarning murakkabligi kabi sohalari bilan chambarchas bog‘langan. Shifrlash jarayonini avtomatlashtirish uchun shifrlash qurilmasi deb ataluvchi maxsus va o‘ta kuchli kompyuterlar ishlab chiqildi. G‘arbiy mamlakatlarda ***B-CRYPT, IBM-4755, Datacryptor*** kabi shifrlash qurilmalaridan keng foydalaniladi. Kriptologiya tarixiga oid ayrim malumotlarni keltirib o‘tamiz.

Mesopotamiyada olib borilgan areologik qazish ishlarida eramizdan avvalgi XX asrga mansub bo‘lgan eng qadimiy shifrlangan matnlardan biri topildi. U sopol taxtachaga o‘yib yozilgan bo‘lib, sopol idishlarni bo‘yash uchun ishlatiladigan bo‘yoqning retsepti haqidagi matn bo‘lib chiqdi. XVII asrda kardinal Rishele tomonidan dunyoda birinchi bo‘lib, shifrlash xizmati tashkil qilindi. Nyuton, Eyler, Leybnits, Gauss, Kardano kabi buyuk matematiklar ham bevosita kriptologiya bilan shug‘ullanganlar. Kriptologiyada quyidagi atamalar qabul qilingan.

Xabarlar fazosi RT — barcha mumkin bo‘lgan xabarlarning ***pt*** fazosi. Shuningdek xabarlarni belgilash uchun ***m*** (message) dan ham foydalaniladi.

Kalitlar fazosi K. Xar bir $k \in K$ kalit *RT* fazodagi biror E_k (encryption) va unga teskari D_k (decryption) almashtirishni belgilaydi. ***.Shifrlangan xabarlar fazosi ST*** – barcha shifrlangan ***ct*** (ciphertext) $ct = E_k(pt)$ matnlarni o‘z ichiga oladi.

Odatda kriptosistemaga quyidagi talablar qo‘yiladi: 1) $E_k\{pt\}$, $D_k\{ct\}$ —lar oson hisoblanadigan bo‘lishi lozim; 2) ***k*** ni bilmay turib, ***ct*** ma’lum bo‘lgan taqdirda ham ***pt*** ni topishning iloji bo‘lmasin.

Klassik kriptosistemalarda ***k*** mahfiy kalit E_k va D_k akslantirishni belgilab beradi. Bunda quyidagi ayniyatning o‘rinli bo‘lishi talab qitlinadi:

$D_k(E_k(pt)) = D_k(ct)=pt.$ Kriptoanaliz bo‘yicha mutaxassisning asosiy vazifasi ana shu kalitni qidirishdan iborat. U quyidagi ko‘rinishlarda shifrlangan matnga hujum qilishi mumkin: 1) faqat shifrlangan matn ma’lum (ciphertext only attack); 2) shifrlangan va shifrlanmagan matnlar ma’lum (known plaintext attack); 3) $(pt,E_k(pt))$ juftlikni aniqlash imkoniyati mavjud va bu erda *pt* – kriptoanalitik tomonidan tanlanadi (chosen plaintext attack).

Axborotlarni kriptografik himoya qilishda, ya’ni axborotlarni ochiq va yopiq usullarda kriptografik shifrlashning turli algoritmlari mavjud bo‘lib, ularning asosini matematika fanining turli sohalarida ishlab chiqilgan mexanizmlar tashkil qiladi. Quyidagi jadvalda ana shunday algoritmlarning ayrimlarini va ularning matematik asosi keltirilgan.

Shifrlash algoritmi	Algoritmning matematik asosi
GOST-28147-89	Sanoq sistemalari, bo‘lish munosabatlari, darajaga ko‘tarish, ikkilik sanoq sistemasida amallar bajarish, mulohazalar algebrasi, munosabatlar, o‘rin almashtirishlar, sonlar nazariyasi
Ryukzak	Vektorlar algebrasi, qoldiqli bo’lish amali, gruppa, halqa, maydon, ikkilik sanoq sistemasi, mulohazalar algebrasi, munosabatlar, o‘rin almashtirishlar, sonlar nazariyasi
El-Gamal	Tub sonlar, logarifm, qoldiqlar nazariyasi, modul

	bo‘yicha ko‘paytirish
DES	Sanoq sistemalari, akslantirishlar, o‘rin almashtirishlar, mulohazalar algebrasi, munosabatlar, o‘rin almashtirishlar, sonlar nazariyasi
RIJNDAEL	Sanoq sistemalari, bo‘lish munosabatlari, darajaga ko‘tarish, ikkilik sanoq sistemasida amallar bajarish, mulohazalar algebrasi,
RSA	Tenglamalar yechimlarining mavjudligi. Bo‘lish munosabatlari, tub sonlar, tub ko‘paytuvchilarga ajratish, xalqa, mulohazalar algebrasi, munosabatlar, o‘rin almashtirishlar, sonlar nazariyasi.

Jadvaldan ko‘rinib turibdiki, axborotlarni kriptografik usul bilan himoya qilish uchun algebraning mulohazalar algebrasi, munosabatlar, o‘rin almashtirishlar, sonlar nazariyasiga oid va boshqa ma’lumotlaridan keng foydalaniladi.

2.2 Simmetrik kriptosistemalar.

Kriptografik tizim, yo qisqacha, kriptotizim shifrlash ham shifrni ochish algoritmlari, bu algoritmlarda ishlatiladigan kalitlar, shu kalitlarni boshqaruv tizimi hamda shifrlanadigan va shifrlangan matnlarning o‘zaro bog‘langan majmuasidir. Kriptotizimdan foydalanishda matn egasi shifrlash algoritmi va shifrlash kaliti vositasida avvalo dastlabki matnni shifrlangan matnga o‘giradi. Matn egasi uni o‘zi foydalanishi uchun shifrlagan bo‘lsa (bunda kalitlarni boshqaruv tizimiga hojat ham bo‘lmaydi) saqlab qo‘yadi va kerakli vaqtda shifrlangan matnni ochadi. Ochilgan matn asli (dastlabki matn)ga aynan bo‘lsa saqlab qo‘yilgan axborotning butunligiga ishonch hosil bo‘ladi. Aks holda axborot butunligi buzilgan bo‘lib chiqadi. Agar shifrlangan matn undan qonuniy foydalanuvchiga(oluvchiga) mo‘ljallangan bo‘lsa u tegishli manzilga jo‘natiladi. So‘ngra shifrlangan matn oluvchi tomonidan unga avvaldan ma’lum bo‘lgan shifr ochish kaliti va algoritmi vositasida dastlabki matnga aylantiriladi.

Bunda kalitni qanday hosil qilish, aloqa qatnashchilariga bu kalitni maxfiyligi saqlangan holda yetkazish, va umuman, ishtirokchilar orasida kalit uzatilgunga qadar xavfsiz aloqa kanalini hosil qilish asosiy muammo bo‘lib turadi. Bunda yana boshqa bir muammo – autentifikatsiya muammosi ham ko‘ndalang bo‘ladi. Chunki: Dastlabki matn (xabar) shifrlash kalitiga ega bo‘lgan kimsa tomonidan shifrlanadi. Bu kimsa kalitning haqiqiy egasi bo‘lishi ham, begona (mabodo kriptotizimning siri ochilgan bo‘lsa) bo‘lishi ham mumkin. Aloqa ishtirokchilari shifrlash kalitini olishganda u chindan ham shu kalitni yaratishga vakolatli kimsa tomonidan yo tajovuzkor tomonidan yuborilgan bo‘lishi ham mumkin.Bu muammolarni turli kriptotizimlar turlicha hal qilib beradi. Kriptotizimda axborotni shifrlash va uning shifrini ochishda ishlatiladigan kalitlarning bir-biriga munosabatiga ko‘ra ular bir kalitli va ikki kalitli tizimlarga farqlanadilar. Odatda barcha kriptotizimlarda shifrlash algoritmi shifr ochish algoritmi bilan aynan yo biroz farqli bo‘ladi. Kriptotizimning ta’bir joiz bo‘lsa "qulfning" bardoshliligi algoritm ma’lum bo‘lgan holda faqat kalitning himoya xossalariga, asosan kalit axborot miqdori(bitlar soni)ning kattaligiga bog‘liq deb

qabul qilingan. SHifrlash kaliti shifr ochish kaliti bilan aynan yo ulardan biri asosida ikkinchisi oson topilishi mumkin bo‘lgan kriptotizimlar simmetrik(sinonimlari: maxfiy kalitli, bir kalitli) kriptotizim deb ataladi.

Bunday kriptotizimda kalit aloqaning ikkala tomoni uchun bir xil maxfiy va ikkovlaridan boshqa hech kimga oshkor bo‘lmasligi shart. Bunday tizimning xavfsizligi asosan yagona maxfiy kalitning himoya xossalariga bog‘liq. Simmetrik kriptotizimlar uzoq o‘tmishga ega bo‘lsa-da, ular asosida olingan algoritmlar kompyuterlardagi axborotlarni himoyalash zarurati tufayli ba’zi davlatlarda standart maqomiga ko‘tarildilar. Masalan, AQSHda ma’lumotlarni shifrlash standarti sifatida 56 bitli kalit bilan ishlaydigan DES(Data Encryption Standart) algoritmi 1977 yilda qabul qilingan. Rossiya(sobiq SSSR)da unga o‘xshash standart (GOST 28147-89) sifatida 128 bitli kalit bilan ishlaydigan algoritm 1989 yilda tasdiqlangan. Bular dastlabki axborotni 64 bitli bloklarga bo‘lib alohida yoki bir-biriga bog‘liq holda shifrlashga asoslanganlar.

Algoritmlarning matematikaviy asosida axborot bitlarini aralashtirish, o‘rniga qo‘yish, o‘rin almashtirish va modul bo‘yicha qo‘shish amallari yotadi. Unda kirish va chiqishdagi matnlarning axborot miqdorlari deyarli bir xil bo‘ladi. Simmetrik kriptotizimni ishlashini bu kungi davrimizning Kumush va Otabeklari orasida elektron maktublar almashish misolida ko‘rib chiqamiz. pinhona aloqaga nisbatan tajovuzkor shaxsni Homid deb ataymiz.

Faraz qilaylikki, Otabek Kumushga pinhona maktub yo‘llamoqchi. Ular orasida aloqa boshlanguncha o‘zlarining yagona o‘zaro maxfiy kalit K nusxalarini bir-birlariga berib, maktubni faqat shifrlangan shaklda yuborishga kelishib qo‘ygan edilar. Otabek Kumushga m maktubini yozib, uni K kaliti bilan shifrlaydi. Natijada m maktubi shifrlangan matn C ga aylanadi. So‘ngra Otabek shifrlangan maktubni elektron pochta orqali Kumushga jo‘natadi. Kumush shifrlangan maktub C ni qabul qilib olgach uni o‘zidagi o‘zaro maxfiy kalit K bilan uning shifrini ochib Otabek yozgan m maktubiga aylantirib uni o‘qiydi. Aloqa kanali himoyalanmagan

bo‘lgani uchun bu maktub Homidning qo‘liga tushishi ham mumkin. Lekin, Homidda Kumush va Otabeklarning maxfiy kaliti bo‘lmagani uchun u xatning mazmunini bilaolmaydi va xatni o‘zgartirib qo‘yaolmaydi. Homidning qo‘lidan maktubni yo‘q qilib yuborishgina keladi xolos. Homid maktub mazmunini bilmay turib Otabek nomidan shifrlanmagan yoki biror kalit bilan shifrlangan maktub jo‘natsa ham, buning qalbaki ekanligi Kumushga darhol oshkor bo‘ladi. CHunki, xat shifrlanmay kelsa, bu pinhona xat almashish haqidagi ularning kelishuviga zid bo‘lib chiqadi. Agar xat Homiddagi boshqa kalit bilan shifrlanib kelsa, uni Kumush o‘zidagi va Otabekdagi maxfiy kalit nusxasi bilan ocha olmaydi va bu bilan xatning Otabekdan emasligini bilib oladi. Shifrlash algoritmi odatda barcha uchun oshkora bo‘ladi. Bunday tizimning xavfsizligi asosan maxfiy kalitning himoya xossalariga bog‘liq.

Simmetrik kriptotizimdan foydalanib elektron yozishmalar boshlash uchun avvalo maxfiy kalitni yoki parolni ikki aloqa ishtirokchisidan biri ikkinchisiga maxfiy holda etkazishi kerak. Maxfiy kalitni etkazish uchun maxfiy aloqa kanali(shaxsan uchrashish, himoyalangan aloqa kanali va sh.o‘.) kerak. Shunday qilib yopiq davra hosil bo‘ladi: maxfiy kalitni topshirish uchun maxfiy kanal kerak, maxfiy kanalni hosil qilish uchun maxfiy kalit kerak. Maxfiy kalit tez-tez o‘zgartirib turilsa (aslida, harbir yozishmaga alohida maxfiy kalit ishlatilganda eng yuqori maxfiylikka erishiladi) bu muammo doimo ko‘ndalang bo‘laveradi.

2.2.1 Simmetrik (maxfiy) kalitli shifrlash sistemasi. Simmetrik shifrlash algoritmida quyidagi usullardan keng foydalaniladi:

1. O`rin almashtirish shifri
2. Siljitish shifri.

O`rin almashtirish shifri oddiy shifrlash hisoblanib, bu usulda satr va ustundan foydalaniladi. Chunki shifrlash jadval asosida amalga oshiriladi. Birinchi bo`lib, shifrlash jadvalidan (XIV asrning oxirlarida) diplomatik munosabatlarda, xarbiy sohalarda axborotni muhofazalashda foydalanilgan.

***O`rin almashtirish shifri***. Almashtirish (podstanovka) usullarining mohiyati bir alfavitda yozilgan axborot simvollarini boshqa alfavit simvollari bilan ma`lum qoida bo`yicha almashtirishdan iboratdir. eng sodda usul sifatida **to`g'ridan-to`g'ri almashtirishni** ko`rsatish mumkin. Dastlabki axborot yoziluvchi A_0 alfavitning s_{0i} simvollariga shifrlovchi A_1 alfavitning s_{1i} simvollari mos quyiladi. Oddiy holda ikkala alfavit ham bir xil simvollar to`plamiga ega bo`lishi mumkin.

Ikkala alfavitdagi simvollar o`rtasidagi moslik ma`lum algoritm bo`yicha K simvollar uzunligiga ega bo`lgan dastlabki matn T_0 simvollarining raqamli ekvivalentlarini o`zgartirish orqali amalga oshiriladi.

Monoalfavitli almashtirish algoritmi quyidagi qadamlar ketma-ketligi ko`rinishda ifodalanishi mumkin

1-qadam. [1xR] o`lchamli dastlabki $A_0$ alfavitdagi har bir simvol $s_0 \in T$ ($i=\overline{1,K}$) ni $A_0$ alfavitdagi $s_{0i}$ simvol tartib raqamiga mos keluvchi $h_{0i}(s_{0i})$ conga almashtirish yo`li bilan raqamlar ketma-ketligi L_{0h} ni shakllantirish.

2-qadam. L_{0h} ketma-ketligining har bir sonini $h_{1i} =(k_1 x\ h_{0i}(s_{0i})+ k_2)(\text{mod } R)$ formula orqali hisoblanuvchi L_{1h} ketma-ketlikning mos soni h_{1i} ga almashtirish yo`li bilan $L_{1h}$ son ketma-ketligini shakllantirish, bu yerda $k_1$-o`nlik koeffitsent; k_2-siljitish koeffitsenti. Tanlangan k_1, k_2 koeffitsentlar h_{0i} h_{1i} sonlarning bir ma`noli mosligini ta`minlashi lozim, $h_{1i}=0$ olinganida esa $h_{1i}=R$ almashinuvi bajarilishi kerak:

3-qadam. L_{1h} ketma-ketlikning har bir soni $h_{1i}(s_{1i})$ni [1xR] o`lchamli shifrlash alfavitning mos $s_{1i} \in T_1$($i=\overline{1,K}$) cimvoli bilan almashtirish yo`li bilan T_1 shifrmatnni hosil qilish.

4-qadam. Olingan shifrmatn o`zgarmas b uzunlikdagi bloklarga ajratiladi. Agar oxirgi blok to`liq bo`lmasa blok orqasiga maxsus simvol-to`ldiruvchilar joylashtiriladi(masalan, *).

Misol. SHifrlash uchun dastlabki ma`lumotlar quyidagilar:

T_0=<HIMOYA_XIZMATI>

A_0=<ABVGDEYOJZIYKLMNOPRSTUFXTSCHSH’`EYUYAO`QG’H_>

A_1=<ORYO’YATE-JMCHXAVDYFQKSEZPITSGHL`SHBUYU QGN>

R=36; k_1=3; k_2=15; b=4

Algoritmning qadamba-qadam bajarilishi quyidagi natijalarni olinishiga olib keladi.

1-qadam. L_{oh}=<35,10,14,16,31,36,23,10,9,14,1,20,10>

2-qadam. L_{1h}=<12,9,21,17,36,14,12,9,6,21,18,3,9>

3-qadam. T_1=<XJEFNVHJTEQYOJ>

4-qadam. T_1=<XJEF NVHJ TEQYO J***>

Rasshifrovka qilishda bloklar birlashtirilib K simvolli shifrmatn T_1 hosil qilinadi. Rasshifrovka qilish uchun quyidagi butun sonli tenglamani echish lozim:

$k_1h_{01}+k_2=nR+h_{1i}$

k_1, k_2, h_{11} va R butun sonlar ma`lum bo`lganda h_{0i} kattaligi n ni saralash orqali hisoblanadi. Bu muolajani shifrmatnning barcha simvollariga tadbiq qilish uning rasshifrovka qilinishiga olib keladi.

Almashtirish usulining kamchiligi sifatida dastlabki va berilgan matnlar statistik xarakteristkalarining bir xilligidir. Dastlabki matn qaysi tilda yozilganligini bilgan kriptoanalitik ushlab qolingan axborotlarni statistik ishlab, ikkala alfavitdagi simvollar o`rtasidagi muvofiqlikni aniqlashi mumkin.

Siljitish shifri. Siljitish shifri ikki turga bo`linadi. Ular oddiy va murakkab siljitish shifrlaridir.

Simmetrik kriptografiyaga oid dastur:

Dasturga kirish uchun foydalanuvchi o’z login va paroliga ega bo’lmog’i lozim .Bu dasturning maxfiyligini saqlaydi. Biz hozirgi kunda axborotlarni saqlashning bir necha usullari mavjud. Quyidagi programma bunga misol bo’la oladi.

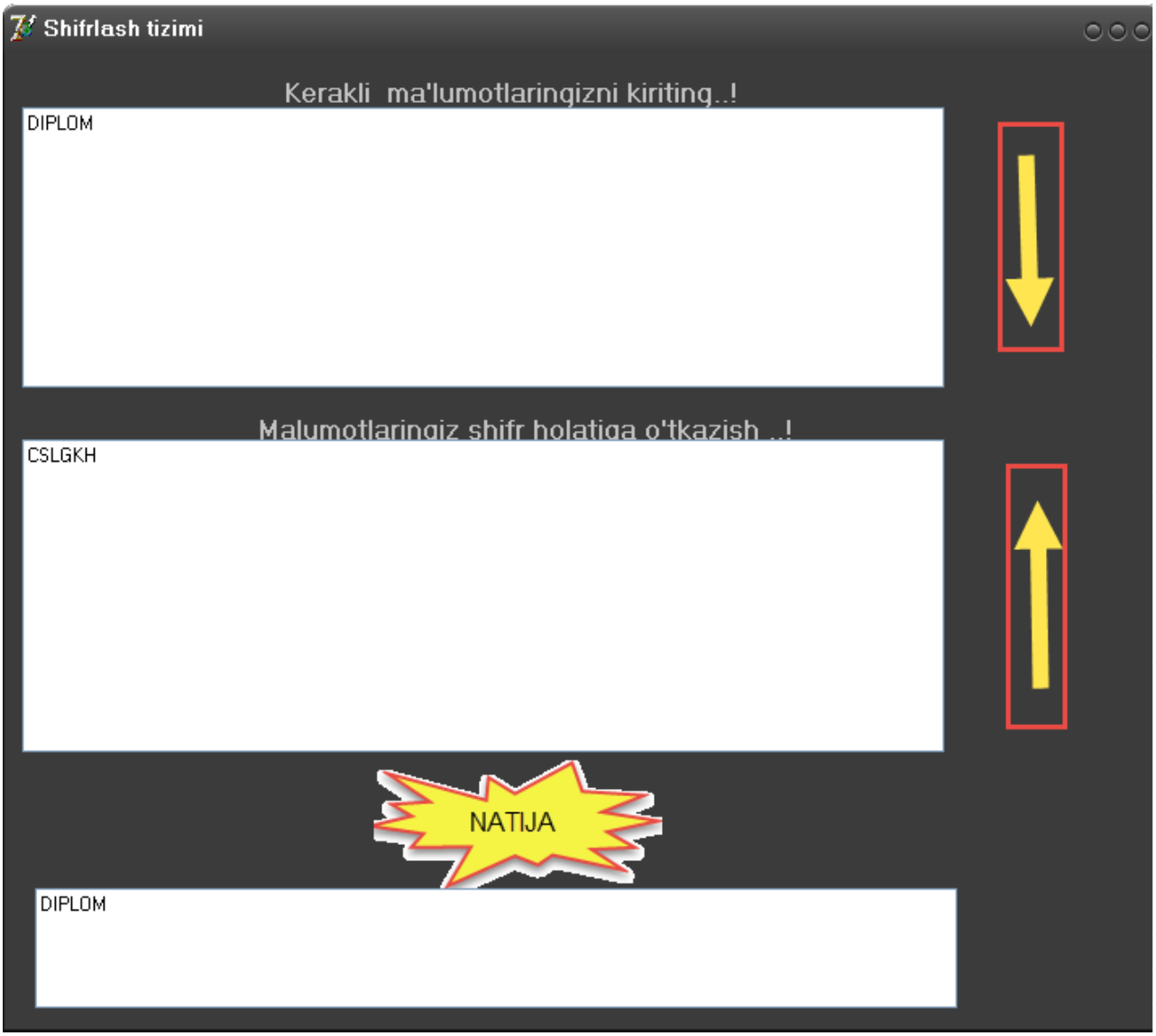
Agar foydalanuvchi o’z login yoki parolini noto’g’ri kiritsa quyidagi holat ro’y beradi.

Bu programmani Delphi dasturlash tilida tuzib chiqilgan. Bu juda oddiy.Uni quyidagi algoritmlar asosida tuzilgan. Bu quyidagi rasm va izoxlarda o’z aksini topgan:

1) Dastur interfeysi tuzib olinadi. Dastur interfeysi biz yuqorida ko'rgan rasmda o'z aksini topgan. Bunda **KIRISH** qismiga quyidagicha kod yoziladi:

```
procedure TForm1.sButton1Click(Sender: TObject);
begin
if sEdit1.Text='Ahmedova' then l:=1 else l:=0;
if sEdit2.Text='Gavhar' then p:=1 else p:=0;
if (p+l)>1 then Form2.Show  else
Label3.Caption:='Login yoki Parolni noto''gri terdingiz. Iltimos boshqatdan urinib ko''ring!';
end;
```

2) Dasturning asosiy qismi 2- forma oynasida joylashgan. U quyidagicha



Shifrlash qismiga quyidagicha kod kiritamiz:

```
procedure TForm2.SpeedButton1Click(Sender: TObject);
var
a,b:string; k:byte; i:integer;
begin
a:=Memo1.Lines.Text;
for i:=1 to length(a) do
begin
k:=pos(a[i],sh);
b:=b+dsh[k];
end;
memo2.Lines.Text:=b;
```

Shifrdan chiqarish bo'limiga quyidagicha kod yozamiz:

```
procedure TForm2.SpeedButton2Click(Sender: TObject);
var
n,m:string; j:integer; l:byte;
begin
n:=memo2.Lines.Text;
for j:=1 to length(n) do
begin
l:=pos(n[j],dsh);
m:=m+sh[l];
end;
memo3.Lines.Text:=m;
end;
```

Quyidagi constanata larni e'lon qilamiz:

```
var
  Form2: TForm2;
   const sh='ABDCEFGHIJKLMNOPQRSTUVXYZSHCHNGabdcefghijklmnopqrstuvxyz';
  const dsh='ZXCVBNMASDFGHJKLPOIUYTREWQzxcvbnmlkjhgfdsaqwertyuiop';
```

Bu kod oynadagi alfavitlardagi mos o'rinlardagi boshqa lotin alfavitlarga almashtirish jarayoni ketadi.

2.3 Nosimmetrik kriptosistemalar.

Shifrlash va shifr ochish kalitlari o‘zaro funktsional bog‘langan bo‘lib ulardan biri asosida ikkinchisi amaliy jihatdan(mavjud hisoblash vositalari taraqqiyoti darajasida) hisoblab topilishi mumkin bo‘lmagan va ulardan biri faqat bitta aloqa ishtirokchisiga ma’lum bo‘lib boshqalardan maxfiy tutiladigan, ikkinchisi esa aloqa ishtirokchilarining hammasiga oshkor bo‘lgan kriptotizim nosimmetrik(sinonimlari: oshkora kalitli, ikki kalitli) kriptotizim deb ataladi.
Nosimmetrik kriptotizim ikki kalitli tizim bo‘lib, unda aloqa ishtirokchilarining har biri o‘zining shaxsiy maxfiy va oshkora kalitlari juftiga ega bo‘lib o‘z oshkora kalitini boshqa aloqa ishtirokchilariga e’lon qiladi. SHaxsiy maxfiy kalit qabul qilinadigan axborot pinhonaligini ta’minlash uchun yaratilganda shifrni ochish kaliti bo‘lib xizmat qiladi. Bunda kimga pinhona axborot jo‘natiladigan bo‘lsa shuning oshkora kalitidan foydalanib shifrlangan axborot jo‘natiladi. Bunday axborotning shifrini faqat yagona maxfiy kalit egasigina ocha oladi. Agar maxfiy kalit autentifikatsiya maqsadida jo‘natmalarga raqamli imzo bosish uchun hosil qilingan bo‘lsa, u shifrlash kaliti sifatida foydalaniladi. Oshkora kalit esa yuqoridagi birinchi holda shifrlash kaliti bo‘lib, ikkinchi holda shifrni ochish (tekshirib ko‘rish) kaliti bo‘lib xizmat qiladi.

Nosimmetrik kriptotizimlar asoslari simmetrik tizimlarda yechilmay qolgan kalit tarqatish va raqamli imzo muammolarining yechimini izlash yo‘llarida Massachusets texnologiya institutida U.Diffi(W.Diffie) va uning ilmiy rahbari M.Xellman(M.E.Hellman) tomonidan 1975 yilda taklif etilgan. 1977 yili shu tamoyil asosida o‘sha institutda R.Rivest, A.SHamir, L.Adlman(R.Rivest, A.SHamir, L.Adleman) tomonidan RSA algoritmi ishlab chiqildi. Keyinchalik elliptik va sh.o‘. bir tomonlama oson hisoblanadigan funktsiyalar asosiga qurilgan boshqa algoritmlar(El Gamal va boshqalar algoritmlari) yaratildi.

Nosimmetrik kriptotizimlar simmetrik kriptotizimlarga nisbatan o‘nlab marta ko‘proq axborot miqdoriga ega(512, 1024,2048,4096 bitli) kalitlardan

foydalanadi va shunga ko‘ra yuzlab marta sekinroq ishlaydi. Nosimmetrik kriptotizimlarning matematik asosida bir tomonlama oson hisoblanadigan funktsiyalar (darajaga oshirish, elliptik funksiya, rekursiya va sh.o‘.) yotadi. U.Diffi va M.Xellman taklif etgan himoyalanmagan ochiq aloqa kanali orqali kalit tarqatish usulining mohiyatini quyidagi misolda ko‘ramiz. Faraz qilaylikki Otabek va Kumush simmetrik kriptotizimdan foydalanish uchun o‘zaro mahfiy kalit belgilab olmoqchilar. Buning uchun ulardan biri biror katta tub son M ni va 1 bilan M-1 orasidan butun son g ni tanlab himoyalanmagan aloqa kanali(masalan, telefon) orqali ikkinchilariga bildirib kelishib oladilar. So‘ngra ikkavlari ham 1 bilan M-1 orasidan aloxida ixtiyoriy butun sonlarni tanlab uni o‘zlarining shaxsiy kalitlari deb belgilaydilar va uni xech kimsaga (bir-birlariga ham) bildirmaydilar. Faraz qilaylikki, Otabekning shaxsiy mahfiy kaliti o, Kumushning shaxsiy maxfiy kaliti esa k bo‘lsin. Bu shaxsiy mahfiy kalitlar o‘zaro mahfiy (ikkavlaridan boshqa xechkim bilmaydigan) kalitni va o‘zlarining shaxsiy oshkora kalitlarini xosil qilishda qatnashadigan kalitlardir. Otabek o‘z shaxsiy oshkora kaliti Eota ni, Kumush o‘z shaxsiy oshkora kaliti Ekum ni xosil qilish uchun g sonini M moduli bo‘yicha o‘z shaxsiy maxfiy kalitlariga teng bo‘lgan darajaga oshirishlari kifoya. Ular o‘z shaxsiy oshkora kalitlarini bir-birlariga va boshqalarga ham ochiq aloqa kanali orqali ma’lum qilganlaridan so‘ng o‘zaro mahfiy kalitni xisoblab topishlari mumkin bo‘ladi. Otabek bilan Kumushning o‘zaro maxfiy kaliti K birlarining oshkora kalitini ikkinchilarining mahfiy kalitiga teng darajaga M moduli bo‘yicha oshirilganiga teng.Endi ular biror simmetrik kriptotizimdan foydalanib maktub almashishda faqat ikkavlarigagina ma’lum bo‘lgan kalit k bilan o‘z maktublarini shifrlaydilar va shu kalit bilan shifrlangan maktub shifrini ochib o‘qiydilar. SHaxsiy oshkora kalitlar, M moduli va g asos Homidga ham ma’lum. Lekin, u shaxsiy mahfiy kalitlardan bexabar bo‘lgani uchun Otabek va Kumushlarning o‘zaro mahfiy kalitlarini bilaolmaydi. CHunki, buning uchun yo Otabekning yo Kumushning shaxsiy mahfiy kalitini bilishi zarur. Uni bilish uchun g asosda M moduli bo‘yicha oshkora kalitning diskret logarifmini hisoblab topish zarur. M soni 2 ning 512 chi darajasiga teng songa yaqin son bo‘lsa va u “yaxshi tub son”

(ya’ni, undan bitta kam sonni yarmisi ham tub son) bo‘lsa diskret logarifmni hisoblashda ishlatiladigan ko‘paytuv amallari ning (M moduli bo‘yicha) soni 2 ning 256 chi darajasiga yaqin bo‘ladi. Buncha amallarni bajarish uchun eng zo‘r zamonaviy superkompyuter ham minglab yillar davomida tinimsiz ishlashi lozim bo‘ladi.Yuqorida ko‘rib o‘tilgan shaxsiy oshkora va shaxsiy mahfiy kalitlar bir tomonlama hisoblanadigan funktsiya asosiga qurilgan bo‘lib, ular maktublarni bevosita shifrlash va shifrini ochish muammosini emas, balki maktub (umuman, harqanday axborot)larni simmetrik kriptotizimlarda shifrlashda va shifr ochishda foydalaniladigan o‘zaro mahfiy kalitlarni oshkora taqsimlash muammosini echib beradi. YAshirin yo‘lli birtomonlama funktsiyalardan foydalanilganda almashiladigan axborotlarni uzatish va raqamli imzo asosida autentifikatsiya muammosini yechish ham oson hal bo‘ladi. Bunday qulay funktsiya turini birinchi bo‘lib RSA algoritmining mualliflari taklif etishgan. Unda oshkora modul M ikki tub sonning ko‘paytmasi bo‘lib, ko‘paytuvchilar sir tutiladi. Ko‘paytuvchilardan bitta kam sonlar ko‘paytmasi ikkinchi(mahfiy) modul bo‘lib, u ham sir tutiladi. Mahfiy modulga nisbatan o‘zaro teskari ikki sondan biri shaxsiy oshkora kalit, ikkinchisi shaxsiy mahfiy kalit deb qabul qilinadi. SHu shaxsga yo‘llaniladigan axborot bloklari uning oshkora kalitida shifrlab(M moduli bo‘yicha oshkora kalitga teng darajaga oshirib) jo‘natiladi. Qabul qilib olingan axborot bloklari shifri shu shaxsning shaxsiy mahfiy kalitida ochiladi(M moduli bo‘yicha maxfiy kalitga teng darajaga oshirib).Faraz qilaylikki, Otabek Kumushga nosimmetrik kriptotizimdan foydalanib pinhona maktub yo‘llamoqchi. Ular orasida aloqa boshlanguncha Kumush o‘z oshkora kaliti nusxasini Otabekka va boshqalarga ma’lum qilgan. Ular bir-birlariga maktubni faqat shifrlangan shaklda yuborishga kelishib qo‘yganlar. Otabek Kumushga m maktubini yozib, uni Kumushning oshkora kaliti bilan shifrlaydi. Natijada m maktubi shifrlangan matn C ga aylanadi. So‘ngra Otabek shifrlangan maktubni elektron pochta orqali Kumushga jo‘natadi. Xat Kumushning oshkora kaliti bilan shifrlangan bo‘lgani uchun uni Kumush o‘z maxfiy kaliti bilan ochib bemalol o‘qiy oladi. YA’ni, shifrlangan matn C Kumushning maxfiy kaliti bilan dastlabki matn m ga aylantiriladi.Aloqa kanali himoyalanmagan bo‘lgani

uchun bu maktub Homidning qo‘liga ham tushishi mumkin. Lekin Homidda Kumushning maxfiy kaliti bo‘lmagani uchun u xatning mazmunini bilaolmaydi va xatni o‘zgartirib qo‘ya olmaydi. Homidning qo‘lidan maktubni yo‘q qilib yuborish va yoki Kumushga uning oshkora kalitidan foydalanib Otabek nomidan shifrlangan yangi qalbaki maktub yo‘llash keladi. Homid maktub mazmunini bilmay turib Otabek nomidan shifrlangan maktub jo‘natsa, buning qalbaki ekanligi Kumushga darhol oshkor bo‘lmasligi mumkin. CHunki, xat Kumushning oshkora kaliti bilan shifrlangan bo‘lgani uchun uni Kumush o‘z maxfiy kaliti bilan ochib o‘qiydi. Bu xatning chindan ham Otabekdan ekaniga ishonch hosil qilish uchun buyerda autentifikatsiya muammosini(Otabekning raqamli imzosini tekshirish orqali) hal qilish lozim bo‘ladi.Bu muammoni yechishda raqamli imzo qo‘yish uchun shaxsiy maxfiy kalitdan, imzoni tekshirish uchun shaxsning oshkora kalitidan foydalaniladi. Bu sal keyinroq ko‘rilgan.

Ma`lumotlarni shifrlashning shunday algoritmlari mavjudki, ularda shifrlash usullarini bemalol ochib berish mumkin. Demak, kriptoanalitik ham ushbu shifrlash algoritmi haqida yetarlicha ma`lumotga ega. Shunday bo`lsada, u shifrlangan ma`lumotni qayta shifrlash imkoniyatiga deyarli ega bo`lmaydi. Sababi, ma`lumotlarni ishfrlashda bir hil usul ishlatilsa, qayta shifrlashda butunlay boshqa usuldan foydalaniladi. Kriptografiyada bunday usullarni ***ochiq kalitli shifrlash usullari*** yoki ***nosimmetrik kriptosistemalari*** deb ataladi.

Kriptografiyada ochiq qalitli shifrlash usullarini qo`llash quyidagi bosqichlarda amalga oshiriladi. Faraz qilaylik ma`lumotni jo`natuvchi (A tomon) uni qabul qiluvchiga (B tomonga) shifrlangan mahfiy xatni jo`natishi lozim. A tomon biror ochiq kalitli shifrlash usulida ma`lumotni shifrlaydi va uni ochiq usulda B tomonga uzatadi. Shifrlash bilan bog’liq va mahfiy saqlanishi lozim bo`lgan ayrim parametrlarni A va B tomonlar o`zaro kelishib olishadi. A tomon B tomonga ma`lumotlarni jo`natishda shifrlash uchun qanday kalitdan foydalanganini hammaga e`lon qilishi mumkin. Ushbu ma`lumotni qayta shifrlashi uchun A tomon foydalangan kalit yaramaydi. Shuning uchun B tomon maxfiy saqlanayotgan parametrlardan foydalanib, butunlay boshqa kalit ishlab chiqadi va

uning yordamida ma`lumotlarni qayta shifrlaydi. Bu ikki tomon o`rtasida kriptoanalitik deb ataluvchi S tomon turadi va u B tomonga ketayotgan shifrlangan ma`lumotni tutib qolishi mumkin. Uning oldida turgan masala shifrlangan matnni qayta shifrlab, uning asl holatini tiklashdan iborat. U ochiq kalitni ham osongina qo`lga kiritishi mumkin. Ammo, bu kalit shifrlangan matnni qayta shifrlashga yordam bera olmaydi. Albatta, K. Shennon printsipiga ko`ra, u qachondir shifrlangan matnni qandaydir usul bilan qayta shifrlashga erishishi mumkin. Ammo, bu jarayon shunday ko`p vaqtni talab qiladiki, matn qayta shifrlangan vaqtda uning dolzarbligi qolmagan bo`ladi. Shuning uchun A va B tomonlar o`zlari uchun hisoblash jarayoni engil, ammo kriptoanalitik uchun o`ta murakkab bo`lgan shifrlash usullarini tanlashlari mumkin. Kriptografiyada ochiq kalitli shifrlash usullarini qo`llashning sababi quyidagicha. Murakkablik nazariyasi nisbatan yaqinda rivojlana boshladi. Bu nazariya turli hisoblash ishlari murakkabligini, boshqacha aytganda hisoblash ishlari uchun eng zamoonaviy komp’yuterlarda qancha vaqt sarf qilinishini o`rganadi. Bunday ma`lumot kriptografiya uchun muhim hisoblanadi. CHunki, ochiq usulda shifrlangan ma`lumotlarni qayta shifrlash uchun kriptoanalitik yuzlab yillarni sarf qilishiga to`g’ri keladi va bu vaqtdan keyin shifrlangan ma`lumot dolzarbligini yo`qotgan bo`ladi.

Ochiq kalitli shifrlash g’oyalari bir tomonlama funktsiyalar bilan bog’liq. Berilgan *x* argument bo`yicha *f(x)* funktsiyaning qiymatini osongina topish mumkin, ammo *f(x)* dan foydalanib *x* ning qiymatini aniqlash nihoyatda qiyin ish. Bu yerda “qiyin ish” jumlasi murakkablik nazariyasi ma`nosida kelmoqda.

f(x) dan foydalanib *x* ning qiymatini aniqlash faqat kriptoanalitik uchun qiyin. Bu ma`lumotlarni rasmiy qabul qiluvchi esa qayta shifrlash uchun yangi kalit ishlab chiqish yo`lini biladi va osongina bu kalit yordamida shifrlangan ma`lumotni qayta shifrlaydi.

Funktsiya qiyin hisoblanadi deb ataladi, agar uni polinomial ish vaqtida hal qilish algoritmi mavjud bo`lmasa.

Agar shunday algoritm mavjud bo`lsa, funktsiyani hisoblanadigan deb ataladi.

NP-***to`liq masalalari*** qiyin hisoblanadigan masalalar sarasiga kiradi.

f(x) funktsiyani ***bir tomonlama*** deb ataladi, agar *x* dan *f(x)* ga osongina o`tilib, *f(x)* dan *x* ga o`tish qiyin hisoblanadigan bo`lsa.

Biz ma'lumotarni shifrlash va qayta shifralshda algebraik elementlardan foydalanish jarayonini ochib berish jarayonni ryukzak algoritmi misolida ko`rib chiqamiz. Chunki, ryukzak algoritmi yardamida ma'lumotlarni shifrlashda algebraic apparat yaqqol ko'rinadi va tahlil qilish uchun oson bo'ladi. ***Masala:*** (***Ryukzak masalasi***) N ta o`zaro turli hildagi musbat butun $A=(a_1, a_2, \ldots, a_N)$ sonlar va yana bitta *k* musbat butun soni berilgan bo`lsin. Agar iloji bo`lsa, shunday a_i larni topish kerakki, ularning yig'indisi *k* ga teng bo`lsin.

Eng oddiy holda *k* soni ryukzakning hajmini, a_i larning xar biri esa ryukzakka solinishi mumkin bo`lgan buyum o`lchamini anglatadi. Demak, shunday buyumlar turini aniqlash kerakki, ularning umumiy o`lchami ryukzak o`lchamiga teng bo`lsin.

Misol tariqasida 3231 va 10 ta sonlar to`plami (43, 129, 215, 473, 903, 302, 561, 1165, 697, 1523) ni ko`raylik.

3231 = 129 + 473 + 903 + 561 + 1165 .

SHunday qilib, biz masala echimini topdik. Bunday masalalarni echishda odatda perebor (hamma imkoniyatlarni ko`rib chiqish) usulidan foydalaniladi. Bizning misolimizda $2^{10}$ = 1024 ta qism to`plamlarni ko`rib chiqish etarli. Buni bajarish muammol emas. Ammo, berilgan to`plam elementlari bir necha yuzta bo`lsa-chi? Aniqlik uchun 300 deylik. Bu o`rinda shuni alohida ta`kidlash joizki, murakkabligi hamma imkoniyatlarni ko`rib chiqish algoritmiga nisbatan pastroq bo`lgan algoritmlar ma`lum emas. Amaliy jihatdan 2^{300} ta qism to`plamni ko`rib chiqishning iloji yo`q. SHuning uchun ryukzak haqidagi masala *NP*-to`liq masalalar sirasiga kiradi.

A to`plamining *n*-qism to`plami *f(x)* funktsiyani quyidagicha aniqlaydi. $0 \le x \le 2^n-1$ intervaldagi ihtiyoriy sonni *p* razryadli ikkilik sanoq sistemasidagi sonlar bilan ifodalash mumkin. Zarur bo`lganda uni oldindan 0 lar bilan to`ldirilishi mumkin. Masalan, 1, 2 va 3 larni 0...01, 0...010, 0...011 tarzida yozilishi mumkin. 2^n-1 esa 1...111 bo`ladi. *f(x)* funktsiyani *x* soniga teng ikkilik sanoq sistemasidagi sonning birlariga mos $a_i$ sonlarning yig'indisi shaklida aniqlaymiz, ya`ni

$f(1)=f(0\ldots.01)=a_n$

$f(2)=f(0\ldots.010)=a_{n-1}$

$f(3)=f(0\ldots.011)=a_n+a_{n-1}$

Bu funktsiyani vektor ko`paytma orqali ifodalasak, $f(x)=AB_x$ bo`ladi. Bu erda B_x – *x* – sonining ikkilik sanoq sistemasidagi ko`rinishining vektor-ustuni.

Masalan, 364 soni uchun bu ifodani

$f(364) = f(0101101100) = 129 + 473 + 903 + 561 + 1165 = 3231$.

tarzida yozish mumkin. Funktsiyaning yana ayrim qiymatlarini ko`raylik.

$f(73) = f(0001001001) = 473 + 561 + 1523 = 2557,$

$f(617) = f(1001101001) = 43 + 473 + 903 + 561 + 1523 = 3503,$

$f(32) = f(1000110100) = 43+903+302+1165=2413,$

$f(672) = f(1010100000) = 43 + 215 + 903=1161,$

$f(306) = f(0100110010) = 129+903+302+697=2031,$

$f(265) = f(0100001001) = 129 + 561 + 1523 = 2213,$

Bu konkret qiymatlardan biz keyinroq foydalanamiz.

f(x) funktsiyani A ning qicm to`plamlaridan foydalanib topilmoqda. Tabiiyki, agar biz *x* ni *f(x)* foydalanib topa olsak, ryukzak masalasi hal bo`ladi, ya`ni *x* ning ikkilik sanoq sistemasidagi ko`rinishi *f(x)* ni hisoblash uchun kerar bo`lgan A ning elementlarini ko`rsatib beradi. Ryukzak masalasi *NP*-to`liq

bo`lgani uchun, *f(x)* bir tomonlama funktsiya bo`ladi. Bu erda albatta *p* etarlicha katta son (200 dan kichik bo`lmagan) bo`lishi zarur.

Dastlab, A “ryukzak vektorlari”dan qanday qilib kriptosistema asosi sifatida foydalanish mumkinligini ko`raylik. Dastlabki matn kodlanadi va *n*-razryadli bloklarga ajratiladi. Agar zarur bo`lsa, oxirgi blok nollar bilan to`ldiriladi. *p*-razryadli bloklarning xar biri shu blok uchun topilgan *f(x)* ning qiymati bilan shirflanadi.

Agar matn o`zbek-lotin alifbosida yozilgan bo`lsa, xar bir xarfni uning alfavitda tutgan o`rni bilan, bo`sh joy belgisi esa 0 bilan kodlanadi. Kodlashning bunday usuli uchun 5 bit (5 ta nol va birlarning kombinatsiyasi) etarli. Quyidagi jadvalda xarflarni kodlash 1 dan boshlanadi.

xarf	son	ikkilik sanoq sistemasida	xarf	son	ikkilik sanoq sistemasida
bo`sh joy	0	00000	N	14	01110
A	1	00001	O	15	01111
B	2	00010	P	16	10000
C	3	00011	Q	17	10001
D	4	00100	R	18	10010
E	5	00101	S	19	10011
F	6	00110	T	20	10100
G	7	00111	U	21	10101
H	8	01000	V	22	10110
I	9	01001	W	23	10111
J	10	01010	X	24	11000
K	11	01011	Y	25	11001

L	12	01100	Z	26	11010
M	13	01101	‘	27	11011

Yuqorida keltirilgan 10 ta elementdan iborat vektor misolida shifrlaymiz. Shifrlanadigan matn “BITIRUV ISHI” bo`lsin. Shifrlanayotgan bloklar 10-razryadli bo`lgani uchun shifrlanayotgan matnni bloklarga ajratamiz:

BI TI RU Vbo`sh joy IS HI

Bu bloklarga quyidagi ikkilik ketma-ketliklar mos keladi:

0001001001, 1001101001, 1000110100, 1010100000, 0100110010, 0100001001 .

Bu ketma-ketlik yuqorida qaralgan *f(x)* funktsiyaning argumentlari bo`lib xizmat qiladi, demak, shifrlangan matn 6-ta sondan iborat bo`ladi:

(2557, 3503, 2413, 1161, 2031, 2213)

Bunday usul bilan aniqlangan *f(x)* funktsiya asosidagi kriptosistema hali mukammallikka da`vo qila olmaydi. Mazkur kriptosistemani mukammallashtirish, ya`ni ochiq kalitli sistemaga aylantirish uchun quyidagi farazlardan foydalanamiz.

Bitta shifrlangan matnni qayta shifrlab, ikki xil matnni hosil qilish mumkin bo`lmasin. Bu shuni anglatadiki, A vektorning elementlaridan foydalanib, hosil qilish mumkin bo`lgan ikkita bir yil yig’indi mavjud bo`lmaydi.Yig’indilar turli sondagi qo`shiluvchilardan tashkil topishi mumkin, ammo unda A ning xar bir elementi faqat bir marta ishtirok etadi.

n-talik $A=(a_1,a_2, ,,, , a_n)$ vektor tez usuvchan deyiladi, agar ikkinchi elementdan boshlab, har bir element o`zidan avval kelgan elementlarning yig’indisidan katta bo`lsa, ya`ni

$$a_j \geq \sum_{i=1}^{j-1} a_i , \ j = 2, 3, 4, ..., n .$$

Barcha imkoniyatlarni ko’rib chiqishda A vektorni o’ngdan chapga qarab bir marta ko’rib chiqish yetarli. Berilgan k (ryukzak o’lchami) uchun biz dastlab $k>a$ shartni tekshiramiz. Agar u o’rinli bo’lmasa, a_p izlanayotgan yig’indiga kirmaydi,

aks holda kiradi. Bu narsa qolgan barcha elementlarning k dan kichik yig'indini beradi.

$$k_1 = \begin{cases} k, & agar\ k < a_n \\ k = k - a_n, & agar\ k \geq a_n \end{cases}$$

ni aniqlaymiz. Endu yuqoridagi jarayonni k_1 va a_{n-1} uchun takrorlaymiz. Shunday qilib, biz a_1 gacha boriladi. Masalaning algoritmi ko'rsatadiki, ihtiyoriy k soni uchun ryukzak masalasi A vector tez o'suvchan bo'lganda bittadan ko'p bo'lmagan yechinmi berishi mumkin.

Agar kriptosistema asosi sifatida tez o'suvchan A vektor olinsa, qayta shifrlash masalasi kriptoanalitik uchun ham, ma'lumotni qabul qiluvchi rasmiy tomon uchun ham nihoyatda osonlashadi. Buning oldini olish uchun biz A vektorni shunday "chayqatamizki", natijaviy B vector tez o'suvchan bo'lmay, ryukzak haqidagi oddiy vektorga aylanadi. "Chayqatish" uchun biz modul bo'yicha ko'paytirish amalidan foydalanamiz.

Biri butun $a > \sum a_i$ sonini tanlab olamiz. A vector tez o'suvchan bo'lani uchun m soni A dagi ementlardan kattaroq bo'ladi. Bu m bilan o'zaro tub bo'lgan boshqa t butun sonini olamiz. m va t sonlar modul va ko'paytuvchi bo'ladi. t ni bu usulda tanlash $tt^{-1}=1$ shartni qanoatlantiruvchi butun t^{-1} topilishini kafolatlaydi. Uni t ga teskari element deb ataladi. Teskari elementni t va m lar orqali osongina topish mumkin bo'ladi. .

Endi ta_i (i=1, 2, …, n) ko'paytirishni bajaramiz va hosil bo'lgan sonlarni m modul bo'yicha keltiramiz. b_i — ta_i (i=1, 2, …, n) ni m modul bo'yicha eng kichik musbat qoldig'i hamda natijaviy vector B = $(b_1, b_2, ..., b_n)$ bo'lsin. Bu vektor shifrlash n-razryadli shifrlash kaliti bo'lib xizmat qiladi. Shifrlash algoritmi esa yuqorida keltirilgan.

t, t^{-1} va m sonlari mahfiy saqlanadi. Kriptoanalitik oldida turgan vaziyatni tahlil qilishdan avval qaralayotgan misolga qaytaylik.

Biz yuqorida ko'rgan (endilikda B bilan belgilangan)

V = (43, 129, 215, 473, 903, 302, 561, 1165, 697, 1523)

vector tez o'suvchan

A = (1, 3, 5, 11, 21, 44, 87, 175, 349, 701)

vektorni t = 1590 va t = 43 sonlarga modul bo'yicha ko'paytirish orqali hosil qilingan. Bu holatni batafsil ko'qib chiqamiz.

B ning dastlabki besh elementi A ning mos elementlarini 43 ga oddiy ko'paytirish yo'li bilan hosil qilingan. Ularni m modul bo'yicha keltirish shart emas. (Amalda dastlabki sonlarning kichik bo'lmasligi zarur. Qolgan elementlar quyidagi hisoblashlardan so'ng olingan:

$43 \cdot 44 = 1892 = 1590 + 302$

$43 \cdot 87 = 3741 = 2 \cdot 1590 + 561$

$43 \cdot 175 = 7525 = 4 \cdot 1590 + 1165$

$43 \cdot 349 = 15007 = 9 \cdot 1590 + 697$

$43 \cdot 701 = 30143 = 18 \cdot 1590 + 1523$

Shuni alohida ta'kidlash joizki, t va m lar o'zaro tub. Haqiqatdan ham,

$43 \cdot 37 = 1591 = 1 \pmod{1590}$

Demak, $t^{-1} = 37$.

Endi rasmiy qabul qiluvchi uchun qayta shifrlahning oson yo'lini qidiramiz. Dastlab, A vector tez o'suvchan bo'lib, B vector undagi xar bir elementni t (mod m) ga ko'paytirib hosil qilingan vaziyatni ko'raylik. Rasmuy qabul qiluvchi t^{-1} va m ni biladi. U A vektorni B ochiq kalitdan topa oladi. Shifrlangan matnning butun sondan iborat bo'lgan c' blogini olganidan so'ng, rasmuy qabul qiluvchi $t^{-1}c$' ni hisoblab, uning eng kichik musbat qoldig'i s ($mod\ m$) ni topadi. Qayta shifrlash vaqtida u A va c yordamida aniqlanadigan ryukzak masalasini osongina hal qiladi. Bu salaning yechimi n bitli yagona ketma-ketlikdan iborat bo'ladi. Shuningdek, u boshlang'ich ma'lumotning to'g'ri blogi bo'ladi, chunki B va c' bilan

aniqlanadigan ryukzakni yig'ishtirish masalasining ihtiyoriy *p'* yechimi *p* ga teng bo'lishi kerak. Haqiqatdan ham,

$$c \equiv t^{-1}c' = t^{-1}Bp' \equiv t^{-1}Ap' \equiv Ap' \pmod{m}.$$

Shuni alohida ta'kidlash joizki, $Ar' < t$, chunki $t > a_1 + a_2 + \ldots + a_p$. Bu shuni anglatadiki, yuqoridagi tenglikni $s = Ar'$ tenglama ko'rinishida qayta yozish mumkin, chunki A va s lar bilan aniqlanadigan masala bir nechta yechimga ega bo'la olmaydi va shuning uchun $r' = r$.

Demak, rasmiy qabul qiluvchi shiftrlangan

(2557, 3503, 2413, 1161, 2031, 2213)

matnni "qo'lda" qayta shifrlashi mumkin. t^{-1}=37 ga ko'paytirib, birinchi sonni hosil qilinadi:

$37 \cdot 2557 = 94609 = 59 \cdot 1590 + 799 = 799 \pmod{1590}$

$37 \cdot 3503 = 129611 = 81 \cdot 1590 + 821 = 621 \pmod{1590}$

$37 \cdot 2413 = 89281 = 56 \cdot 1590 + 241 = 241 \pmod{1590}$

$37 \cdot 1161 = 42957 = 27 \cdot 1590 + 27 = 27 \pmod{1590}$

$37 \cdot 2031 = 75147 = 47 \cdot 1590 + 417 = 417 \pmod{1590}$

$37 \cdot 2213 = 81881 = 51 \cdot 1590 + 791 = 791 \pmod{1590}$.

Shunday qilib, biz quyidagi oltiltikni hosil qildik:

(799, 621, 241, 27, 417,791) .

A = (1, 3, 5, 11, 21, 44, 87, 175, 349, 701) .

799 soni va tez o'suvchan A vector 10-razryadli 0001001001 ketma-ketlikni beradi. Haqiqatdan ham 799 > 701 bo'lgani uchun oxirgi bit 1 ga teng bo'lishi lozim. Endi A dagi sonlar 799-701 = 98 ayirma bilan solishtiriladi. O'ngdan chapga qarab 98 dan kichik son 87. Navbatdagi 98-87=11 ayirmadan kichik son 11. Yakunda 11-11 ayirmaga teng son 0 ga teng. Demak, 11, 87 va 701 larning A dagi o'rni mos ravishda 4, 7, va 10 ga, ya'ni 0001001001 teng..

Shunday qilib, 621,..., 791 sonlar keyingi beshta 10-razryadli ketma-ketliklarni beradi. Hosil qilingan barcha ketma-ketliklarni qayta kodlab, rasmiy qabul qiluvchi boshlang'ich matnga ega bo'ladi:

BITIRUV ISHI

Ryukzak haqidagi tez o'suvchan vektorga asoslangan kriptosistema oshiq kalitli shifrlash usullariga yorqin namuna bo'la oladi.

Biz endi ma`lumotlarni shifrlashning ryukzak usulining matematik apparatini ko`raylik.

Ta`rif-1. Ryukzak vektori deb n ($n \geq 3$) ta tartiblangan natural sonlardan tashkil topgan $A = (a_1,...,a_n)$ vektorga aytiladi.

**Ta`rif-2**. Ryukzak masalasining boshlang'ich ma`lumotlari deb (A, α) juftlikka aytiladi. Bu erda A - ryukzak vektori, α - natural son. (A, α) ma`lumotlar uchun ryukzak masalasining echimi deb A ning shunday qism to`plamiga aytiladiki, uning elementlari yig'indisi α ga teng bo`ladi. Bu yig'indida A ning har bir elementi faqat bir marta ishtirok etadi.

Odatda ryukzak masalasi qo`yilganda, ($A$, $\alpha$) ma`lumotlar uchun masala echimga ega bo`lishini aniqlashga to`g'ri keladi. Kriptografiyada qo`llanayotgan variantda esa shunday echim mavjud degan nuqtai-nazardan deb hisoblanadi. Masala *NP*-to`liq masalalar sinfiga kiradi.

A ryukzak vektoridan faqat ikkilik sanoq sistemasidagi sonlardan tashkil topgan S matn blogini shifrlash uchun foydalaniladi. Unda S ning bir soniga A vektorning mos o`rinlarida turgan elementlari yig'indisi olinadi. Agar bu yig'indini α bilan belgilasak, ryukzak masalasi A dan foydalanib α ni, yoki α dan foydalanib A topish masalasiga keladi. Bu masalani boshqacha qilib,

$$\alpha = \sum_{i=1}^{n} a_i c_i$$

ko`rinishida ham yozish mumkin. Masalan, $n$=6 va $A$=(3, 41, 5, 1, 21, 10) bo`lsin. U holda ikkilik (1, 1, 0, 0, 1, 0) va (1, 0, 1, 1, 0, 1) bloklar mos ravishda 65 va 19 tarzida shifrlanadi. Berilgan A vektor uchun shifrlangan matn 81 dan kichik bo`lgan sonlardan tashkil topadi va xar bir matnga faqat bitta shifrlangan matn mos keladi.

A=(14, 28, 56, 82, 90, 132, 197, 284, 341, 455) bo`lgan vektor uchun α=515 ga mos keluvchi shifrlangan matn ikkita boshlang'ich matnga mos keladi:

f(0, 1, 1, 0, 1, 0, 0, 0, 1, 0)=28+56+90+341=515

f(1, 0, 0, 1, 1, 1, 1, 0, 0, 0)=14+82+90+132+197=515

Ammo, α=517 uchun (1, 1, 1, 0, 1, 1, 1, 0, 0, 0) vektor yagona boshlang'ich matn bo`ladi:

f(1, 1, 1, 0, 1, 1, 1, 0, 0, 0)=14+28+56+90+132+197=517.

Qayta shifrlashning bir qiymatli bo`lishi uchun $A$ ryukzak vektori har bir $\alpha$ da barcha ($A$, $\alpha$) boshlang'ich ma`lumotlar uchun bittadan ortiq echimga ega bo`la olmaydi. Bunday ryukzak vektorlarini in`ektiv deb ataladi. CHunki, 1-misolda qaralgan A vektor yordamida hosil qilingan funktsiya in`ektivdir.

Ta`rif-4***. A={$a_1$, $a_2$, …, $a_n$} ryukzak vektori ***o`suvchan (***tez o`suvchan***) deb ataladi, agar ixtiyoriy $j$=2, 3, …, $n$ lar uchun $a_j \geq a_{j-1}$ (mos ravishda $a_j = \sum_{i=1}^{j-1} a_i$) shartlar o`rinli bo`lsa.

Ko`rinib turibdiki, tez o`suvchan vektorlar o`suvchan ham bo`la oladi. A vektor uchun $max\ A$=max($a_j \mid 1 \leq j \leq n$) deylik. x nomanfiy son bo`lsin. [x] orqali eng katta $\leq x$ butun sonni belgilaylik.

Butun x va m>2 sonlar uchun x ni m bo`lganda eng kichik nomanfiy qoldiqni ($x$ mod $m$) orqali belgilaymiz. Ko`rish mumkinki,

$$(x, \text{ mod } m) = x - [x/t] \cdot t .$$

Ushbu munosabatni x=(x, mod m) + [x/m] $\cdot\ t$ tarzida ham yozish mumkin.

Endi modul bo`yicha ko`paytirishning ikki variantini aniqlaymiz. *A* ryukzak vektori va $m>max\ A$ butun soni va shunday natural $t<m$ sonini olamizki, *t* va *m* lar o`zaro tub, ya`ni eng katta umumiy bo`luvchi $(t, m)=1$ ga teng. Agar, shunday $B = (b_1, b_2, ..., b_n)$ vektor komponentlari barcha $i=1, 2, \ldots, n$ lar uchun

$b_i = (ta_i, \text{ mod } m)$, dlya i = 1,..., p ,

formula bilan hosil qilingan bo`lsa, u xolda B vektor A vektordan *m* modulga va *t* ko`paytuvchiga nisbatan modul bo`yicha ko`paytirish orqali hosil qilingan deb ataladi.

$(t, m)=1$ shart shunday teskari $t^{-1} = u$ sonning mavjudligini kafolatlaydiki, $tu \equiv 1 \pmod{m}$ shart o`rinli bo`ladi. Bu xolat B dan *t* va *u* larga nisbatan modul bo`yicha ko`paytirish orqali *A* ni hosil qilish mumkinligini anglatadi (t>max B, chunki b_i larning hammasi *mod m* bo`yicha olinadi).

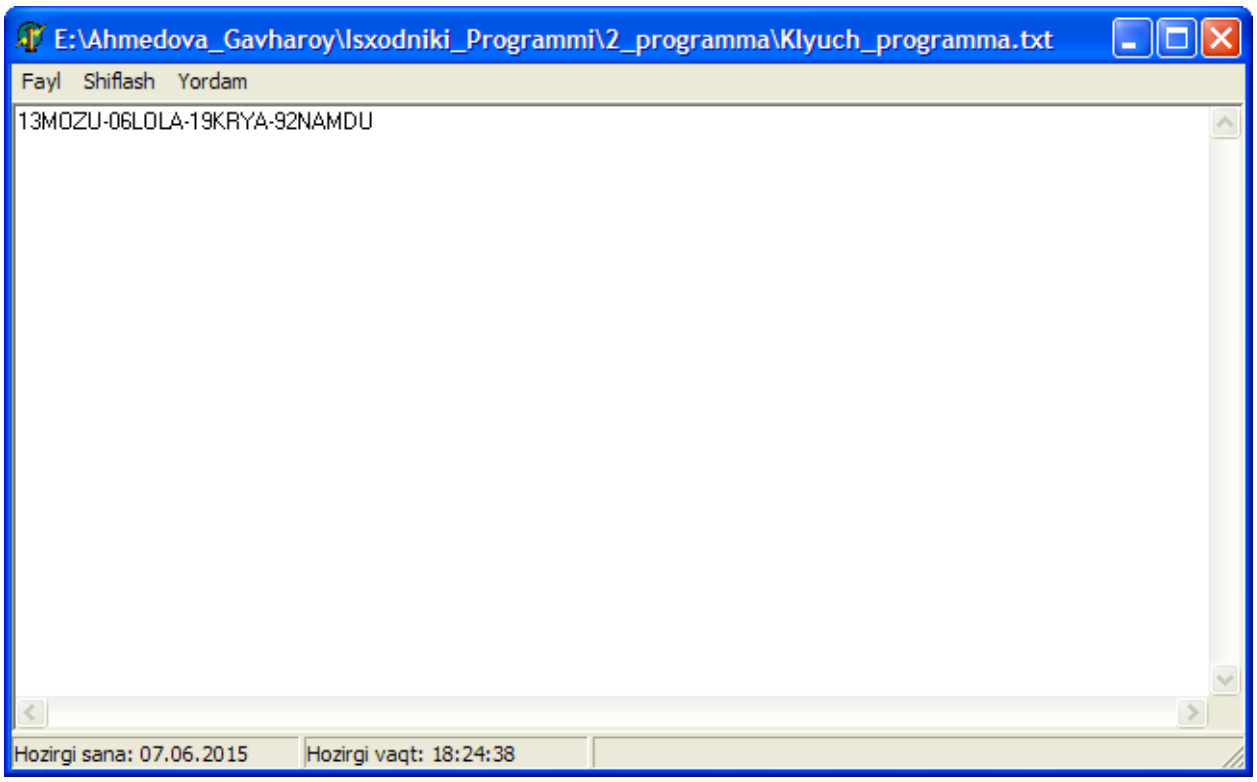
Agar yuqoridagi $t>max\ A$ shart o`ziga nisbatan kuchliroq bo`lgan $m > \sum_{i=1}^{n} a_i$ shart bilan almashtirilsa, u xolda B vektor A dan *m* va *t* ga nisbatan kuchli modul bo`yicha ko`paytirish orqali hosil qilingan deyiladi. Bu erda $m > \sum_{i=1}^{n} b_i$ munosabatning o`rinli bo`lishi shart emas va A vektor B dan *t* va *u* larga nisbatan modul bo`yicha ko`paytirish orqali hosil qilinadi.

Nossimmetrik kriptografiyaga oid dastur

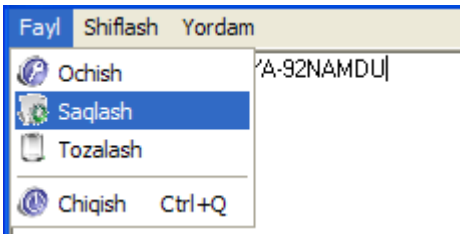
Bu dasturda fayllar bilan ishlashdan unuumli foydalanilgan. Ya'ni dasturda kiritilgan fayllar ni saqlash, uzatish , ochish umuman olganda fayllar ustida ish bajariladi. Masalan kiritilgan fayllarni **shifrlab** kerakli joyga joyga jo'natiladi. Jo'natilgan fayllni bu programma orqali ochib **shifrdan yechish** mumkin. Bu albatta foydalanuvchi tomoniga anchagina qulaylik va maxfiylikni beradi. Dastur Delphi dasturlash tilida tuzilgan. Buni quyidagi izox va rasmalarda ko'rishingiz mumkin:

Bu dastur tuzilishishida bizga Memo, Main Menu,Timer, OpenDialog, SaveDialog komponentalari kerak bo'ladi.

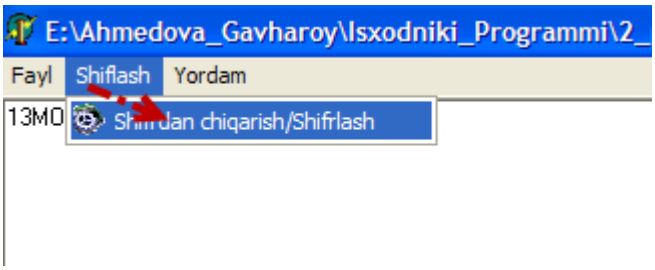
1) Dastur interfeysi quyidagicha :



2) Fayl menyusi quyidagilardan tashkil topgan:



3) 2-menyuda shirlash va shifrdan yechish qismi joylashgan:



4) Dasturni Delphi dasturlash tilida quyidagicha tuzilgan:

File-> Ochish qismiga quyidagicha kod yoziladi:

```
procedure TForm1.N5Click(Sender: TObject);
begin
if OpenDialog1.Execute then begin
  Form1.Caption := OpenDialog1.FileName;
  Memo1.Lines.LoadFromFile
    (OpenDialog1.FileName);
  Memo1.SelStart := 0;
 end;
end;
```

Saqlash:

```
procedure TForm1.N6Click(Sender: TObject);
begin
SaveDialog1.FileName := Form1.Caption;
 if SaveDialog1.Execute then begin
   Memo1.Lines.SaveToFile
     (SaveDialog1.FileName + '.txt');
   Form1.Caption:=SaveDialog1.FileName;
 end;
end;
```

Eng asosiysi bu **shifrlash**ni amalga oshirish hisoblanadi:

```
procedure TForm1.N3Click(Sender: TObject);
begin
if Memo1.Text=''then
begin
ShowMessage('Textni kiriting!!!');
end
else
cd:=12;
str:=Memo1.Text;
str1:=Decode(str,cd);
Memo1.Text:=str1;

end;
```

4.1 Bir tomonlamali funksiyalar.

Oddiy autentifikatsiyani tashkil etish sxemalari nafaqat parollarni uzatish, balki ularni saqlash va tekshirish turlari bilan ajralib turadi. Eng keng tarqalgan usul - foydalanuvchilar parolini tizimli fayllarda, ochiq holda saqlash usulidir. Bunda fayllarga o‘qish va yozishdan himoyalash atributlari o‘rnatiladi (masalan, operatsion tizimdan foydalanishni nazoratlash ro’yxatidaga mos imtiyozlarni tavsiflash yordamida). Tizim foydalanuvchi kiritgan parolni parollar faylida saqlanayotgan yozuv bilan solishtiradi. Bu usulda shifrlash yoki bir tomonlama funksiyalar kabi kriptografik mexanizmlar ishlatilmaydi. Ushbu usulning kamchiliga - niyati buzuq odamning tizimda ma’mur imtiyozlaridan, shu bilan birga tizim fayllaridan, jumladan parol fayllaridan foydalanish imkoniyatidir.

Xavfsizlik nuqtai nazaridan parollarni bir tomonlama funksiyalardan foydalanib uzatish va saqlash qulay hisoblanadi. Bu holda foydalanuvchi parolning ochiq shakli o’rniga uning bir tomonlama funksiya h(.) dan foydalanib olingan tasvirini yuborishi shart. Bu o‘zgartirish g‘anim tomonidan parolni uning tasviri orqali oshkor qila olmaganligini kafolatlaydi, chunki g‘anim yechilmaydigan sonli masalaga duch keladi.

Ko‘p martali parollarga asoslangan oddiy autentifikatsiyalash tizimining bardoshliga past, chunki ularda autentifikatsiyalovchi axborot ma’noli so‘zlarning nisbatan katta bo‘lmagan to‘plamidan jamlanadi. Ko‘p martali parollarning ta’sir muddati tashkilotning xavfsizligi siyosatida belgilanishi va bunday parollarni muntazam ravishda almashtirib turish lozim. Parollarni shunday tanlash lozimki, ular lug‘atda bo‘lmasin va ularni topish qiyin bo‘lsin.

Bir martali parollarga asoslangan autentifikatsiyalashda foydalanishga har bir so‘rov uchun turli parollar ishlatiladi. Bir martali dinamik parol faqat tizimdan bir marta foydalanishga yaroqli. Agar, hatto kimdir uni ushlab qolsa ham parol foyda bermaydi. Odatda bir martali parollarga asoslangan autentfikatsiyalash tizimi masofadagi foydalanuvchilarni tekshirishda qo‘llaniladi.

Foydalanuvchilarni autentifikatsiyalash uchun bir martali parollarni qo‘llashning quyidagi usullari ma’lum:

1. Yagona vaqt tizimiga asoslangan vaqt belgilari mexanizmidan foydalanish.

2. Legal foydalanuvchi va tekshiruvchi uchun umumiy bo‘lgan tasodifiy parollar ro’yxatidan va ularning ishonchli sinxronlash mexanizmidan foydalanish.

3. Foydalanuvchi va tekshiruvchi uchun umumiy bo‘lgan bir xil dastlabki qiymatli psevdotasodifiy sonlar generatoridan foydalanish.

Birinchi usulni amalga oshirish misoli sifatida SecurID autentikatsiyalash texnologiyasini ko‘rsatish mumkin. Bu texnologiya Security Dynamics kompaniyasi tomonidan ishlab chiqilgan bo‘lib, qator kompaniyalarning, xususan Cisco Systems kompaniyasining serverlarida amalga oshirilgan.

Vaqt sinxronizatsiyasidan foydalanib autentifikatsiyalash sxemasi tasodifiy sonlarni vaqtning ma’lum oralig‘idan so‘ng generatsiyalash algoritmiga asoslangan. Autentifikatsiya sxemasi quyidagi ikkita parametrdan foydalanadi:

• har bir foydalanuvchiga atalgan va autentifikatsiya serverida hamda foydalanuvchining apparat kalitida saqlanuvchi noyob 64-bitli sondan iborat maxfiy kalit;

• joriy vaqt qiymati.

Masofadagi foydalanuvchi tarmoqdan foydalanishga uringanida undan shaxsiy identifikatsiya nomeri RICHni kiritish taklif etiladi. PIN to‘rtta o‘nli raqamdan va apparat kaliti displeyida akslanuvchi tasodifiy sonning oltita raqamidan iborat. Server foydalanuvchi tomonidan kiritilgan PIN-koddan foydalanib ma’lumotlar bazasidagi foydalanuvchining maxfiy kaliti va joriy vaqt qiymati asosida tasodifiy sonni genera-siyalash algoritmini bajaradi. So‘ngra server generatsiyalangan son bilan foydalanuvchi kiritgan sonni taqqoslaydi. Agar bu sonlar mos kelsa, server foydalanuvchiga tizimdan foydalanishga ruxsat beradi.

Autentifikatsiyaning bu sxemasidan foydalanishda apparat kalit va serverning qat’iy vaqtiy sinxronlanishi talab etiladi. Chunki apparat kalit bir necha yil ishlashi va demak server ichki soati bilan apparat kalitining muvofiqligi asta-sekin buzilishi mumkin.

Ushbu muammoni hal etishda Security Dynamics kompaniyasi quyidagi ikki usuldan foydalanadi:

- apparat kaliti ishlab chiqilayotganida uning taymer chastotasining me’yoridan chetlashishi aniq o‘lchanadi. Chetlashishning bu qiymati server algoritmi parametri sifatida hisobga olinadi;
- server muayyan apparat kalit generatsiyalagan kodlarni kuzatadi va zaruriyat tug‘ilganida ushbu kalitga moslashadi.

Autentifikatsiyaning bu sxemasi bilan yana bir muammo bog‘liq. Apparat kalit generatsiyalagan tasodifiy son katta bo‘lmagan vaqt oralig‘i mobaynida haqiqiy parol hisoblanadi. Shu sababli, umuman, qisqa muddatli vaziyat sodir bo‘lishi mumkinki, xaker PIN-kodni ushlab qolishi va uni tarmoqdan foydalanishga ishlatishi mumkin. Bu vaqt sinxronizatsiyasiga asoslangan autentifikatsiya sxemasining eng zaif joyi hisoblanadi.

Bir martali paroldan foydalanuvchi autentifikatsiyalashni amalga oshiruvchi yana bir variant - «so‘rov-javob» sxemasi bo‘yicha autentifikasiyalash. Foydalanuvchi tarmoqdan foydalanishga uringanida server unga tasodifiy son ko‘rinishidagi so‘rovni uzatadi. Foydalanuvchining apparat kaliti bu tasodifiy sonni, masalan DES algoritmi va foydalanuvchining apparat kaliti xotirasida va serverning ma’lumotlar bazasida saqlanuvchi maxfiy kaliti yordamida rasshifrovka qiladi. Tasodifiy son - so‘rov shifrlangan ko‘rinishda serverga qaytariladi. Server ham o‘z navbatida o‘sha DES algoritmi va serverning ma’lumotlar bazasidan olingan foydalanuvchining maxfiy kaliti yordamida o‘zi generatsiyalagan tasodifiy sonni shifrlaydi. So‘ngra server shifrlash natijasini apparat kalitidan kelgan son bilan taqqoslaydi. Bu sonlar mos kelganida foydalanuvchi tarmoqdan foydalanishga ruxsat oladi. Ta’kidlash lozimki, «so‘rov-javob» autentifikatsiyalash sxemasi ishlatishda vaqt sinxronizatsiyasidan foydalanuvchi autentifikatsiya sxemasiga qaraganda murakkabroq.

Foydalanuvchini autentifikatsiyalash uchun bir martali paroldan foydalanishning ikkinchi usuli foydalanuvchi va tekshiruvchi uchun umumiy bo‘lgan tasodifiy parollar ruyxatidan va ularning ishonchli sinxronlash mexanizmidan foydalanishga asoslangan. Bir martali parollarning bo‘linuvchi ro‘yxati maxfiy parollar ketma-ketligi yoki to‘plami bo‘lib, har bir parol faqat bir

marta ishlatiladi. Ushbu ro‘yxat autentifikatsion almashinuv taraflar o‘rtasida oldindan taqsimlanishi shart. Ushbu usulning bir variantiga binoan so‘rov-javob jadvali ishlatiladi. Bu jadvalda autentifikatsilash uchun taraflar tomonidan ishlatiluvchi so‘rovlar va javoblar mavjud bo‘lib, har bir juft faqat bir marta ishlatilishi shart.

Foydalanuvchini autentifikatsiyalash uchun bir martali paroldan foydalanishning uchinchi usuli foydalanuvchi va tekshiruvchi uchun umumiy bo‘lgan bir xil dastlabki qiymatli psevdotasodifiy sonlar generatoridan foydalanishga asoslangan. Bu usulni amalga oshirishning quyidagi vari-antlari mavjud:

- *o‘zgartiriluvchi bir martali parollar ketma-ketligi.* Navbatdagi autentifikatsiyalash sessiyasida foydalanuvchi aynan shu sessiya uchun oldingi sessiya parolidan olingan maxfiy kalitda shifrlangan parolni yaratadi va uzatadi;
- *bir tomonlama funksiyaga asoslangan parollar ketma-ketligi.* Ushbu usulning mohiyatini bir tomonlama funksiyaning ketma-ket ishlatilishi (Lampartning mashhur sxemasi) tashkil etadi. Xavfsizlik nuqtai nazaridan bu usul ketma-ket o‘zgartiriluvchi parollar usuliga nisbatan afzal hisoblanadi.

Keng tarqalgan bir martali paroldan foydalanishga asoslangan au-tentifikatsiyalash protokollaridan biri Internet da standartlashtirilgan S/Key (RFC1760) protokolidir. Ushbu protokol masofadagi foydalanuvchilarning haqiqiyligini tekshirishni talab etuvchi ko‘pgina tizimlarda, xususan, Cisco kompaniyasining TACACS tizimida amalga oshirilgan.

4.1.1 Sertifikatlar asosida autentifikatsiyalash

Raqamli sertifikatlar ishlatilganida kompьyuter tarmoga foydalanuvchilari xususidagi hech qanday axborotni saklamaydi. Bunday axborotni foydalanuvchilarning o‘zi so‘rov sertifikatlarida taqdim etadilar. Bunda maxfiy axborotni, xususan maxfiy kalitlarni saqlash vazifasi foydalanuvchilarning o‘ziga yuklanadi.

Foydalanuvchi shaxsini tasdiklovchi raqamli sertifikatlar foydalanuvchilar so‘rovi bo‘yicha maxsus vakolatli tashkilot sertifikatsiya markazi SA (Certificate Authority) tomonidan, ma’lum shartlar bajarilganida beriladi. Ta’kidlash lozimki, sertifikat olish muolajasining o‘zi ham foydalanuvchining haqiqiyligini tekshirish (ya’ni, autentifikatsiyalash) bosqichini o‘z ichiga oladi. Bunda tekshiruvchi taraf sertifikatsiyalovchi tashkilot (sertifikatsiya markazi SA) bo‘ladi.

Sertifikat olish uchun mijoz sertifikatsiya markaziga shaxsini tasdiqlovchi ma’lumotni va ochiq kalitini takdim etishi lozim. Zaruriy ma’lumotlar ro’yxati olinadigan sertifikat turiga bog‘liq. Sertifikatsiyalovchi tashkilot foydalanuvchining haqiqiyligi tasdig‘ini tekshirganidan so‘ng o‘zining raqamli imzosini ochiq kalit va foydalanuvchi xususidagi ma’lumot bo‘lgan faylga joylashtiradi hamda ushbu ochiq kalitning muayyan shaxsga tegishli ekanligini tasdiqlagan holda foydalanuvchiga ser-tifikat beradi.

Sertifikat elektron shakl bo‘lib, tarkibida qo‘yidaga axborot bo‘ladi:

- ushbu sertifikat egasining ochiq kaliti;
- sertifikat egasi xususidagi ma’lumot, masalan, ismi, elektron pochta adresi, ishlaydigan tashkilot nomi va h.;
- ushbu sertifikatni bergan tashkilot nomi;
- sertifikatsiyalovchi tashkilotning elektron imzosi ushbu tashkilotning maxfiy kaliti yordamida shifrlangan sertifikatsiyadaga ma’lumotlar.

Sertifikat foydalanuvchini tarmoq resurslariga murojaat etganida autentifikatsiyalovchi vosita hisoblanadi. Bunda tekshiruvchi taraf vazifasini korporativ tarmoqning autentifikatsiya serveri bajaradi. Sertifikatlar nafaqat autentifikatsiyalashda, balki foydalanishning ma’lum xuquqlarini taqdim etishda

ishlatilishi mumkin. Buning uchun sertifikatga qo‘shimcha hoshiyalar kiritilib ularda sertifikatsiya egasining foy-dalanuvchilarning u yoki bu kategoriyasiga mansubligi ko‘rsatiladi.

Agar abonent axborot almashinuvi bo‘yicha sherigidan sertifikat tarkibidaga ochiq kalitni olsa, u bu sertifikatdagi sertifikatsiya markazining raqamli imzosini ushbu sertifikatsiya markazining ochiq kaliti yordamida tekshirish va ochiq kalit adresi va boshqa ma’lumotlari sertifikatda ko‘rsatilgan foydalanuvchiga tegishli ekanligiga ishonch hosil qilishi mumkin. Sertifikatlardan foydalanilganda foydalanuvchilar ro’yxatini ularning parollari bilan korporatsiya serverlarida saqlash zaruriyati yo‘qoladi. Serverda sertifikatsiyalovchi tashkilotlarning nomlari va ochiq kalitlarining bo‘lishi etarli.

Sertifikatlar asosida autentifikatsiyalash jarayonini amalga oshirishda sertifikatsiyalovchi tashkilot vazifasini kim bajarishi xususidaga masalani yechish muhim hisoblanadi. Xodimlarni sertifikat bilan ta’minlash masalasini korxonaning o‘zi yechishi juda tabiiy hisoblanadi. Korxona o‘zining xodimlarini yaxshi biladi va ular shaxsini tasdiqlash vazifasini o‘ziga olishi mumkin. Bu sertifikat berilishidaga dastlabki autentifikatsiyalash muolajasini osonlashtiradi. Korxonalar sertifikatlarni generatsiyalash, berish va ularga xizmat ko‘rsatish jarayonlarini avtomatlashtirishni ta’minlovchi mavjud dasturiy maxsulotlardan foydalanishlari mumkin. Masalan, Netscape Communications kompaniyasi serverlarini korxonalarga shaxsiy sertifikatlarini chiqarish uchun taklif etadi.

Sertifikatsiyalovchi tashkilot vazifasini bajarishda tijorat aso-sida sertifikat berish bo‘yicha mustaqil markazlar ham jalb etilishi mumkin. Bunday xizmatlarni, xususan, Verisign kompaniyasining sertifikatsiyalovchi markazi taklif etadi. Bu kompaniyaning sertifikatlari halqaro standart X.509 talablariga javob beradi. Bu sertifikatlar ma’lumotlar himoyasining qator maxsulotlarida, jumladan himoyalangan kanal SSL protokolida ishlatiladi.

4.1.2 Qat’iy autentifikatsiyalash

Kriptografik protokollarida amalga oshiriluvchi qat’iy autentifikatsiyalash g‘oyasi quyidagicha. Tekshiriluvchi (isbotlovchi) taraf qandaydir sirni bilishini namoyish etgan holda tekshiruvchiga o‘zining haqiqiy ekanligini isbotlaydi. Masalan, bu sir autentifikatsion almashish taraflari o‘rtasida oldindan xavfsiz usul bilan taqsimlangan bo‘lishi mumkin. Sirni bilishlik isboti kriptografik usul va vositalardan foydalanilgan holda so‘rov va javob ketma-ketligi yordamida amalga oshiriladi.

Eng muhimi, isbotlovchi taraf faqat sirni bilishligini namoyish etadi, sirni o‘zi esa autentifikatsion almashish mobaynida ochilmaydi. Bu tekshiruvchi tarafning turli so‘rovlariga isbotlovchi tarafning javoblari yordami bilan ta’minlanadi. Bunda yakuniy so‘rov faqat foydalanuvchi siriga va protokol boshlanishida ixtiyoriy tanlangan katta sondan iborat boshlangach so‘rovga bog‘liq bo‘ladi.

Aksariyat hollarda qat’iy autentifikatsiyalashga binoan har bir foydalanuvchi o‘zining maxfiy kalitiga egaligi alomati bo‘yicha autentifikatsiyalanadi. Boshqacha aytganda foydalanuvchi uning aloqa bo‘yicha sherigining tegishli maxfiy kalitga egaligini va u bu kalitni axborot almashinuvi bo‘yicha haqiqiy sherik ekanligini isbotlashga ishlata olishi mumkinligini aniqlash imkoniyatiga ega.

X.509 standarti tavsiyalariga binoan qat’iy autentifikatsiyalashning quyidagi muolajalari farqlanadi:

- bir tomonlama autentifikatsiya;
- ikki tomonlama autentifikatsiya;
- uch tomonlama autentifikatsiya.

Bir tomonlama autentifikatsiyalash bir tomonga yo‘naltirilgan axborot almashinuvini ko‘zda tutadi. Autentifikatsiyaning bu turi quyidagilarga imkon yaratadi:

- axborot almashinuvchining faqat bir tarafini haqiqiyligini tasdiklash;
- uzatilayotgan axborot yaxlitligining buzilishini aniqlash;

- "uzatishning takrori" tipidaga xujumni aniqlash;

- uzatilayotgan autentifikatsion ma’lumotlardan faqat tekshiruvchi taraf foydalanishini kafolatlash.

Ikki tomonlama autentifikatsilash bir tomonliligiga nisbatan isbotlovchi tarafga tekshiruvchi tarafning qo‘shimcha javobi bo‘ladi. Bu javob tekshiruvchi tomonni aloqaning aynan autentifikatsiya ma’lumotlari mo‘ljallangan taraf bilan o‘rnatilayotganiga ishontirish lozim.

Ta’kidlash lozimki, ushbu turkumlash shartlidir. Amalda ishlatiluvchi usul va vositalar to‘plami autentifikatsiya jarayonini amalga oshirish-dagi muayyan shart-sharoitlarga bog‘liq. Qat’iy autentifikatsiyaning o‘tkazilishi ishlatiladigan kriptografik algoritmlar va qator qo‘shimcha parametrlarni taraflar tomonidan so‘zsiz muvofiklashtirishni talab etadi.

Qat’iy autentifikatsiyalashning muayyan variantlarini ko‘rishdan oldin bir martali parametrlarning vazifalari va imkoniyatlariga to‘xtash lozim. Bir martali parametrlar ba’zida "nonces" - bir maqsadga bir mar-tadan ortiq ishlatilmaydigan kattalik deb ataladi.

Bir martali parametrlarning quyidagi ishlatilish misollarini ko‘rsatish mumkin:

- "so‘rov-javob" prinsipida qurilgan protokollarda o‘z vaqtidaligini tekshirish. Bunday tekshirishda tasodifiy sonlar, soatlarni sinxronlash bilan vaqt belgalari yoki muayyan juft (tekshiruvchi, isbotlovchi) uchun ketma-ketliklarning nomerlaridan foydalanish mumkin;

- o‘z vaqtidaligini yoki noyoblik kafolatini ta’minlash. Protokolning bir martali parametrlarini bevosita (tasodifiy sonni tanlash yo‘li bilan) yoki bilvosita (bo‘linuvchi sirdagi axborotni taxlillash yordamida) nazoratlash orqali amalga oshiriladi;

- xabarni yoki xabarlar ketma-ketligini bir ma’noli identifikatsiyalash. Bir ohangda o‘suvchi ketma-ketlikning bir martali qiymatini (masalan, seriya nomerlari yoki vaqt belgilari ketma-ketliga) yoki mos uzun-likdagi tasodifiy sonlarni tuzish orqali amalga oshiriladi.

Ta’kidlash lozimki, bir martali parametrlar kriptografik protokollarning boshqa variantlarida ham (masalan, kalit axborotini taqsimlash protokollarida) keng qo‘llaniladi.

Qat’iy autentifikatsiyalash protokollarini qo‘llaniladigan kriptografik algoritmlariga bog‘liq holda quyidagi guruhlarga ajratish mumkin:

- shifrlashning simmetrik algoritmlari asosidagi qat’iy autentifikatsiyalash protokollari;
- bir tomonlama kalitli xesh-funksiyalar asosidagi qat’iy autentifikatsiyalash protokollari;
- shifrlashning asimmetrik algoritmlari asosidagi qat’iy autentifikatsiyalash algoritmlari;
- elektron raqamli imzo asosidaga qat’iy autentifikatsiyalash algoritmlari.

4.1.3 Raqamli imzodan foydalanish asosidagi autentifikatsiyalash.

X.509 standartining tavsiyalarida raqamli imzo, vaqt belgisi va tasodifiy sonlardan foydalanish asosidagi autentifikatsiyalash sxemasi spetsifikatsiyalangan. Ushbu sxemani tavsiflash uchun quyidagi belgilashlarni kiritamiz:

- t_A, r_A va g_V - mos holda vaqt belgisi va tasodifiy sonlar;
- S_A - qatnashuvchi A generatsiyalagan imzo;
- ***certA*** - qatnashuvchi A ochiq kalitining sertifikati;
- ***certB*** - qatnashuvchi V ochiq kalitining sertifikati;

Misol tariqasida autentifikatsiyalashning quyidagi protokollarini keltiramiz:

1. Vaqt belgisidan foydalanib bir tomonlama autentfikatsiyalash: A→B :

$$certA,\ t_A,\ B,\ S_A(t_A,B)$$

Qatnashuvchi V ushbu xabarni olganidan so‘ng vaqt belgisi t_A ning to‘g‘riligani, olingan identifikator V ni va sertifikat ***certA*** daga ochiq kalitdan foydalanib raqamli imzo $S_A(tA,B)$ ning korrektligini tekshiradi.

2. Tasodifiy sonlardan foydalanib bir tomonlama autentifikatsiya-lash:

A←B : g_V

A→B : certA, r_A, B, $S_A(r_A, r_B, B)$

Qatnashuvchi V qatnashuvchi A dan xabarni olib aynan u xabarning adresati ekanligiga ishonch hosil qiladi; sertifikat ***certA*** dan olingan qatnashuvchi A ochiq kalitidan foydalanib ochiq ko‘rinishda olingan $\boldsymbol{g_A}$ soni, birinchi xabarda jo‘natilgan gv soni va o‘zining identifikatori V os-tidagi imzo $S_A(r_A, r_B, B)$ ning korrektligini tekshiradi. Imzo chekilgan tasodifiy son $\boldsymbol{g_A}$ ochiq matnni tanlash bilan xujumni oldini olish uchun ishlatiladi.

3. Tasodifiy sonlardan foydalanib ikki tomonlama autentifikatsiyalash:

$A \leftarrow V : g_V$

$A \rightarrow B$: cert$A$, r_A, B, $S_A(r_A, r_B, B)$

$A \leftarrow B$:cert$B$,A, $S_B(r_A, r_B, A)$

5.1 Elektron raqamli imzo.

O‘zbekiston Respublikasining “Elektron raqamli imzo to‘g‘risida”gi Qonuniga muvofiq, elektron raqamli imzo — elektron hujjatdagi mazkur elektron hujjat axborotini elektron raqamli imzoning yopiq kalitidan foydalangan holda maxsus o‘zgartirish natijasida hosil qilingan hamda elektron raqamli imzoning ochiq kaliti yordamida elektron hujjatdagi axborotda xatolik yo‘qligini aniqlash va elektron raqamli imzo yopiq kalitining egasini identifikatsiya qilish imkoniyatini beradigan imzo.

Elektron raqamli imzoning yopiq kaliti — elektron raqamli imzo vositalaridan foydalangan holda hosil qilingan, faqat imzo qo‘yuvchi shaxsning o‘ziga ma’lum bo‘lgan va elektron hujjatda elektron raqamli imzoni yaratish uchun mo‘ljallangan belgilar ketma-ketligi.

Elektron raqamli imzoning ochiq kaliti — elektron raqamli imzo vositalaridan foydalangan holda hosil qilingan, elektron raqamli imzoning yopiq kalitiga mos keluvchi, axborot tizimining har qanday foydalanuvchisi foydalana oladigan va elektron hujjatdagi elektron raqamli imzoning haqiqiyligini tasdiqlash uchun mo‘ljallangan belgilar ketma-ketligi.

Mazkur Qonunga ko‘ra elektron raqamli imzodan foydalanish sohasini davlat tomonidan tartibga solishni O‘zbekiston Respublikasi Vazirlar Mahkamasi va u maxsus vakolat bergan organ amalga oshiradi. Aloqa, axborotlashtirish va telekommunikatsiya texnologiyalari sohasida O‘zbekiston Respublikasi aloqa, axborotlashtirish va telekommunikatsiya texnologiyalari davlat qo‘mitasi ERIni ro‘yxatga oluvchi vakolatli davlat organi hisoblanadi. Mazkur vazifa Qo‘mita tizimidagi «UNICON.UZ» – Fan-texnika va marketing tadqiqotlari markazi Davlat unitar korxonasi qoshidagi Elektron raqamli imzolar kalitlarini ro‘yxatga olish markazi tomonidan amalga oshiriladi.

Elektron raqamli imzolar kalitlarini ro‘yxatga olish markazi elektron raqamli imzoning ochiq kalitlari va shifrlash sertifikatlaridan quyidagi maqsadlarda foydalanishni ta’minlash uchun mo‘ljallangan:

- uzatiladigan elektron hujjatlar va ommaviy axborot resurslarining butunligini, shuningdek ularning ishonchli autentifikatsiya qilinishini nazorat qilish;
- axborot o‘zaro hamkorligi sub’ektlarining yuridik jihatdan ahamiyatli elektron identifikatsiyalash tizimini yaratish;
- tizim sub’ektlarining axborot o‘zaro ishlashida xavfsizlik va foydalana olishning ajratilishini ta’minlash;
- axborot o‘zaro hamkorligi sub’ektlarining elektron raqamli imzo kalitlarini boshqarish tizimini yaratish.

Kalitlarni ro‘yxatga olish markazi «Elektron raqamli imzo to‘g‘risida»gi Qonun talablariga muvofiq vazifa va funksiyalarni bajaradi.

Kalitlarni ro‘yxatga olish markazi tomonidan tayyorlanadigan elektron raqamli imzo kalitining sertifikati ITU-T X.509, RFC3279, RFC3280 xalqaro tavsiyalarida belgilangan formatdan foydalanadi.

Dasturiy ta’minot o‘z ichiga Sertifikatlashtirish markazi va ma’muriy boshqaruvni oladi. Sertifikatlashtirish markazining serveri ERI kalitlarini ro‘yxatga olish markazi funksiyalarining kompleksini ta’minlaydi va ERI ochiq kalitlari sertifikatlarining muhofazalangan saqlash joyidan iborat. Ma’muriy boshqaruvning

dasturiy ta’minoti o‘z funksiyalarini bajarishlari uchun Kalitlarni ro‘yxatga olish markazini uzoqdan turib boshqarilishini ta’minlaydi.

Qabul qilib olingan ma’lumotlarning haqiqiy yoki haqiqiy emasligini aniqlash masalasini, ya’ni ma’lumotlar autentifikatsiyasi masalasining mohiyati haqida to‘xtalamiz.

Har qanday yozma xat yoki hujjatning oxirida shu hujjatni tuzuvchisi yoki tuzish uchun javobgar bo‘lgan shaxsning imzosi bo‘lishi tabiiy holdir. Bunday holat odatda quyidagi ikkita maqsaddan kelib chiqadi. Birinchidan, ma’lumotni olgan tomon o‘zida mavjud imzo namunasiga olingan ma’lumotdagi imzoni solishtirgan holda shu ma’lumotning haqiqiyligiga ishonch hosil qiladi. Ikkinchidan, shaxsiy imzo ma’lumot hujjatiga yuridik jihatdan mualliflikni kafolatlaydi. Bunday kafolat esa savdo–sotiq, ishonchnoma, majburiyat va shu kabi bitimlarda alohida muhimdir[3].

Hujjatlardagi qo‘yilgan shaxsiy imzolarni soxtalashtirish nisbatan murakkab bo‘lib, shaxsiy imzolarning mualliflarini hozirgi zamonaviy ilg‘or kriminalistika uslublaridan foydalanish orqali aniqlash mumkin. Ammo elektron raqamli imzo xususiyatlari bundan farqli bo‘lib, ikkilik sanoq sistemasi xususiyatlari bilan belgilanadigan xotira registrlari bitlariga bog‘liq. Xotira bitlarining ma’lum bir ketma-ketligidan iborat bo‘lgan elektron imzoni ko‘chirib biror joyga qo‘yish yoki o‘zgartirish kompyuterlar asosidagi aloqa tizimlarida murakkablik tug‘dirmaydi.

Bugungi yuqori darajada rivojlangan butun dunyo sivilizatsiyasida hujjatlar, jumladan maxfiy hujjatlarning ham, elektron ko‘rinishda ishlatilishi va aloqa tizimlarida uzatilishi keng qo‘llanilib borilayotganligi elektron hujjatlar va elektron imzolarning haqiqiyligini aniqlash masalalarining muhimligini keltirib chiqarmoqda.

Ochiq kalitli kriptografik tizimlar qanchalik qulay va kriptobardoshli bo‘lmasin, autentifikatsiya masalasining to‘la yechilishiga javob bera olmaydi. Shuning uchun autentifikatsiya uslubi va vositalari kriptografik algoritmlar bilan birgalikda kompleks holda qo‘llanilishi talab etiladi.

Quyida ikkita (A) va (B) foydalanuvchilarning aloqa munosabatlarida autentifikatsiya tizimi raqib tomonning o‘z maqsadi yo‘lidagi qanday hatti-harakatlaridan va kriptotizim foydalanuvchilarining foydalanish protokolini o‘zaro buzilishlardan saqlashi kerakligini ko‘rsatuvchi holatlar ko‘rib chiqiladi.

5.1.1 DSA ERI standarti. ГОСТ Р 34.10-94 elektron raqamli imzosi

1991 yilda NIST (National Institute of Standard and Technology) tomonidan DSA (Digital Signature Algorithm) algoritmiga asoslangan DSS (Digital Signature Standard) ERI standartining loyihasi muhokamaga qo‘yildi. Ushbu algoritm bardoshliligi yetarli katta tub xarakteristikaga ega bo‘lgan chekli maydonda diskret logarifmlash masalasining murakkabligiga asoslangan [5, 17, 23]. Quyida algoritm qadamlari ketma-ketligi keltirilgan.

Imzoni shakllantirish

1. Ma’lumot jo‘natuvchi M -ma’lumotni va quyidagi parametrlarni keng doiradagi tizim foydalanuvchilariga ochiq e’lon qiladi:

p – tub son, $2^{512} < p < 2^{1024}$, bit uzunligi 64 ga karrali;

q - tub son, $2^{159} < q < 2^{160}$, $p-1$ ning bo‘luvchisi;

$g = h^{(p-1)/q} \bmod p$, bu yerda h ushbu $0 < h < p$ va $h^{(p-1)/q} \bmod p > 1$ shartlarni qanoatlantiruvchi butun son;

y – ochiq kalit bo‘lib, $y = q^x \bmod p$ formula orqali aniqlanadi. Bu yerda x – maxfiy kalit bo‘lib, $0<x<q$ oraliqdan olingan va faqat imozolovchining o‘zigagina ma’lum;

$H(M)$ – M ma’lumotdan $[1;q]$ oraliqdagi butun sonni generatsiya qiluvchi xesh-funksiya.

2. Ma’lumot jo‘natuvchi $0<k < q$ oraliqdan tasodifiy k sonni tanlaydi, uni maxfiy tutadi va imzo generatsiyasidan keyin darhol yo‘qotadi.

3. Ma’lumot jo‘natuvchi r va s qiymatlarni quyidagi qonuniyat orqali hisoblaydi:

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

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

M - ma’lumotga qo‘yilgan imzo (r, s) sonlar juftligidan iborat.

Imzoni tekshirish. Qabul qiluvchi *M'* ma'lumotni va (*r', s'*) imzoni qabul qilib oladi. У *M* va *M'* ma'lumotlarning mos kelishini tekshirishi lozim. Buning uchun u quyidagi qadamlar ketma-ketligini bajaradi:

1. $0 < s' < q$ yoki $0 < r' < q$ shartlardan birortasi bajarilmasa, imzo qalbaki deb hisoblanadi va imzoni tekshirish tugatiladi.

2. $v = (s')^{-1} (mod\ q)$ topiladi.

3. $z_1 = H(M')\ v\ mod\ q$, $z_2 = r'\ v\ mod\ q$ hisoblanadi.

4. Keyin $u = g^{z_1} y^{z_2}\ mod\ p\ mod\ q$ hisoblanadi.

5. Agar $r' = u$ tenglik o‘rinli bo‘lsa, u holda imzo haqiqiy va $M = M'$ tenglik to‘g‘ri.

Algoritmning to‘g‘riligi. $M = M'$, $s' = s$ va $r' = r$ bo‘lsin. U holda $r = u$ tenglik o‘rinli bo‘lishi ko‘rsatiladi.

Demak, $v = (s')^{-1}\ mod\ q$, $z_1 = H(M')\ v\ mod\ q$, $z_2 = r'\ v\ mod\ q$ ekanligidan, quyidagini yozish mumkin:

$$u = g^{z1} y^{z1}\ mod\ p\ mod\ q = g^{H(M)s-1} g^{xrs-1}\ mod\ p\ mod\ q =$$
$$= g^{k(xr+H(M))-1(xr+H(M))}\ mod\ p\ mod\ q = g^k\ mod\ p\ mod\ q = r.$$

Bundan ko‘rish mumkinki, $r = u$ tenglik o‘rinli. Shunday qilib, algoritm to‘g‘riligi isbotlandi.

5.1.2 ГОСТ Р 34.10-94 elektron raqamli imzosi

Ushbu paragrafda 2000 yilgacha Rossiya standarti hisoblangan ГОСТ Р 34.10–94 ERI algoritmi qarab chiqiladi. Bu algoritm DSA algoritmiga o‘xshash va quyidagi boshlang‘ich ochiq parametrlardan foydalanadi:

1) Uzunligi L bo‘lgan katta p tub son tanlanadi, bu yerda L son 509 bitdan 512 bitgacha yoki 1020 bitdan 1024 bitgacha oraliqdan tanlanadi, ya'ni $2^{509} < p < 2^{512}$ yoki $2^{1020} < p < 2^{1024}$.

2) Uzunligi L_1 bo‘lgan katta q tub son tanlanadi, bu yerda L_1 son 254 bitdan 256 bitgacha oraliqdan tanlanadi, ya'ni $2^{254} < p < 2^{256}$.

3) $g^q \bmod p = 1$ shartni qanoatlantiruvchi $0 < g < p-1$ oraliqdagi g son tanlanadi.

4) $y = g^x \bmod p$ dan y - ochiq kalit hisoblanadi, bu yerda $0 < x < q$ oraliqdan olingan x -maxfiy kalit.

5) $H(M)$ - xesh-funksiya berilgan M - ma'lumot bo'yicha hisoblangan butun son bo'lib, *1* dan q gacha oraliqdagi qiymatlarni qabul qiladi, ya'ni $1 < H(M) < q$.

Imzoni generatsiya qilish algoritmi. Boshlang'ich ma'lumotlar: M - ma'lumot, berilgan parametrlar va maxfiy kalit. Natija: imzo - (r, s).

1) $1 \le k \le q$ intervaldan tasodifiy k soni olinadi, u maxfiy saqlanadi va imzo qo'yilgandan keyin darhol yo'qotiladi.

2) $r = (g^k \bmod p)(\bmod q)$ hisoblanadi.

3) Jo'natilayotgan M - ma'lumotning $e := H(M)$ - xesh qiymati hisoblanadi.

4) Agar $r = 0$ yoki $H(M) \bmod q = 0$ bo'lsa, u holda 1- qadamga o'tilib, boshqa k tanlanadi.

5) $s = (xr + kH(M)) \bmod q$ hisoblanadi, bu yerda maxfiy kalit x faqat imzo qo'yuvchining o'zigagina ma'lum.

6) Agar $s = 0$ bo'lsa, u holda 1-qadamga boriladi.

7) M ma'lumot imzosi - (r, s) juftligidan iborat.

Imzoni tekshirish algoritmi. Boshlang'ich ma'lumotlar: M ma'lumot, berilgan parametrlar, imzoni tekshirish kaliti va M ma'lumot imzosi. Natija: imzo haqiqiyligi yoki qalbakiligi haqidagi tasdiq.

1) Agar $1 \le r, s \le n - 1$ shart bajarilmasa, u holda imzo qalbaki va imzoni tekshirish algoritmi tugatiladi. Bu shartlar bajarilsa keyingi qadamga o'tiladi.

2) $e := h(m)$ hisoblanadi.

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

4) $u_1 := sw \bmod q$ hisoblanadi.

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

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

7) Agar $u = r$ shart bajarilsa, u holda imzo haqiqiy, aks holda imzo qalbaki va imzoni tekshirish algoritmi tugatiladi.

ГОСТ Р 34.10-94 imzo algoritmining to‘g‘riligi. ГОСТ Р 34.10-94 elektron raqamli imzo generatsiyasi algoritmidan olingan r parametrning qsiymatini imzoni tekshirish algoritmidagi u parametr qiymati bilan tengligini ko‘rsatishimiz kerak.

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

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

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

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

= / $(g^q \bmod p)=1$ shartga ko‘ra, $(g^q \bmod p)^{xw \bmod q} (\bmod q)=1$ tenglik o‘rinli/=

$= g^{kH(M)w \bmod q} \bmod p \ (\bmod q) =$ / $w=H(M)^{(q-2)} \bmod q$, $0<H(M)<q$ (q –tub) shartga va Eylera – Ferma teoremasiga ko‘ra $H(M)^{(q-2)} \bmod q= H(M)^{-1}$ ekanligi kelib chiqadi, shunga ko‘ra g ning darajasini $kH(M)w=kH(M)H(M)^{q-2} \bmod q= kH(M)H(M)^{-1}=k$ kabi ifodalash mumkin / $= g^k \bmod p \ (\bmod q) = r$. Shunday qilib talab qilingan shart ko‘rsatildi.

III.Xulosa.

Zamonaviy axborot kommunikatsiya texnologiyalarining, ayniqsa internetning keng joriy qilinishi insoniyatga ko`plab imkoniyatlarni tuhfa qilmoqda.Ma`lumotlarga qaraganda ayni kunda dunyo bo`yicha internet xizmatidan muntazam foydalanuvchilar soni 300 milliondan oshib ketdi. e`tiborlisi shuki bu ko`rsatkich soniyalar ichida o`zgarib boryapti. Har ikki-uch daqiqada bir kishi ro`yxatdan o`tayotgani fikrimiz dalilidir. Yana bir hayratlinarli raqam, bir kunda 7 milliondan ortiq veb-sahifalar yaratilyapti. Internetning bu qadar ommalashuviga uning axborotni tez va arzon narxda etkazib berishi asosiy sabab bo`lmoqda. Pochta xizmati bilan taqqoslaganda ‘o`rgimchak to`ri’ning xizmati 720 barobar tez va 355 barobar arzondir.

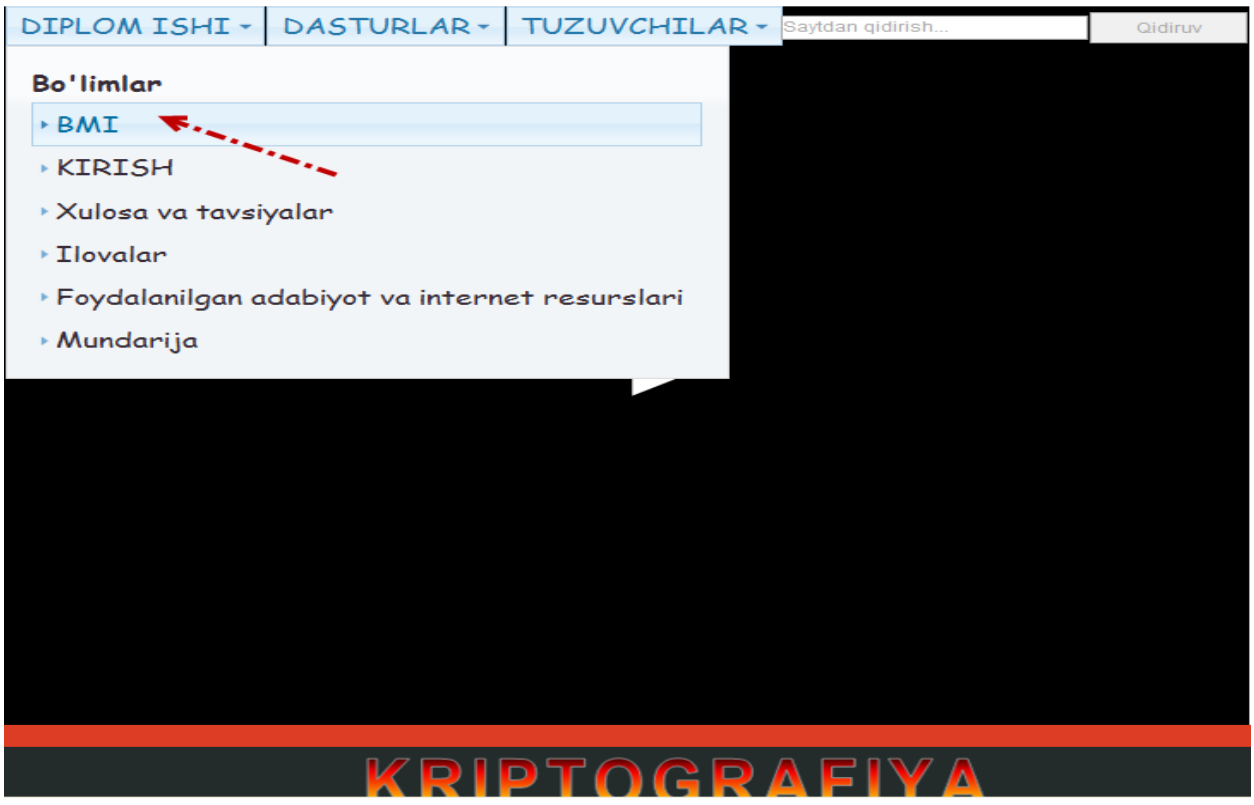
Internetda axborotlarni matnli, audio, video, grafik ob`ektlar, baza ma`lumotlari, dasturlar va boshqa ko`rinishda kuzatish mumkin. Mazkur xizmatga ulangan har qanday kishi istalgan vaqtda-kechasimi yo kunduzi, bir turdagi materiallar bilan bir necha marta tanishishi, tarmoqqa ma`lumotlar joylashtirishi, ularni ko`paytirishi mumkin.

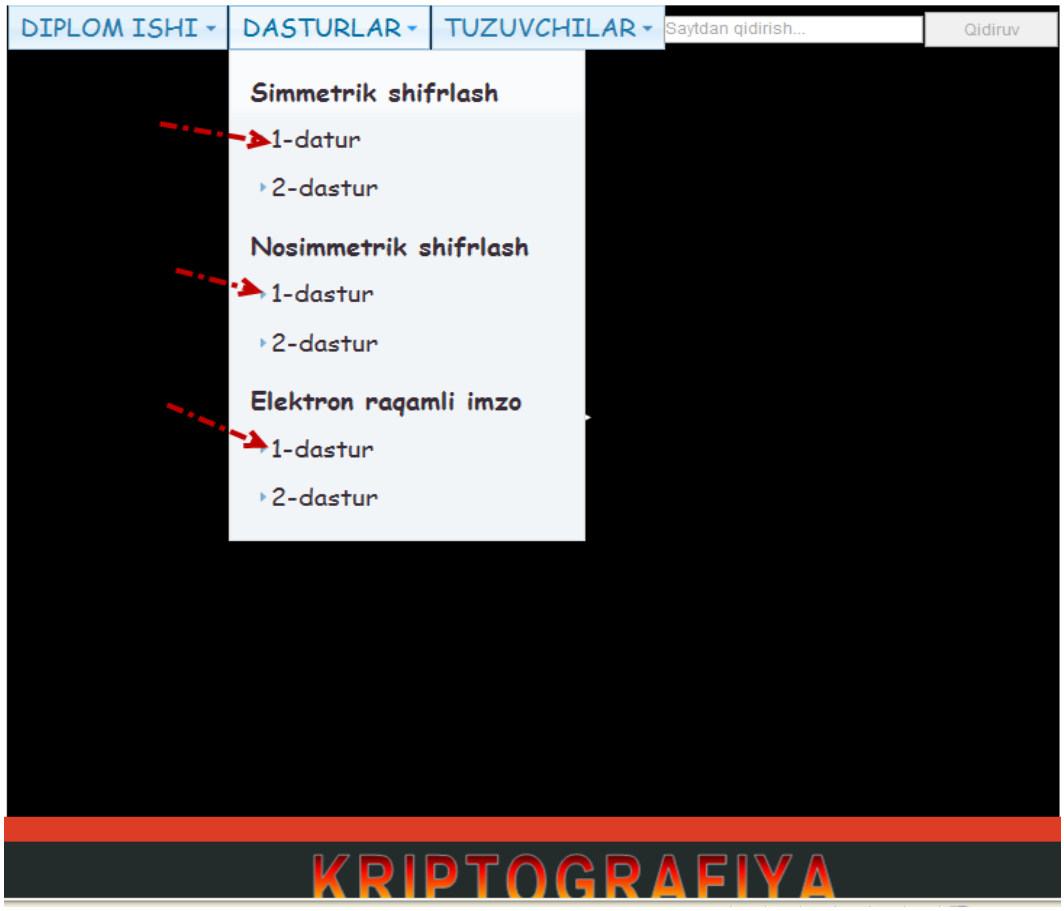
Afsuski, zamonaviy axborot kommunikatsiya texnologiyalarining keng joriy qilinishi insoniyatga ko`plab imkoniyatlarni tuhfa etish barobarida, jamiyatga bir qator muammolar, xususan, kompyuter jinoyatchiligi va kiberterrorizm xavfini ham paydo qilmoqda. So`nggi kunlarda ommaviy axborot vositalarida kiberjinoyatchilik, kiberterrorizm singari yangi atamalarning tez – tez tilga olinayotgani bu borada insoniyat oldida jiddiy xavf paydo bo`layotganini anglatadi. Bu kabi jinoyatlar, eng avvalo kompyuterlar, kompyuter tarmoqlari va tizimlari ishiga noqonuniy aralashuv orqali ma`lumotlarni o`g’irlash, o`zlashtirish, o`zgartirish kabi harakatlarda namoyon bo`lmoqda. Shu sababli axborot xavfsizligini ta`minlashga e`tiborsizlik bilan qarashga haqqimiz yo`q. Axborot xavfsizligini ta`minlash kechiktirib bo`lmaydigan va

barcha bilishi hamda o`rganishi bo`lgan muammo hisoblanadi. Bu muammoni echish uchun qadim davrlardan boshlab insonlar turli xil usul va uslublardan foydalanishgan. Ushbu usul va uslublarni o`rganishgan, ularni takomillashtirishgan hamda yangilarini yaratishgan. O`z vaqtida unumli qo`llanilgan musul va uslublarni unutmasligimiz hamda ularni o`rganish orqali yangilarini yaratishimizni davr taqoza qiladi. Axborot xavfsizligini ta`minlashning usullaridan biri kriptografiyadir. Shu sababli, yuqorida keltirilgan fikrga tayangan holda ushbu bitiruv malakaviy ishi, ‘Kriptografiya masalalarni yechishda bir tomonlama funksiyalardan foydalanish’ mavzusi bo`yicha biz axborot, axborotning jamiyatdagi o`rni, hozirgi axborot kommunikatsiya texnologiyalari davrida elektron axborotlar, axborotlashgan jamiyatda elektron hujjatlar hamda ularning harakati va ular xavfsizligini ta`minlash haqida fikrlarimizni keltirib o`tdik.Biz ushbu bitiruv malakaviy ishida ‘RSA usulida matnlarni shifrlash va deshifrlash dasturini yaratish’ mavzusi bo`yicha axborot asrida eng muhim masalalar hisoblangan ‘Axborotlashgan jamiyatda elektron hujjatlar’ ga tavsif bergach ‘Axborot xavfsizligi va axborot urushlari’, ‘Axborotlar xavfsizligi tushunchalari va himoya tizimlari’ hamda ‘Kriptografiya – maxfiy xabarning ma`nosini yashirish’ masalalariga to`xtalib o`tdik. Keyin esa kriptografiya haqida qisqacha ma`lumot berilgandan so`ng bevosita Simmetrik va nosimmetrik usulida matnlarni shifrlash va deshifrlash haqidagi tavsiflarimizni keltirdik hamda mutanosib dasturlarni tuzdik. Dastur DELPHI tilida yaratildi.

ILOVALAR

Bitiruv malakaviy ishning umumiy interfeysi quyidagicha:





BMI TUZILISHI SXEMASI

Mavzu: Kriptografik masalalarni yechishda bir tomonli funksiyalarni qo'llash.

Reja:

Tuzuvchilar:

Ahmedova Gavharoyning

Foydalanilgan adabiyot va internet resurslari.

1 Каримов И.А. Юксак маънавият енгилмас куч. –Т.: «Ўзбекистон», 2009. -216 б.

2 Karimov I. A. Mamlakatimizni modernizatsiya qilish va kuchli fuqarolik jamiyati barpo etish – ustuvor maqsadimizdir. (2010 yil 27 yanvarda bo‘lib o‘tgan O‘zbekiston Respublikasi Oliy Majlisi Qonunchilik palatasi va Senatining qo‘shma majlisidagi ma’ruzasi. Manba: http:www.press-service.uz/uz/news/archive/ dokladi).

3 Акбаров Д. Й. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг кўлланишлари. ”Ўзбекистон маркаси” нашриёти. Тошкент – 2009 йил, -398 б.

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

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

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

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

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

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

10 Молдовян Н.А., Молдовян А. А., Еремеев М.А. Криптография: от при-митивов к синтезу алгоритмов. –СПб.: БХВ-Петербург, 2004. -448 стр.

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

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

261 стр.

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

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

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

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

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

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

19 www.ziyonet.uz

20. www.intuit.ru

21. http//all-ebooks.com

22. www.kodges.ru

23. www.mirknig.ru

24. www.rsa.com

VI. Mundarija.