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

BUXORO MUHANDISLIK TEXNOLOGIYA INSTITUTI

«Informatika va axborot texnologiyalari» kafedrasi

5140900 – Kasb ta’limi («Informatika va axborotlar texnologiyalasi») ta’lim yo’nalishi bo’yicha

Uinstonning ‘ikkilangan kvadrat’ shifri tahlili va uni dasturini yaratish mavzusidagi

BITIRUV MALAKAVIY ISH

Bajardi: **22-09 MIIT guruhi talabasi**
Majidov Muhammad Bahodir o’g’li

Rahbar: **Sohibov T.F.**

Himoyaga ruxsat etildi

“____”_____2013y.

Kafedra mudiri: _____ dots. Razzoqov Sh.I.

BUXORO - 2013

BUXORO YUQORI TEXNOLOGIYALAR MUHANDISLIK TEXNIKA INSTITUTI
«TEXNOLOGIK JARAYONLARNI AVTOMATLASHTIRISH» fakulteti

«Informatika va axborot texnologiyalari» kafedrasi

5140900 – Kasb ta'limi («Informatika va axborotlar texnologiyasi») ta'lim yo'nalishi
22-09 MIIT guruhi

«Tasdiqlayman»_____
Kafedra mudiri dots.Razzoqov Sh.I.
«_____» _____ 2012 y.

BITIRUV MALAKAVIY ISHI BO'YICHA TOPSHIRIQ

Talabasi *Majidov Muhammad Bahodir o'g'li*

1. Bitiruv malakaviy ish mavzusi *Uinstonning 'ikkilangan kvadrat' shifri tahlili va uni dasturini yaratish.*

Kafedra majlisida 12.11.2012 yil tasdiqlangan.

2. Bitiruv malakaviy ishini topshirish muddati: 5.06.2013yil

3. Bitiruv malakaviy ishni bajarish uchun kerakli ma'lumotlar:

Adabiyotlar, BMI mavzusi bo'yicha nazariy ma'lumotlar, dastur interfeysini yaratishda Turbo Pascal dasturi.

4. Hisoblash-tushuntirish yozuvlarining tarkibi (ishlab chiqilgan masalalar ro'yxati):

Kirish; Mavzu bo'yicha nazariy ma'lumotlar; Asosiy qism; Mavzu mazmunining qisqacha bayoni; BMI dasturiy mahsulotini yaratish tartibi va uni yaratishda qo'llaniladigan dastur tizimlari; Hayot faoliyati xavfsizligi; Xulosa; Foydalanilgan adabiyotlar ro'yxati; Ilova.

5. Chizma ishlab chiqarish ro'yxati (chizmalar nomi aniq ko'rsatiladi): *Yo'q*

6. Bitiruv ishi bo'yicha maslahatchilar:

№	Bo'lim mavzusi	Maslahatchi o'qituvchi	Imzo	
			Topshiriq Berildi	Topshiriq Bajarildi
1	Nazariy qism	Sohibov T.F.		
2	Asosiy qism	Sohibov T.F.		
3	Hayot faoliyati xavfsizligi qismi			

7. Bitiruv ishini bajarish rejasi:

№	Bitiuv ishi bosqichlari nomi	Bajarish muddati, sana	Tekshiruvdan o'tganlik belgisi
1	Mavzu bilan tanishish, adabiyotlar ustida ishlash	Sentabr-Oktabr	
2	Bitiruv malakaviy ishining I bobi ustida ishlash	Noyabr-Dekabr	
3	BMI mavzusining dasturi ustida ishlash	Yanvar-Fevral	
4	Bitiruv malakaviy ishining II bobi ustida ishlash	Aprel	
5	«Hayot faoliyati xavfsizligi» bobi ustida ishlash	May	
6	Bitiruv malakaviy ishini rasmiylashtirish	Iyun	
7	Bitiruv malakaviy ishi himoyasiga tayyorlanish	__iyun __ iyun	
8	Bitiruv malakaviy ishini himoya qilish	_____iyun	

Bitiruv malakaviy ishi rahbari: _____ Sohibov T.F.

Topshiriqni bajarishga oldim: _____ Majidov M.B

Topshiriq berilgan sana: 15.11.2012 yil

22-09 MIIT guruhi talabasi Majidov Muhammad Bahodir o'g'lining "Uinstonning 'ikkilangan kvadrat' shifri tahlili va uni dasturini yaratish" mavzuidagi bitiruv malakaviy ishiga

ANNOTATSIYA

Axborot kommunikatsiya texnologiyalari yordamida electron hujjat aylanishi kun sayin oshib bormoqda. Uni o'g'irlash ham osonlashdi. Shuning uchun hozirgi kunda electron hujjatlar xavfsizligini ta'minlashni tashkil qilish kechiktirib bo'lmaydigan muammolardan biriga aylandi. Electron hujjatlar xavfsizligini ta'minlashda kriptografik usullarni qo'llash eng ishonchli vosita hisoblanadi. Buning uchun kriptografik usul nima ekanligini anglashimiz lozim. Ushbu BMI da aynan shu haqda tafsif berilgan va ta'limiy xarakterga ega bo'lgan dastur yaratilgan.

Ushbu BMI ning tarkibi: Kirish, Nazariy qism, Asosiy qism, Hayot faoliyati xavfsizligi qismi, Ilova, Xulosa, Adabiyotlar ro`yxati.

Kirish. Axborotlarni himoyalashning dolzarbligi, ishning maqsad va vazifalari hamda uning amaliy ahamiyati haqidagi ma'lumotlar keltirilgan.

Mavzuga doir tayanch ma`lumotlar nazariy qismda kiritilgan. Bu qismda axborotlashgan jamiyatda axborot kommunikatsiya texnologiyalari tadbig'i, axborot asrida axborot xavfsizligi, axborotni himoyalashning kriptografik usullari va kriptoanalitik hujumlar haqida qisqacha tushunchalar berilgan.

Asosiy qismda an`anaviy simmetrik kriptotizimlar, bigrammali shifrlash va Uinstonning 'ikkilangan kvadrat' shifri haqida kerakli ma'lumotlar keltirilgach bevosita Uinstonning 'ikkilangan kvadrat' usulida matnni shifrlash va deshifrlash dasturini yaratish tahlillari berilgan.

Hayot faoliyati xavfsizligi qismida kasb-hunar va ilm-fanni egallash, mehnat bandligi va samaradorligi hamda mehnatga oid munosabat va rag'batlantirish bo'yicha ma'lumotlar berilgan.

Xulosa qismida axborotlarni himoyalashda kriptografiyaning o'rni va uning usullarini o'rganishda ta'limiy xarakterdagi Uinstonning 'ikkilangan kvadrat' usulida matnni shifrlash va deshifrlash dasturi haqida fikrlar keltirilgan.

Ilova qismida matnni Uinstonning ikkilangan kvadrat usulida shifrlash va deshifrlash dasturi matni, matnni Uinstonning ikkilangan kvadrat usulida shifrlash dasturi oyna ko`rinishi hamda shifrmatnni Uinstonning ikkilangan kvadrat usulida deshifrlash dasturi oyna ko`rinishi va Uinstonning 'ikkilangan kvadrat' shifrini o`rgatish metodikasi materiallari berilgan.

Adabiyotlar ro`yxatida BMI ni tayyorlashda kerak bo`lgan barcha adabiyotlar ro`yxati kiritilgan.

Buxoro muhandislik texnologiya instituti 22-09 MIIT guruhi talabasi Majidov Muhammad Bahodir o'g'lining "Uinstonning 'ikkilangan kvadrat' shifri tahlili va uni dasturini yaratish" mavzusidagi bitiruv malakaviy ishiga

TAQRIZ

Axborotlar xavfsizligini ta'minlashda kriptografik usullarning o'rni beqiyosdir. Kriptografik usullar haqida tushunchaga ega bo'lish uchun esa har qanday kriptografik usul haqidagi ma'lumot bilan tanishish zarar qilmaydi. Ushbu ta'limiy xarakterdagi "Uinstonning 'ikkilangan kvadrat' shifri tahlili va uni dasturini yaratish" mavzusidagi ish aynan shu vazifa uchun xizmat qiladi.

Bitiruv malakaviy ish kirish, nazariy qism, asosiy qism, hayot faoliyati xavfsizligi qismi, xulosa, adabiyotlar ro`yxati va ilova qismlaridan tashkil topgan.

Bitiruv malakaviy ishining asosiy qismida Uinstonning 'ikkilangan kvadrat' usulida matnni shifrlash va deshifrlash dasturini yaratish uchun kerak bo'lgan an`anaviy simmetrik kriptotizimlar, bigrammali shifrlash haqida kerakli ma'lumotlar keltirilgach bevosita dasturini yaratish haqidagi ma`lumotlar to`liq tushunarli qilib yoritilgan.

Bitiruv malakaviy ishning dolzarbligini, davlat standartlari nizomi talablarga to`liq javob berishni hisobga olib, talaba Majidov Muhammadga «Muallim informatika va axborotlar texnologiyasi» mutaxassisligi bakalavri ilmiy darajasi berishga va ishni yaxshi (78 foiz) bahoga loyiq deb hisoblayman.

Rahbar: Sohibov T.F.

MUNDARIJA

KIRISH

I. AXBOROTLASHGAN JAMIYATDA AXBOROT HIMOYASI

1.1. Axborotlashgan jamiyatda axborot kommunikatsiya texnologiyalari tadbig'i

1.2. Axborot asrida axborot xavfsizligi

1.3. Axborotni himoyalashning kriptografik usullari

1.4. Kriptoanalitik hujumlar

II. UINSTONNING 'IKKILANGAN KVADRAT' SHIFRI DASTURI

2.1. An`anaviy simmetrik kriptotizimlar

2.2. Bigrammali shifrlash

2.3. Uinstonning 'ikkilangan kvadrat' shifri

2.4. Uinstonning 'ikkilangan kvadrat' usulida matnni shifrlash va deshifrlash

2.5. Uinstonning 'ikkilangan kvadrat' shifrini o`rgatish metodikasi

III. HAYOT FAOLIYATI XAVFSIZLIGIDA MEHNAT TARBIYASI

3.1. Kasb-hunar va ilm-fanni egallash

3.2. Mehnat bandligi va samaradorligi

3.3. Mehnatga oid munosabat va rag'batlantirish

XULOSA

FOYDALANILGAN ADABIYOTLAR

ILOVA

KIRISH

XX asr oxirida ‘axboriy jamiyat’ va ‘axborotlashuv’ atamalari nafaqat mazkur soha vakillari, balki siyosatchilar, iqtisodchilar, olimlar va pedagoglar lug’at boyligidan ham mustahkam o`rin egalladi. Ko`p hollarda bu tushuncha fuqarolik jamiyati platformasida yangi evolyutsion odimni amalga oshirib XXI asrga axborotlashgan jamiyat sifatida munosib kirib borish imkonini beradigan axborot – kommunikatsiya texnologiyalari, telekommunikatsiya vositalarining rivojlanishi bilan uyg’un holda ta`riflanadi. Dunyo yangi davr-axborot asriga, elektron iqtisodiy faoliyat, tarmoq jamoatlari va chegarasiz tashkilotlar asriga qadam qo`ydi. Yangi davrning boshlanishi jamiyat hayotining iqtisodiy va ijtimoiy tomonlarini tubdan o`zgartirishi tabiiy. Bunday o`zgarishlar informatsion dunyodagi inson roliga bevosita ta`sir ko`rsatadi. Boisi inson jamiyatning axboriy-texnik xususiyatlari yo`nalishiga mos ravishda o`zgarib boradi.

Mavzuning dolzarbligi. To`g’ri va xolis axborotga ega bo`lish, u asosida hatti-harakatlar strategiyasini belgilash hamda axboriy jamiyatni qurishga intilish bugungi kunning dolzarb masalalariga aylanish sababi ham shundadir. Bu esa o`z navbatida, dunyo miqyosida axborot, uning muhofazasi bilan bog’liq muammolarning yanada kuchayishiga va ular xavfsizligini ta`minlashning yanada dolzarblasha borishi hech kimga sir emas. Shuning uchun, ushbu axborotlarni himoyalash usullaridan biri bo`lgan ‘Uinstonning ‘ikkilangan kvadrat’ shifri tahlili va uni dasturini yaratish’ mavzusidagi bitiruv malakaviy ishining dolzarb va muhim ekanligi ravshan bo`ladi.

Ishning maqsadi. Ushbu bitiruv malakaviy ishi mavzusi orqali axborotlar xavfsizligi muammolari, axborotlashgan jamiyatda axborotlarni himoya qilish qanchalik muhim va ahamiyatga ekanligini yoritish hamda kriptografiyaning axborotlarni himoyalashning usullaridan biri ‘Uinstonning ‘ikkilangan kvadrat’ shifri tahlili va uni 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 axborot xavfsizligini ta`minlash muhimligi va uning asosiy tushunchalarini tavsiflagach, axborotlarni Uinstonning ‘ikkilangan kvadrat’ shifrlash va deshifrlash tizimi hamda u orqali matnlarni himoyalashga doir

tahlillarimizni hamda dasturiy ta`minotni yaratishga doir tadqiqotlarimizni bayon qilamiz.

Ishning amaliy ahamiyati. O`zbekiston Respublikasining milliy kriptografik algoritmlarini yaratish, ularni takomillashtirish va axborotni kriptografik muhofazalashning milliy dasturiy va apparat-dasturiy vositalarini ishlab chiqish O`zbekiston Respublikasi Prezidentining 2007 yil 3 apreldagi ‘O`zbekiston Respublikasida axborotning kriptografik muhofazasini tashkil etishga oid chora-tadbirlar to`g’risidagi’ 614-sonli qarorida birinchi galdagi vazifa qilib qo`yilganligini hisobga olsak, mazkur bitiruv malakaviy ishi bo`yicha keltirilgan tahliliy matn, algoritm va dastur bu qarorning bajarilishini ta`minlashga xizmat qiladi.

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

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

I. Axborotlashgan jamiyatda axborot himoyasi

1.1. Axborotlashgan jamiyatda axborot kommunikatsiya texnologiyalari tadbig'i

Axborot kommunikatsiya texnologiyalari sohasini jadal sur`atlar bilan taraqqiy ettirish O`zbekiston iqtisodiyotida amalga oshirilayotgan tarkibiy o`zgarishlar hamda iqtisodiy islohotlarning bosh yo`nalishlaridan biri hisoblanadi. Va u respublikani axborotlashgan jamiyatga aylantirish uchun xizmat qiladi. Bu esa mamlakatimiz iqtisodiyotini jadal sur`atlar bilan rivojlanishida o`ziga xos etakchi tarmoq – 'lokomotiv' rolini o`taydi.

Mustaqilligimizning ilk yillaridyoq, muhtaram Prezidentimiz Islom Karimov: 'Biz yaqin yillar davomida aloqa va telekommunikatsiya rivoji bo`yicha jahon standartlari darajasiga ko`tarilishimiz lozim. Rivojlangan kommunikatsiya tizimi bo`lmasa, O`zbekistonning kelajagi bo`lmaydi. Biz buni aniq his qilishimiz lozim', - deya ta`kidlagan edilar.

Ushbu dasturiy vazifalardan kelib chiqib, mamlakatimizda kompyuter va axborot texnologiyalari, telekommunikatsiya va ma`lumot uzatish tarmoqlarini, internet xizmatlarini rivojlantirish va zamonaviylashtirish, ularni dunyo standartlari darajasiga etkazish maqsadida keng ko`lamli islohotlar bosqichma – bosqich amalga oshirilmoqda.

Albatta, ijtimoiy hayotning barcha tarmoqlarida bo`lgani kabi axborot kommunikatsiya texnologiyalari sohasidagi islohotlarni muvofaqqiyatli amalga oshirish, uning huquqiy asoslarini shakllantirish, muntazam takomillashtirib borish zarur.

Sohaga oid normativ – huquqiy hujjatlarning qabul qilinishi va takomillashtirilishi kompleks ravishda, izchillik bilan, ilmiy asoslangan holda mavjud qonun hujjatlari, chet el qonunchiligi tajribasi, shuningdek, axborot kommunikatsiya texnologiyalarining rivojlanish istiqbollari hisobga olinib amalga oshirilmoqda.

O`tgan davr mobaynida shu maqsadlarda 11 ta Qonun, O`zbekiston Respublikasi Prezidentining 3 ta Farmoni, O`zbekiston Respublikasi Prezidenti hamda Vazirlar Mahkamasining 40 dan ziyod qarorlari va 300 dan ortiq idoraviy qonun osti hujjatlari qabul qilindi.

Ayniqsa, 2003 – 2004 yillarda ‘Elektron raqamli imzo to`g’risida’gi, ‘Elektron hujjat aylanishi to`g’risida’gi va ‘Elektron tijorat to`g’risida’gi O`zbekiston Respublikasi Qonunlarining qabul qilinishi jamiyatni axborotlashtirish, zamonaviy axborot kommunikatsiya texnologiyalaridan unumli foydalanish imkoniyatlarini yaratdi. Mazkur qonun hujjatlarini ishlab chiqishda ushbu sohadagi xalqaro huquqiy me`yorlar hamda bir qator rivojlangan davlatlarning tajribalari ham atroflicha o`rganilib, milliy qonunchiligimizga maqbul jihatlari uyg’unlashtirildi. [27]

Mamlakatimizda axborot kommunikatsiya texnologiyalarining jadal sur`atlarda rivojlanishi elektron hujjat aylanishi, elektron raqamli imzo, elektron to`lovlar kabi yana bir qancha yangi xizmat turlarining shakllanishiga, jumladan, tadbirkorlarimizga masofadan turib dunyoning xohlagan mamlakatidan o`ziga hamkor topish va tijorat ishlarini yuritishiga keng yo`l ochdi.

Xorijiy mamlakatlar tajribasidan ma`lumki, elektron tijoratning shiddat bilan rivojlanishiga internetdan foydalanuvchilar soni aholining 20-25 foizini tashkil etgandagina erishish mumkin. Bugungi kunda mamlakatimizda internetdan foydalanuvchilar soni 10 million nafardan ortgani elektron tijoratning kelgusidagi yorqin istiqbolidan darak berib turibdi.

O`zbekistonda elektron hujjatlarga huquqiy mavqe beruvchi ‘Elektron hujjat aylanishi to`g’risida’gi Qonunning qabul qilinishi, shubhasiz, elektron hujjat aylanishi tizimini rivojlantirishga ko`maklashib, davlat hokimiyatining turli idoralari o`rtasidagi hujjat aylanishini avtomatlashtirishga qulay imkoniyat yaratmoqda.

‘Elektron raqamli imzo to`g’risida’gi O`zbekiston Respublikasi Qonuni elektron hujjatda-gi elektron raqamli imzo va qogozdagi imzo teng kuchga ega ekanligini ta`minlab berdi. Natijada yuridik va jismoniy shaxslar tomonidan internet tarmog’idan foydalangan holda kerak bo`lgan barcha hisobot formalari va boshqa ma`lumotlarni elektron ravishda interektiv holda olish hamda soliq va statistika hisobotlarini topshirish imkoniyatini yaratdi. Bu tizim kichik biznes va tadbirkorlik sub`ektlarining vaqtini tejash, davlat xizmatchilari bilan bevosita muloqot uchun navbat kutish yoki soliq hisobotlarini to`ldirishdagi xato va kamchiliklarni tuzatishga emas, balki o`z tadbirkorlik ishlarini rivojlantirishga sarf etishlariga imkon bermoqda. [27]

Shuningdek, mazkur Qonunning qabul qilinishi va ijrosinig ta`minlanishi natijasida respublikamizda 9 ta elektron raqamli imzo kalitlarini ro`yxatga olish markazlari tashkil etildi. Agar elektron raqamli imzo kalitlari soni 2006 yilda 93 tani tashkil etgan bo`lsa, hozirgi kunga kelib 300 mingtadan oshib ketdi. [27]

Shu bilan bir qatorda, mijozlarga yangi xizmat turlarini ko`rsatishning huquqiy asoslari kafolatlab qo`yildi. Bu bilan iqtisodiyotimizga ‘Pay Net’, ‘Fast Pay’, ‘Moblis’, ‘E-karmon’ kabi elektron to`lovlar xizmatini ko`rsatuvchi muassasalar kirib keldi. ‘SMS - banking’, ‘Internet - banking’ kabi yangi elektron to`lov xizmatlari joriy etildi. endilikda ushbu xizmatlar sharofati bilan mijozlar kommunal xizmatlar, mobil’ aloqa va internet xizmatlarini hisob – kitob qilib, o`y – ro`zgor mollarini internet orqali sotib olishmoqda.

2005 yildan boshlab O`zbekiston davlat organlarining internetdagi rasmiy veb – saytlarining ochilishi tadbiq etildi. O`zbekiston Respublikasi Vazirlar Mahkamasining ‘Axborotlashtirish sohasida normativ – huquqiy bazani takomillashtirish to`g’risida’gi 256 – sonli qarori bilan ushbu saytlarga asosiy talablar belgilangan bo`lib, unda saytlarni to`laqonli rasmiylashtirish, undan foydalanish va yangilash maqsadida veb – saytda joylashtiriladigan zaruriy axborotlar ro`yxati, mazmuni va boshqa kerakli shartlarga nisbatan xalqaro standartlar aniq shakllantirildi. [27]

Davlat va xo`jalik boshqaruvi, mahalliy davlat hokimiyati organlarining axborot kommunikatsiya texnologiyalaridan foydalanish vositasida jismoniy va yuridik shaxslar bilan o`zaro tezkor hamkorligini ta`minlash, shuningdek, davlat va xo`jalik boshqaruvi, mahalliy davlat hokimiyati organlari tomonidan ko`rsatiladigan xizmatlardan keng foydalanishini ta`minlash maqsadida Vazirlar Mahkamasi tomonidan 2007 yil 23 avgustida ‘Davlat va xo`jalik boshqaruvi, mahalliy davlat hokimiyati organlarining axborot kommunikatsiya texnologiyalaridan foydalangan holda jismoniy va yuridik shaxslar bilan o`zaro hamkorligini yanada takomillashtirish chora – tadbirlari to`g’risida’gi qarori qabul qilinib, u bilan axborot kommunikatsiya texnologiyalaridan foydalangan holda interaktiv davlat xizmatlari ko`rsatish to`g’risidagi nizomi tasdiqlandi.

Davlat va xo`jalik boshqaruvi, mahalliy davlat hokimiyati organlari faoliyati samaradorligini oshirish, davlat va jamiyat qurilishi sohasida zamonaviy axborot

kommunikatsiya texnologiyalaridan keng foydalanishni ta`minlash maqsadida O`zbekiston Respublikasi Prezidenti tomonidan 2012 yil 21 martda ‘Zamonaviy axborot kommunikatsiya texnologiyalarini yanada joriy qilish va rivojlantirish to`g’risida’gi qaror qabul qilindi. Unda davlat organlari, shuningdek yuridik va jismoniy shaxslarning axborot tizimlarini bosqichma – bosqich integratsiya qilish asosida Milliy axborot tizimi shakllanishini ta`minlash, interaktiv davlat xizmatlari sifatini yaxshilash va ularning ro`yxatini kengaytirish, milliy axborot tizimida axborot xavfsizligini ta`minlash va boshqa qator vazifalarni ko`zlab, axborot kommunikatsiya texnologiyalarini yanada joriy qilish va rivojlantirishning asosiy vazifalari belgilab berildi. [27]

Muhtaram YUrtboshimiz Oliy Majlis palatalarining 2010 yil 12 noyabr kuni bo`lib o`tgan qo`shma majlisida taqdim etgan Kontseptsiyada axborot sohasini isloh qilish, axborot va so`z erkinligini ta`minlash borasidagi qonunchilik tashabbuslari ushbu sohada bosqichma – bosqich amalga oshirilayotgan tadrijiy islohotlarning uzviy davomi bo`lib, axborot olishnig erkin va teng huquqligini ta`minlash, davlat hokimiyati va boshqaruvi organlari faoliyatinining ochiqligi printsiplarini amalga oshirish, sohada bozor mexanizmlarini yanada takomillashtirish va axborot kommunikatsiya texnologiyalarini keng joriy etish, fuqarolik institutlari tizimida ommaviy axborot vositalarining rolini yanada kuchaytirishga qaratilgan samarali huquqiy mexanizmlarini yaratishni nazarda tutadi.

Kontseptsiyada ommaviy axborot vositalarining davlat hokimiyati va boshqaruvi organlari faoliyati ustidan jamoatchilik nazoratini ta`minlash, davlat organlari va jamoatchilik o`rtasida mustahkam aloqa o`rnatish borasidagi rolini kuchaytirish maqsadida ‘Davlat hokimiyati va boshqaruvi organlari faoliyatining ochiqligi to`g’risida’gi O`zbekiston Respublikasi Qonunini qabul qilish taklif etildi. Bu qonunnning hayotga joriy etilishi davlat hokimiyati organlari faoliyati haqida jamoatchilikni xabardor qilib borishning huquqiy mexanizmlarini yaratib, davlat organlarining axborot xizmatlari va media – tuzilmalari ishini faollashtirish, ular tomonidan ma`lum bir muddatlarda brifing va matbuot anjumanlarini tashkil etib borish, yurtimizda amalga oshirilayotgan islohotlarning ochiqligi va oshkoraligini ta`minlash, ommaviy axborot vositalarinin axborot olish yuzasidan murojaatlarini ko`rib chiqish muddatlarini qisqartirish, axborot olish sohasidagi qonunchilik

talablarini buzganlik uchun yuridik mansabdor shaxslarning ma`muriy javobgarligini kuchaytirishga xizmat qiladi.

Shuningdek, qonun loyihasida davlat hokimiyati va boshqaruvi organlari faoliyatining oshkoraligi va shaffofligini ta`minlash bo`yicha axborot kommunikatsiya texnologiyalarining o`rni va roli alohida belgilab qo`yilmoqda. Zero, bugungi tezkor va shiddatkor zamonda zamonaviy axborot kommunikatsiya texnologiyalarining cheksiz imkoniyatlaridan samarali foydalanishni davrning o`zi taqoza etmoqda. [27]

Zamonaviy axborot kommunikatsiya texnologiyalarini yanada kengroq joriy etishga xorijiy investitsiyalarni jalb etishning huquqiy asoslarini mustahkamlash, ilg'or texnologiyalarga asoslangan qurilma va vositalar ishlab chiqarish ko`lamini oshirish, yangi axborot kommunikatsiya texnologiyalari va xizmatlarini joriy etish maqsadida iste`molchilarning huquqlarini inobatga olgan holda tegishli qonunlar va qonun hujjatlariga o`zgartish va qo`shimchalar kiritish, yangi qonunlarni ishlab chiqib, qabul qilishni ham davrning o`zi taqoza etmoqda.

Muhtaram Prezidentimiz 2012 yilda mamlakatni ijtimoiy – iqtisodiy rivojlantirish yakunlari hamda 2013 yilga muljallangan iqtisodiy dasturning eng muhim ustivor yo`nalishlariga bag'ishlangan Vazirlar Mahkamasining majlisidagi ma`ruzasida axborot kommunikatsiya va telekommunikatsiyalar texnologiyalari sohasidagi chora – tadbirlar va loyihalarni jadal amalga oshirish tobora muhim ahamiyat kasb etayotganini ta`kidlab, shunday dedilar: 'Biz o`zimizga shuni aniq tasavvur etishimiz kerakki, iqtisodiyotning barcha sohalariga, kundalik hayotimizga zamonaviy axborot kommunikatsiya tizimlarini keng joriy etish bo`yicha tub va ijobiy ma`nodagi portlash effektini beradigan o`zgarishlarni amalga oshirmasdan turib, istiqboldagi maqsadlarimizga erishish qiyin bo`ladi'. [27]

Darhaqiqat, bugungi kunda oldimizda ma`suliyatli vazifalar turibdi. Ya`ni, qisqa vaqt mobaynida nafaqat axborot xizmatlari ko`rsatishning ko`plab turlari bo`yicha mavjud kamchiliklarni bartaraf etishimiz, balki zamonaviy axborot kommunikatsiya texnologiyalarini joriy etish borasida yuksak darajaga erishgan ilg'or mamlakatlar safiga qo`shilishimiz zarur. Bu borada 'Elektron hukumat' tizimini, shu jumladan boshqaruv jarayonlarini, shuningdek, biznes sohasiga va fuqarolarga davlat xizmatlari ko`rsatish tizimini shakllantirish kontseptsiyasi va kompleks dasturlarni

ishlab chiqishni jadallashtirishga, axborot tizimlarining idoralararo va idoraviy komplekslarni integratsiya qiladigan milliy tizimni yaratishga alohida e`tibor qaratish lozimligi Yurtboshimiznig ma`ruzasida ustivor yo`nalish sifatida belgilab berildi.

Albatta, yaqin istiqboldagi ushbu maqsad – muddaolarni amalga oshirish uchun, birinchi navbatda, mazkur sohani tartibga soluvchi qonunchilikni yanada mustahkamlash, samarali huquqiy mexanizmlarni takomillashtirish hamda joylarda sohaga oid qonun hujjatlari ijrosini ta`minlash borasida faoliyat olib borish ustivor vazifalardan sanaladi. Pirovard, bu sa`y – harakatlar istemolchilarning barcha qatlamlari hamda jadallik bilan rivojlanib borayotgan zamonaviy axborot kommunikatsiya texnologiyalari talablariga mos tushadigan, tubdan yangilangan zamonaviy axborot kommunikatsiya tarmoqlari vujudga kelishiga zamin yaratib, mamlakatimizda axborotlashtirish jarayonlari yanada jadallashadi hamda O`zbekiston jahon axborot makonida o`ziga xos va munosib o`ringa ega bo`ladi. Mamlakatimizda barcha sohalarda bo`lgani kabi zamonaviy axborot kommunikatsiya texnologiyalarini rivojlantirish jarayoni izchil davom ettirilmoqda. eng avvalo O`zbekistonda mazkur sohani tartibga soluvchi qonunchilik bazasi yaratilayotganini alohida ta`kidlash joiz. [27]

1.2. Axborot asrida axborot xavfsizligi

Axborot asrida dunyoni harakatlantiruvchi asosiy kuch axborot ekani hech kimga sir emas. Agar qorayib 9 asr davom etgan agrar davrda er, 300 yilga yaqin davom etgan sanoat (industrial) zamonida asosiy boylik texnika sanalgan bo`lsa, XX asrning ikkinchi yarmida paydo bo`lgan turli axborotlar oqimi global tizimda hal qiluvchi ahamiyat kasb etadigan bo`ldi. XX asr oxiriga kelib insoniyat tarixida ilk bor sanoat rivojlangan mamlakatlar ijtimoiy ishlab chiqarishda axborotlar mehnatining asosiy predmeti bo`lib qoldi. Hozirgi mehnat resurslarini moddiy ishlab chiqarish sohasidan axborot sohasiga bevosita jalb etish tendentsiyasi yuzaga kelgan-ki, bu endilikda axborot inqolobi nomini olgan eng sezilarli belgiga aylangan. XX asr oxirida ‘axboriy jamiyat’ va ‘axborotlashuv’ atamalari nafaqat mazkur soha vakillari, balki siyosatchilar, iqtisodchilar, olimlar va pedagoglar lug’at boyligidan ham mustahkam o`rin egalladi. Ko`p hollarda bu tushuncha fuqarolik jamiyati platformasida yangi evolyutsion odimni amalga oshirib XXI asr axboriy jamiyat - axborot asri nomini oldi. Natijada ishlab chiqarish tizimi, odamlar dunyoqarashi, ularning hayot tarzida

jiddiy o`zgarishlar ro`y bermoqda. Axborot texnologiyalarning tubdan o`zgarishi millionlab odamlarning kundalik hayotini o`zgartirmoqda. Axborot eng muhim strategik, boshqaruv resurslaridan biriga aylandi. Uni ‘ishlab chiqarish’ va qabul qilish ijtimoiy hayot rivojida muhim asosni tashkil etadigan bo`ldi. Bu esa sayoramizning har qanday nuqtasidagi axborot manbalari istalgan odam uchun ochiq bo`lishi bilan birga ular tomonidan yaratilajak axborot ham butun insoniyat mulkiga aylanishi mumkinligidan dalolat beradi. Bugungi kun sharoitida axborot olish huquqi va uning oshkoraligi jamiyatning barcha a`zolari uchun hayotiy muhim ahamiyat kasb etishi bor haqiqat. [10]

Dunyo yangi davr-axborot asriga, elektron iqtisodiy faoliyat, tarmoq jamoatlari va chegarasiz tashkilotlar asriga qadam qo`ydi. Yangi davrning boshlanishi jamiyat hayotining iqtisodiy va ijtimoiy tomonlarini tubdan o`zgartirishi tabiiy. Bunday o`zgarishlar informatsion dunyodagi inson roliga bevosita ta`sir ko`rsatadi. Boisi inson jamiyatning axboriy-texnik xususiyatlari yo`nalishiga mos ravishda o`zgarib boradi.

Hozir dunyo bo`ylab aylanayotgan axborot mikdorining oshib, borayotgani hisobiga uning foydali va zararli tomonlari ham ko`rinib qolmoqda. [1] Tabiiyki, bunday sharoitda axborot xavfsizligi masalasi dolzarb ahamiyatga ega. Shu bois, mutaxassislar tomonidan ommaviy axborot bilan ishlash mexanizmini yaratish zarurligi, uning mazmuni va shakllarini, uslubiy va amaliy tomonlarini ko`rib chiqish lozimligi ilgari surilmoqda. Chunki, axborotning muhimlik darajasi qadim zamonlardan ma`lum. Shuning uchun ham qadimda axborotni himoyalash uchun turli xil usullar qo`llanilgan. Agar ma`lumot ishonchli himoyalansa va bu himoya tusigini engib o`tish qiyin bo`lsa u bardoshli deyish qabul qilingan. Himoya usullaridan biri - sirli yozuvdir. Undagi xabarni xabar yuborilgan manzil egasidan boshqa shaxs o`qiy olmagan. Asrlar davomida bu san`at - sirli yozuv jamiyatning yuqori tabaqalari, davlatning elchixona rezidentlari va razvedka missiyalaridan tashqariga chiqmagan. Hozirgi kunga kelib hamma narsa tubdan o`zgardi, ya`ni axborot o`z qiymatiga ega bo`ldi va keng tarqaladigan mahsulotga aylandi. Uni endilikda ishlab chiqaradilar, saqlaydilar, uzatadilar, sotadilar va sotib oladilar. Bulardan tashqari uni o`g’irlaydilar, buzib talqin etadilar va soxtalashtiradilar. Shuning uchun axborotni himoyalash

ehtiyoji yanada kuchaydi. Axborotni qayta ishlash sanoatining paydo bo`lishi axborotni himoyalash sanoatining paydo bo`lishiga olib keldi. [10]

Maxfiy va qimmatbaho axborotlarga ruxsatsiz kirishdan himoyalash eng muhim vazifalardan biri sanaladi. Kompyuter egalari va foydalanuvchilarning mulkiy himoyalash - bu ishlab chiqarilayotgan axborotlarni jiddiy iqtisodiy va boshqa moddiy hamda nomoddiy zararlar keltirishi mumkin bo`lgan turli kirishlar va o`g'irlashlardan himoyalashdir. Himoyalashning bir necha usullari mavjud va ulardan o`z o`rnida foydalanish yaxshi natijalarni beradi.

'Axborot xavfsizligi' tushunchasi yalpi xarakterga ega bo`lib, u shaxs, jamiyat va davlatning axborot sohasidagi manfaatlariga rioya etish, uning predmeti haqida aniq ma`lumotga ega bo`lish, ob`ektlarini bilish va sub`ektlari harakatlariga to`g'ri baho bera olish, axborot muhofazasini etarli darajada ta`minlash, unga nisbatan noqonuniy harakatlarning oldini olish, ma`lumotlarni izlash, to`plash, saqlash, ularga ishlov berish va ulardan foydalanish qoidalariga amal qilish va boshqalarni o`z ichiga oladi. [10]

Axborot xavfsizligining etakchi yo`nalishlari to`rtta: texnikaviy, siyosiy, huquqiy va ma`naviy. Albatta, har bir tasnif nisbiy xarakterga ega. Chunki ularni bir-biridan keskin ajratib bo`lmaydi, bu yaxlit muammo. Shu urinda ularga qisqacha tavsif berib o`tish maqsadga muvofiq.

Texnikaviy yo`nalish doirasiga axborot xavfsizligiga qarashli elektron qurilmalar, dasturlar hamda ularni ishlab chiquvchilar, ulardan foydalanuvchilar kiradi. Mazkur qurilmalar va dasturlar ko`proq ushbu sohadagi ilmiy tadqiqot, loyiha - konstruktorlik tashkilotlari tomonidan ishlab chiqiladi. Ular elektron, optik, radio, mexanik, elektromexanik va boshqa ko`rinishlardan iborat bo`ladi. Soha mutaxassislari ma`lumotlarni masofaga uzatish zarurligi yuzasidan ularni muhofaza qiluvchi maxsus dasturlarni ishlab chiqadi. Bu erda kriptografik usullardan keng foydalaniladi. Bunday usullarni ishlatish-ma`lumotlarni shifrlash va natijada axborot shaklini o`zgartirishdan iborat. Yaxshi, sifatli shifr axborotni begona odamlarning o`qishiga imkoniyat bermaydi. [10]

Siyosiy yo`nalish ham keng qamrovli bo`lib, tarkibiga tashkiliy ma`muriy, iqtisodiy va boshqa sohalarni oladi. Uni qisqacha qilib, axborot xavfsizligi sohasida amalga oshiriladigan siyosat, deyish mumkin. Siyosiy yo`nalish tashkiliy masalalar

bilan bog’liq bo`lib, unda davlat, jamiyat, xalq xo`jaligi tarmoqlari, kontsernlar, assotsatsiyalar, jamoat tashkilotlari, o`quv yurtlari, tadqiqot institutlari o`z sirlarini saqlashni ta`minlaydilar. Buning uchun birinchi o`rinda axborot tizimlarini yaratish, rivojlantirish va takomillashtirish, axborotni muhofaza qilishda tegishli huquqiy, ma`muriy va boshqa hujjatlar hamda tizimlarni yaratish kerak. [10]

Huquqiy yo`nalish - axborot xavfsizligining eng murakkab tizimlaridan biridir. Kiberhududni himoyalash harakatlari XX asrning o`rtalarida AQSHda boshlangan. Bugungi kunda AQSHda axborot xavfsizligi bilan bog’liq 20 dan ortiq davlat miqyosidagi hujjatlar qabul qilingan. Natijada mamlakat axborot kommunikatsiya texnologiyalari sohasida dunyoda eng rivojlangan huquqiy tizimga ega bo`ldi. [26]

Yurtimizda ham axborot texnologiyalarini rivojlantirish va ma`lumotlarni himoyalashga doir bir qator hujjatlar qabul qilingan. Bular ‘Axborot erkinligi printsiplari va kafolatlari to`g’risida’gi Qonun, Prezidentimizning ‘Axborot - kommunikatsiya texnologiyalarini yanada rivojlanirishga oid qo`shimcha chora - tadbirlar to`g’risida’gi, ‘O`zbekiston Respublikasi jamoat ta`lim axborot tarmogini tashkil etish to`g’risida’gi hamda Vazirlar Mahkamasining ‘Matbuot, axborot tizimlar va telekommunikatsiyalar sohasida boshqaruv tuzilmasini takomillashtirish to`g’risida’gi, ‘Davlat va xo`jalik boshqaruvi organlarining jamoatchilik bilan aloqalarini rivojlantirish chora - tadbirlari to`g’risida’gi qarorlaridir.

Virtual ommaviy axborot sohasiga doir qonunchilikni rivojlantirish ustida AQSH, Germaniya, Rossiya, Xitoyda jiddiy izlanishlar olib borilayotgan bo`lsa-da, natijalar hozircha qoniqarli emas. Buning ikkita asosiy sababi bor. Birinchidan, gap muammoning o`zi murakkab ekanida. Huquqiy normalarni ishlab chiqish aniq ob`ekt va sub`ekt, predmet va tarkibni talab etadi. Virtual kengliklarda esa bu tushunchalar o`ta mavhum. Chunki amaliyot va huquq, qolaversa, mutaxassislar ham bu masalada bir to`xtamga kelisha olmayapti. Ikkinchidan, erkin axborot oqimi masalasida G’arb va SHarq mamlakatlarining qarashlarida jiddiy ziddiyatlar bor. Bu har bir mamlakatning milliy qonunchiligiga o`z ta`sirini o`tkazmasdan qolmaydi. Oxirgi yillarda huquqiy informatika, huquqiy kibernetika, kabi tushunchalarning hayotimizga kelayotgani fikrimiz tasdig’idir.

Ma`naviy yo`nalish axborot xavfsizligi tizimining eng murakkab yo`nalishidir. Chunki ikki ming yil ichida fan - texnika misli ko`rilmagan darajada rivojlangan

bo`lsa-da, inson jismi, tabiati avvalgidek turibdi. Mazkur muammo Prezident Islom Karimovning ‘Yuksak ma`naviyat-engilmas kuch’ asarida atroflicha tushuntirib berilgan: ‘…Aksariyat hollarda ko`pchilik ma`naviyat o`zi nima, degan savolga aniq va lo`nda javob berishga qiynaladi. Men bunday holatga o`z shaxsiy tajribamda ko`p bor guvoh bo`lganman…Shu fikrni davom ettirib, ma`naviyat-insonni ruhan poklanish, qalban ulg’ayishga chorlaydigan, odamning ichki dunyosi, irodasini baquvvat, iymon-e`tiqodini butun qiladigan, vijdonini o`yg’otadigan beqiyos kuch, uning barcha qarashlarining mezonidir, desak, menimcha, tariximiz va bugungi hayotimizda har tomonlama o`z tasdig’ini topib borayotgan haqiqatni yaqqol ifoda etgan bo`lamiz’, deyiladi mazkur asarda.

Ma`naviyat bilan bog’liq axborot xavfsizligi tushunchasi ko`p bug’inli, ildizi esa ancha chuqur. Ijtimoiy tasavvurlardan iborat bo`lgan arxetiplarning o`zini tushunish qanchalik murakkab. Shuning uchun kosmopolitizm va ‘ommaviy madaniyat’ deb nomlanayotgan illatlar rivojlanib ketayotgan bugungi axborot asrida milliy madaniyatni saqlab qolish, tan olish kerakki oson kechmaydi. [1]

Globallashuv jarayonida AQSH va G’arbiy Evropa mamlakatlaridagi ayrim qora kuchlar tomonidan ishlab chiqilayotgan ‘ommaviy axborot’ oqimlari kurrai zamin bo`ylab tarqalayotgan ekan, tabiiyki, ushbu jarayon butun dunyo aholisiga o`zining salbiy ta`sirini o`tkazishi kunday ravshan bo`lib qoldi.

Ma`naviy ta`sirga qarshi turish nega qiyin? Nega boshqa sohalarni eplab bo`ladi-yu (texnikaviy, siyosiy yoki huquqiy sohalardagi axborot xavfsizligini), ammo ma`naviyat sohasida xorijiy axborotga qarshilik ko`rsatish ancha murakkab? Chunki mamlakatimizda joriy qilingan tarbiya tizimi ma`naviy o`lchovlarga, umuminsoniy va milliy mezonlar garmoniyasiga asoslangan. ‘ommaviy madaniyat’ esa ko`proq odamning tabiatidagi biologik instinktlarga ‘murojaat’ etadi.

Xulosa o`rnida ta`kidlash o`rinliki, odamlarni ‘uni ko`rma, buni eshitma’ deyish bilan tarbiyalab bo`lmaydi. Aksincha, aholi bilan ommaviy axborot vositalari orqali muloqot qilinayotganda salbiy ma`lumotlarga ijobiy materiallar berish yo`li bilan qarshi kurashish mumkin. Shu bois, XXI asrning ibtidosida biz uchun yot g’oya va ma`naviy ta`sirlarga qarshi birgalikda harakat qilinsa, maqsadga muvofiq bo`ladi.

1.3. Axborotni himoyalashning kriptografik usullari

Axborotlarni kriptografik usullar orqali himoyalash, himoyalashning texnikaviy yo`nalishi doirasiga kiradi.

Kriptografiya - axborotlarni aslidan o`zgartirilgan holatga o`tkazishlarning matematik uslublarini topish va takomillashtirish bilan shug'ullanadi.

Kriptografiya axborotlarni dinamik o`zgartirish usullari orqali uni dushman uchun tushunarsiz holatga keltirish bilan shugullanadi. Bunday dinamik o`zgartirishlar axborotlarni himoyalashning ikkita asosiy, konfedentsiallik (dushmanni aloqa kanalidan axborotni olishi) va yaxlitlik (dushman xabar ma`nosini o`zgartirishi yoki yolg'on xabarni aloqa kanalidan uzata olmasligi) muammosini echadi. Konfedentsiallik va yaxlitlik muammolari o`zaro chambarchars bog'liq bo`lib, ularning birining echimi ikkinchisi echimi sifatida ham qo`llaniladi. [2]

Kriptografik tizimlar yo`nalishidagi izlanishlar qadim zamonlardan buyon olib borilgan. Ayniqsa, birinchi va ikkinchi jahon urushi yillari davrida u muhim ahamiyat kasb etdi va jadal rivojlandi. Urushdan keyingi yillarda hisoblash texnikalarining yaratilishi va takomillashib, insoniyat faoliyatining barcha sohalariga chuqur va keng ma`noda kirib borishi, kriptografik uslublarni tabiiy ravishda rivojlanib va takomillashib borishini taqozo etdi.

Kriptografik uslublarning axborotlar tizimi muhofazasi masalalarida qo`llanishi, ayniqsa, hozirgi kunda muhimdir. Haqiqatan ham, bir tomondan kompyuter tizimlarining internet tarmoqlari bilan bog'liq ravishda katta hajmdagi davlat va harbiy ahamiyatga ega bo`lgan axborotlarni hamda shu kabi iqtisodiy, shaxsiy va boshqa turdagi axborotlarni tez va sifatli uzatish va qabul qilishdagi roli ortib bormoqda. Ikkinchi tomondan esa bunday axborotlarning keng ma`nodagi muhofazasini ta`minlash masalalari muhimlashib bormoqda. [6]

Hozirgi zamon kriptografiyasi quyidagi to`rtta bo`limni o`z ichiga oladi:

- Simmetrik kriptotizimlar.
- Ochiq uslubga (kalitga) yoki yana boshqacha aytganda ochiq algoritmga asoslangan kriptotizimlar.
- Elektron imzo tizimlari.
- Kriptotizimlarda kalitlardan foydalanish uslublarini boshqarish.

Kriptografik uslublardan foydalanishning asosiy yo`nalishlari:

- maxfiy ma`lumotlarni aloqa kanali (masalan, elektron pochta) bo`yicha uzatish;
- uzatilgan ma`lumotlarning haqiqiyligini ta`minlash;
- axborotlarni (hujjatlarni, ma`lumotlar jamg'armasini) kompyuterlar tizimi xotiralarida shifrlangan holda saqlash va shular kabi masalalarni o`z ichiga oladi.

Kriptografik uslublar axborotlar matnini asli holidan o`zgartirib, faqat kalitni bilgan holdagina uni asli holatini olish imkoniyatini beradi.

Axborotlar matnini asli holidan o`zgartirishga shifrlash, shifrlangan axborotni asli holiga keltirishga esa deshifrlash deyiladi.

Shifrlash – ochiq matn deb ataluvchi dastlabki matnni shifrlangan matn holatiga o`tkazish jarayonidir.

Deshifrlash – shifrlashga teskari bo`lgan jarayon, ya`ni kalit yordamida shifrlangan matnni dastlabki matn holatiga o`tkazishdir.

Kalit – bevosita dastlabki matnni shifrlash va deshifrlash uchun zarur bo`lgan ma`lumotdir.

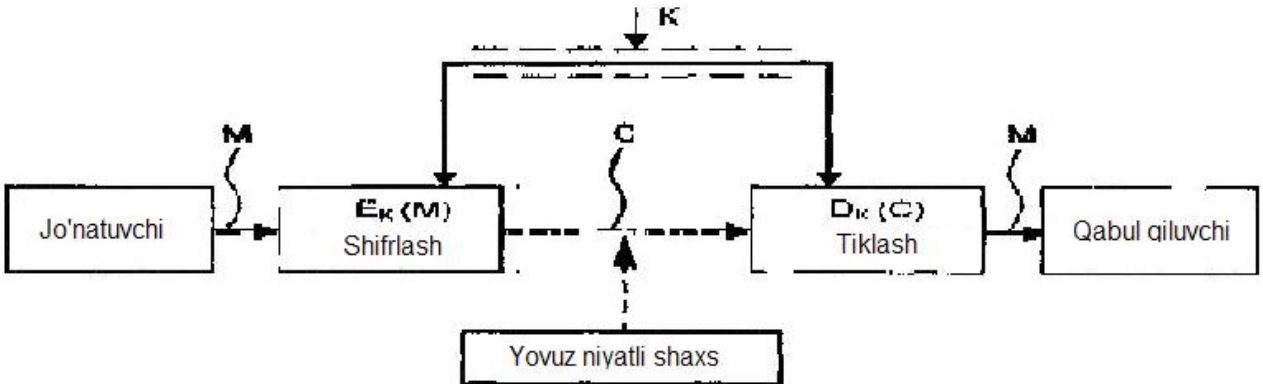
Kriptografik tizim yoki kriptotizim – ochiq matnni shifrlash (deshifrlash) jarayonini tashkil etuvchi amallar majmui bo`lib, matn belgilarini biror bir usulda almashtirishlar ketma-ketligidan iborat.

Kriptoanaliz yoki kriptotahlil esa shifrlash uslubini (kalitini yoki algoritmini) bilmagan holda shifrlangan matnning asli holatini topish uslublari masalalari bilan shug'ullanadi.

Kriptochidamlilik yoki kriptomustahkamlik - kriptotahlil orqali shifrlangan matnning asli holatini topishning qiyinlik darajasi.

Agar kriptotahlil orqali shifrlangan matnning asli holatini topishning iloji bo`lmasa, bu shifrlash kriptotizimi yuqori kriptochidamli deyiladi.

Uzatiladigan axborotni kriptografik tizim orqali himoyalashning umumiy sxemasi quyidagicha bo`ladi:



1.3.1-rasm

Uzatuvchi berilgan M xabarni biror bir kriptotizimda, tanlangan K kalit orqali, $S=E_k(M)$ yordamida shifrlaydi va C shifr matnni aloqa kanali orqali uzatadi.

Kanalda ushlab oluvchi kutib o`tiribdi va uning C shifr matnni ushlab olish ehtimoli katta. Ushlab oluvchi C shifr matn ma`nosini tushunmaydi va uni ochishga harakat qiladi. Ammo, unda kalit mavjud emas. Shuning uchun u C shifr matnni kalitsiz, kriptotahlil usullari orqali ochishga harakat qiladi. Agar xabarni shifrlash uchun ishlatilgan kriptotizim kriptochidamli bo`lsa, ushlab oluvchi uni ocha olmaydi.

Haqiqiy qabul qiluvchi S shifr matnni olgach, shifrlash uchun ishlatilgan kriptotizim va uning K kaliti orqali, $D=E_k^{-1}$ teskari o`zgartirishi yordamida qayta deshifrlaydi va ochiq matn M ko`rinishidagi birlamchi xabarni oladi:

$$D_k(C)= E_k^{-1}(E_k(M))=M$$

E_k dinamik o`zgartirish kriptoalgoritmlar deb nomlanuvchi kriptografik o`zgartirishlar oilasidan tanlanadi. Alohida ishlatovchi dinamik o`zgartirish tanlanadigan yordamchi parametr K kriptografik kalit deb ataladi. Kriptotizim har xil variantdagi tadbiqga ega: instruktsiyalar to`plami, apparat vositalar, kompyuterning kompleks dasturlari bo`lib, ular ochiq matnni shifrlaydi va har xil usullar orqali qayta ochadi.

Aniqroq aytganda kriptografik tizim teskari dinamik o`zgartirishli bir parametrli oila hisoblanadi.

$$E_k : \overline{M} \to \overline{C}$$

K (kalit) parametr K to`plamdan tanlanadi va bu to`plam kalitlar kengligi deyiladi.

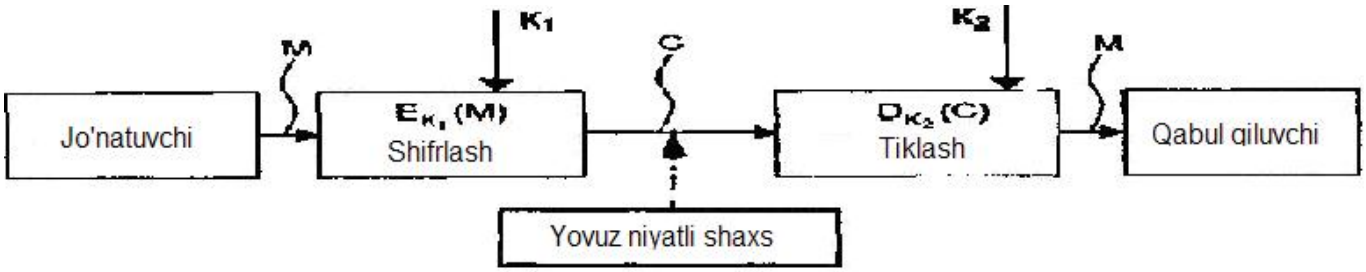
Umuman olganda shifrli dinamik o`zgartirish qayta ochish dinamik o`zgarishiga qarab simmetrik va assimmetrik bo`ladi. [6] Shuning uchun, bu dinamik o`zgartirish funktsiyasining muhim xususiyati kriptotizimlarni ikki sinfga ajratadi:

- simmetrik (bir kalitli) kriptotizimlar;

- assimmetrik (ikki kalitli) kriptotizimlar (ochiq kalit bilan).

Yagona yashirin kalitli simmetrik kriptotizim sxemasi 1.3.1-rasmda ko`rsatilgan edi. Unda shifrlash va qayta ochish bloklarida yagona yashirin kalit ishlatilgan.

K_1 va K_2 ikki har xil kalitli assimmetrik kriptotizimning umumiy sxemasi quyidagicha.



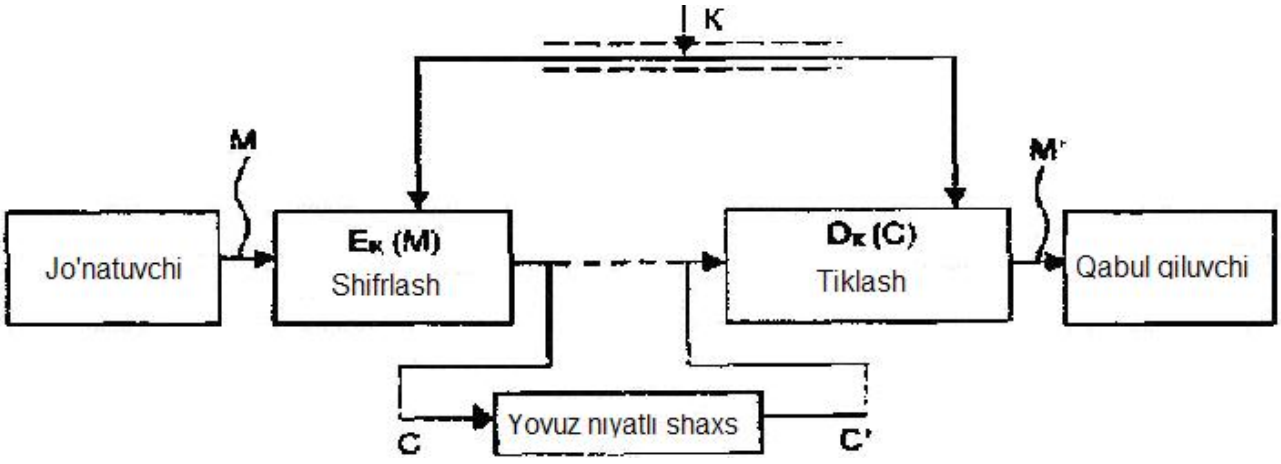
1.3.2-rasm

Bu kriptotizimda bir kalit ochiq bo`lsa, ikkinchisi yashirin bo`ladi.

Simmetrik kriptotizimlarda yashirin kalitni qabul qiluvchiga va uzatuvchiga kalitlarni tarqatishning himoyalangan kanali orqali uzatish kerak. Yashirin kalitlarni tarqatishning ham turli usullari mavjud. [6]

Assimmetrik kriptotizimlarda ochiq kalit himoyalanmagan kanal orqali uzatiladi, yashirin kalit esa generatsiyalangan o`rnida qolaveradi. [6]

Quyida ushlab oluvchining faol harakatlari holatidagi kriptotizimdagi axborot oqimi sxemasi keltirilmoqda.



1.3.3-rasm

Faol ushlab oluvchi nafaqat barcha shifr matnlarni o`qib olishi, balki o`z bilishicha ularni o`zgartirishi ham mumkin.

Ushlab oluvchi tomonidan ochiq matn M ni olish uchun S shifrlangan matnni qayta ochish yoki to`g’ri hisoblanishi zarur bo`lgan S’ shifr matnni olish uchun o`z

M’ matnni shifrlash va unda u haqiqiy kalitni bilmasa, bu harakat kriptoanalitik hujum deb ataladi.

Agar qo`llanilgan kriptoanalitik hujumlar qo`yilgan maqsadga olib kelmasa va kriptoanalitik haqiqiy kalitga ega bo`lmagan holda kriptotahlil orqali S dan M ni yoki M’ dan S’ ni chiqarib olmasa, demak bunday kriptotizim kriptochidamli hisoblanadi.

Omadli tahlilchi birlamchi matn yoki kalitni ochishi mumkin. Bundan tashqari u kriptotizimdagi kamchiliklarni topishi mumkin, bu esa yuqorida aytilgan natijalarga olib keladi.

Kriptotahlilning fundamental qoidasini birinchi bo`lib, XIX asrda gollandiyalik olim A. Kerkxoff keltirib, unda shifr chidamliligi (kriptotizimnin) faqatgina maxfiy kalit bilan aniqlanishi lozim degan. Boshqacha aytganda, Kerkxoff qoidasi shundan iboratki, dushmanga yashirin kalitdan boshqa shifrlash algoritmi ham unga ma`lum bo`lishi kerak. Bu shunday shartlanganki, kriptografik o`zgartirishlarni amalga oshiruvchi kriptotizimlar oilasi ochiq tizim sifatida qaraladi. Bunday qarash axborotni himoyalash texnologiyasini muhim tamoyilini ifodalaydi: tizimning himoyalanganligi maxfiy axborot yo`qolgan holatda tezkor o`zgartirish mumkin bo`lmagan biron-bir maxfiylikka bog’liq bo`lmasligi kerak. [4]

Oddiy holda kriptotizim apparat va dasturiy vositalar to`plamini ifodalab, uni ma`lum vaqt va vositalarni sarflagan holda o`zgartirish mumkin, kalit esa oson o`zgaruvchan ob`ekt hisoblanadi. Shu tufayli kriptotizim chidamliligi faqat kalit maxfiyligi bilan bog’liq bo`lishi kerak.

1.4. Kriptoanalitik hujumlar

XXI asrga kelib, o`zining beqiyos imkoniyatlari bilan birgalikda axborot - muammo, axborotdan himoyalanish esa ehtiyoj darajasiga ko`tarildi. O`tmishda kabutarlar, choparlar yoki pochta xizmati vositasida kerakli manzilga kunlab, haftalab va hatto oylab etib borgan axborot, kompyuter, internet kashf etilgach, axborot kommunikatsiya texnologiyalari yordamida soniyalar ichida butun dunyoga tarqalishga ulguryapti. Zamonaviy axborot kommunikatsiya texnologiyalarining jadal taraqqiyoti insoniyat hayotining barcha jabhalarida o`lkan imkoniyatlar eshigini ochishi bilan birga ayni paytda jiddiy tashvishlarni ham yuzaga keltirayotganligini ham inkor etib bo`lmaydi. Bugungi davr axborot makoni hisoblanmish internetda ham turli tahdid va axborot xurujlari kuchaydi. So`nggi paytlarda yuqori

texnologiyalar sohasi mutaxassislaridan tashqari sotsiologlar tomonidan ham ‘kiberxuruj’ atamasi tez – tez tilga olinadigan bo`ldi. Ba`zi ekspertlar bugun ko`plab davlatlarda kuzatilayotgan internet orqali informatsion xurujlar kiber urushning bir ko`rinishi bo`lishi mumkinligidan xavotirda ekanini va axborot xavfsizligini ta`minlash yanada murakkablashib borishini ham yashirmayapti.

Axborot xavfsizligi deb ma`lumotlarni yo`qotish va o`zgartirishga yo`naltirilgan tabiiy yoki sun`iy xossali tasodifiy va qasddan ta`sirlardan har qanday tashuvchilarda axborotning himoyalanganligiga aytiladi. Ilgarigi xavf faqatgina konfidentsial (maxfiy) xabarlar va hujjatlarni o`g’irlash yoki nusxa olishdan iborat bo`lsa, hozirgi paytdagi xavf esa kompyuter ma`lumotlari to`plami, elektron ma`lumotlar, elektron massivlardan ularning egasidan ruxsat so`ramasdan foydalanishdir. Bulardan tashqari, bu harakatlardan moddiy foyda olishga intilish ham rivojlanadi. [7]

Kriptografiya o`z oldiga yashirin ma`lumotlarni bilmoqchi bo`lgan begona kishilardan ma`lumotlarni yashirishni maqsad qilib qo`yadi. Bunday kishilarni kriptograflar yomon maqsadni ko`zlovchi kishilar, dushmanlar yoki axborotlarni o`g’irlovchilar deb ataydi. Shuning uchun ular xohlagan ma`lumotni qo`lga kiritishga intilishi va ma`lumotga kriptoanalitik hujum uyushtirishi mumkin.

Kriptoanalitik hujumlarning to`rt asosiy turi mavjud:

1. Faqat shifrmatnga ega bo`lgan kriptoanalitik hujum. Kriptoanalatik bir necha xabarli $S_1$, $S_2$,... $S_n$ shifrmatnlarga ega, bunda ularning barchasi birta $E_k$ shifrlash algoritmi bilan shifrlangan. Kriptoanalitikni ishi shundan iboratki, ko`p xabarlar imkoniyatidan kelib chiqqan holda M_1, M_2,... M_i birlamchi matnlarni ochish yoki yaxshisi shu xabarlarni shifrlash uchun ishlatilgan K kalitni hisoblab topish keyinchalik shu kalit bilan shifrlangan boshqa shifrmatnlarni ochish uchun kerak.

2. Ochiq matn mavjud holatdagi kriptoanalitik hujum. Kriptoanalitik bir necha S_1, S_2,... S_i shifrmatnlarga balki, shu xabarlarning M_1, M_2,... M_i ochiq matnlariga ham ega. Uning ishi shundan iboratki, shu xabarlarni shifrlashda ishlatilgan K kalitni shu kalit bilan yangi shifrlangan ixtiyoriy D_k qayta ochish algoritmini topish.

3. Ochiq matnni tanlash imkoniyati mavjud holatdagi kriptoanalitik hujum. Kriptoanalitik nafaqat bir necha S_1, S_2,... S_i shifrmatnlar va ularning ochiq matnlari M_1, M_2,... M_i ga ega, balki, o`z xohishi bo`yicha ochiq matnni tanlab so`ngra uni shifrlangan ko`rinishda olishi mumkin. Bunday kriptoanaliz ochiq matn ma`lum

bo`lgan kriptoanalizga qaraganda juda katta foyda berishi mumkin, chunki kriptoanalitik ochiq matnlarni shunday blokini tanlashi mumkinki, kalit to`g'risida ko`proq axborotga ega bo`lishi mumkin. Kriptoanalitikning ishi xabarni shifrlashda ishlatilgan K kalitni yoki shu kalit bilan shifrlangan yangi xabarlarni ochishi mumkin bo`lgan D_k algoritmini topish.

4. Ochiq matnni moslashuvchan tanlovi holatidagi kriptoanalitik hujum. Bu ochiq matn tanlashning maxsus varianti hisoblanadi. Kriptoanalitik nafaqat ochiq matnni tanlashi va shu matnni shifrlab olish mumkin balki, oldingi shifrlash natijasidan kelib chiqib o`z tanlovini o`zgartirishi mumkin. Ochiq matnni sodda tanlovli kriptoanalizda kriptoanalitik ochiq matnni shifrlash uchun bir nechta katta bloklarni tanlashi mumkin. Ochiq matnni moslashuvchan tanlovida u boshida kichik bloklarni tanlashi, so`ngra birinchi tanlovga qarab keyingi blokni tanlashi mumkin va hokazo. [7]

II. Uinstonning ‘ikkilangan kvadrat’ shifri dasturi

2.1. An`anaviy simmetrik kriptotizimlar

Kriptografiya – ma`lumotlarni o`zgartirish usullarining to`plam bo`lib, ma`lumotlarni himoyalash bo`yicha quyidagi ikkita asosiy muammolarni hal qilishga yo`naltirilgan: maxfiylik; yaxlitlik.

Maxfiylik orqali yovuz niyatli shaxslardan axborotni yashirish tushunilsa, yaxlitlik esa yovuz niyatli shaxslar tomonidan axborotni o`zgartira olmaslik haqida dalolat beradi.

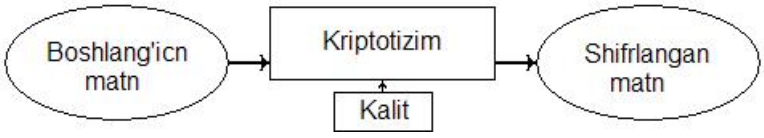
Kriptografiya nuqtai – nazaridan shifr – bu kalit demakdir va ochiq ma`lumotlar to`plamini yopiq (shifrlangan) ma`lumotlarga o`zgartirish kriptografiya o`zgartirishlar algoritmlari majmuasi hisoblanadi. [6]

Kalit – kriptografiya o`zgartirishlar algoritmining ba`zi – bir parametrlarining maxfiy holati bo`lib, barcha algoritmlardan yagona variantini tanlaydi. Kalitlarga nisbatan ishlatiladigan asosiy ko`rsatkich bo`lib, kriptomustahkamlik hisoblanadi.

Kriptografiya himoyasida shifrlarga nisbatan quyidagi talablar qo`yiladi:

- etarli darajada kriptomustahkamlik;
- shifrlar va qaytarish jarayonining oddiyligi;
- axborotlarni shifrlash oqibatida ular hajmini ortib ketmasligi;
- shifrlashdagi kichik xatolarga ta`sirchan bo`lmasligi;

Shifrlash jarayoni quyidagicha amalga oshiriladi:



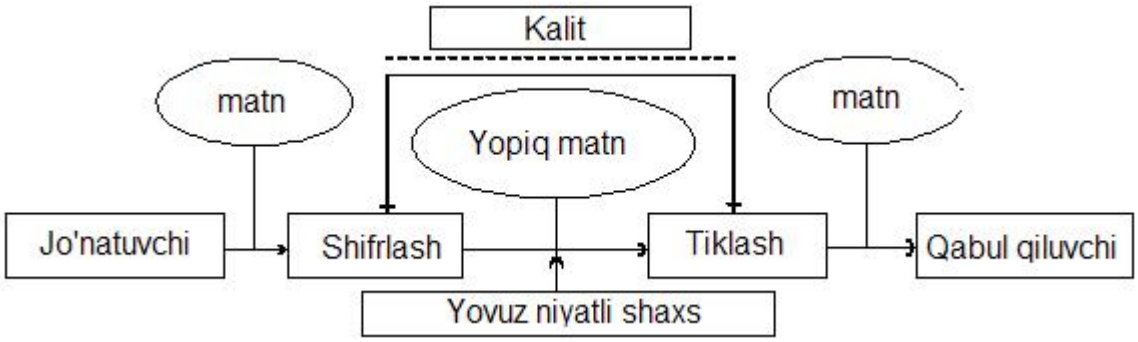
Tiklash yoki deshifrlash jarayoni quyidagicha amalga oshiriladi:

Kriptotizimlar ikki sinfga, ya`ni simmetrik (bir kalitli) kriptotizimlar va assimmetrik (ikki kalitli) kriptotizimlar (ochiq kalit bilan) ajratilishi haqida yuqorida aytib o`tgan edik.

Simmetrik shiflashtirishda axborotni shifrlash va uni qayta ochish uchun bitta kalitning o`zidan foydalaniladi. Bu usul foydalanilganda qabul qiluvchi va yuboruvchi oldindan qaysi kalit ishlatilishini kelishib olishlari kerak. Bu kalit faqat

qabul qiluvchi va yuboruvchida bo`lishi shart, boshqalarning esa kalit haqida ma`lumotga ega bo`lmaslikliklari talab qilinadi, aks holda kalit yovuz niyatli shaxslar qo`liga tushib qolishi mumkin. [6]

Simmetrik kriptotizimini quyidagicha tasvirlash mumkin.



Bu erda kalit qandaydir himoyalangan kanal orqali jo`natiladi (chizmada punktir chiziqlar bilan tasvirlangan).

Barcha simmetrik kriptotizimlar to`rt guruhga bo`linadi:

- o`rinlarini almashtirish;
- almashtirish;
- gammalashtirish;
- blokli shifrlash
- tahliliy o`zgartirish.

O`rinlarni almashtirish shifrlash usuli bo`yicha boshlang'ich matn belgilarining matnli ma`lum bir qismi doirasida maxsus qoidalar yordamida o`rinlari almashtiriladi.

Ushbu usul eng oddiy va eng qadimiy usuldir.

O`rinlarni almashtirish bir alfavitli yoki ko`p alfavitli bo`lishi mumkin.

Murakkab o`zgartirishli shifrlar ko`p alfavitli deb nomlanadi, chunki berilgan xabarning har bir ramzni shifrlash uchun o`zining sodda o`zgartirish shifrlashiga qo`llaniladi. Ko`p alfavitli o`rniga qo`yish ketma-ket va tsiklik qo`llaniladigan alfavitni almashtiradi.

r-alvafitli o`rniga qo`yishda berilgan xabarni x_0 ramzi V_0 alfavitning y_0 ramzi bilan almashtiriladi. X_1 ramzi V_1 alfavitning y_1 ramzi bilan va shu tariqa X_{r-1} ramz V_{r-1} alfavit y_{r-1} ramzi bilan X_r ramzi esa yana V_0 alfavit y_r ramzi bilan almashtiriladi.

Ko`p alfavitli o`rniga qo`yishning effekti shundaki birlamchi tilning statistik tabiati niqoblanishi ta`minlanadi, chunki A berilgan alfavitning aniq ramzi V_j

shifrlash alfavitlari har xil ramzlariga o`zgartirilishi mumkin. Himoyaning ta`minlanish darajasi V_j ketma-ket ishlatiladigan alfavitlar davri r uzunligiga proportsional.

Ko`p alfavitli joylashtirish shifrlarini taklif etgan va amaliyotga qo`llagan kriptograf Man Batist Albartidir. U nafaqat kriptograf balki mashhur arxitektor va san`atkor bo`lgan. 1956 yilda u tomonidan yozilgan 'SHifr to`g'risida traktat' deb nomlanuvchi asari kriptografiya bo`yicha Evropada 1-ilmiy ish hisoblangan. Butun dunyo kriptograflari A. Albertini kriptografiya asoschisi deb atashni ma`qul ko`rishadi. [8]

O`rinlarni almashtirish usullariga misol sifatida quyidagilarni keltirish mumkin:

- shifrlovchi jadval;
- sehrli kvadrat.

Shifrlovchi jadval usulida kalit sifatida quyidagilar qo`llaniladi:

- jadval o`lchovlari;
- so`z yoki so`zlar ketma-ketligi;
- jadval tarkibi xususiyatlari.

Almashtirish orqali amalga oshiriladigan shifrlashda shifrlanadigan matn ramzlari oldindan o`rnatilgan almashtirish qoidalari asosida u yoki bu alfavit harflari bilan almashtiriladi.

Sodda almashtirish shifrlarida berilgan matnning har bir ramzi shu alfavitning boshqa ramzlari bilan almashtiriladi. Ko`pincha sodda almashtirish shifrlarini bir alfavitli almashtirish shifrlari deb atashadi.

Gammalashtirish usuli bo`yicha boshlang'ich matn belgilari shifrlash gammasi belgilari, ya`ni tasodifiy belgilar ketma-ketligi bilan birlashtiriladi.

Tahliliy o`zgartirish usuli bo`yicha boshlang'ich matn belgilari analitik formulalar yordamida o`zgartiriladi, masalan, vektorni matritsaga ko`paytirish yordamida. Bu erda vektor matndagi belgilar ketma-ketligi bo`lsa, matritsa esa kalit sifatida xizmat qiladi.

Blokli shifrlash usuli boshlangich matn blokiga (qismiga) asosiy almashtirish usullarini ketma ket (mumkin bo`lgan almashtirishni takrorlash va galma – gal almashish) qo`llashga asoslangan. Rossiyaning GOST 28147-89 va AQSH ning DES shifrlash algoritmlari ushbu usulni qo`llaydi.

2.2. Bigrammali shifrlash

Trisemussning shifrlash jadvallari. 1508 yil Germaniyalik abbat Iogan Trisemuss “Poligrafiya” deb nomlanuvchi kitobni yozdi. Bu kitobda birinchi marta taxminiy tartibda alfavit bilan to`ldiruvchi shifrlash jadvallarini qo`llashni tizimli tushuntirib berdi. Bunday shifrni olish uchun alfavit harflarini va kalitli so`zni (yoki iborani) yozish uchun jadvallar qo`llanilgan. Jadvalga qator bo`yicha kalitli so`z kiritiladi, bunda takrorlanuvchi harflar tashlab yuboriladi. So`ngra bu jadval tartib bo`yicha alfavitning kiritilmagan harflari bilan to`ldiriladi. Kalitli so`z yoki iborani eslab qolish osonligi tufayli bunday yondashuv shifrlash va qayta ochish jarayonini soddalashtirar edi. [15]

Bu shifrlashni misolda ko`rib o`tsak. Lotin alifbosi uchun jadval hajmini 6x5 deb olamiz. Kalitli so`z sifatida esa AXBOROT so`zini olamiz. Agar kalitli so`zda harflar takrorlansa, navbatdagi takrorlanuvchi harf tashlab yuborilganligi uchun kalit so`z AXBORT ko`rinishni oladi. Kalitli so`z AXBORT ning harflarini jadvalning birinchi qatori, birinchi yacheykasidan boshlab joylashtirishni boshlaymiz. Agar birinchi qator to`lsa, harflarni ikkinchi qatordan boshlab joylashtirishni davom ettiramiz. Kalit so`z kiritilgach, alfavit harflarini boshdan boshlab jadvalga joylashtirishni boshlaymiz. Agar alfavit harfi kalit so`zda mavjud bo`lsa, u tashlab yuboriladi va navbatdagi harfni joylashtirish davom ettiriladi. Qator to`lgach navbatdagi qatordan joylashtirish boshlanadi.

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

Shifrlashda bu jadvaldan ochiq matnni navbatdagi harfi topiladi va shu ustundagi pastda joylashgan harf shifrmatn harfi sifatida yoziladi. Agar matn harfi eng pastki qatorda bo`lsa, shifr matn uchun shu ustunning eng yuqorigi harfi olinadi.

Masalan, shu jadval yordamida quyidagi xabarni shifrlasak:

MEN DIPLOM ISHIMNI HIMOYA QILDIM

Quyidagi shifr matnini olamiz:

UJV INWSEU NYMNUVN MNUEAT XNSINU

Bu shifr matni deshifrlash uchun jadvaldan shifr matnni navbatdagi harfi topiladi va shu ustundagi yuqorida joylashgan harf matn harfi sifatida yoziladi. Agar matn harfi eng yuqori qatorda bo`lsa, matn uchun shu ustunning eng quyi harfi olinadi.

Matn deshifrlansa:

MEN DIPLOM ISHIMNI HIMOYA QILDIM

Bunday shifrlash jadvallari ko`p grammali deyiladi, chunki shifrlash bir harfdan bajariladi. Trisemuss shifrlash jadvallari ikki harfdan shifrlay olishini birinchilardan bo`lib bilib olgan. Bunday shifrlashlar bigrammali shifrlashlar deyiladi.

Pleyferning bigrammali shifri. Pleyfer shifri 1854 yil ixtiro qilingan bo`lib, almashtirishning eng mashhur bigrammasi hisoblanadi. U birinchi jahon urushida Buyuk Britaniyada qo`llanilgan. Pleyferning shifri asosida birlamchi xabarda taxminiy joylashagan alifbo harflari shifrlovchi jadvali yotadi. [15]

Xabarni uzatuvchi va qabul qiluvchi tomonidan shifrlanadigan jadvalni eslab qolish qulayligi uchun kalitli so`z (yoki iborani) jadvalni boshlang'ich qatorlarini to`ldirishda ishlatish mumkin. Umuman olganda Pleyfer shifrlash jadvali strukturasi Trisemussning shifrlash jadvallariga o`xshash. Shuning uchun shifrlash va qayta ochish protseduralarini tushunish maqsadida Pleyfer tizimida oldin ko`rib o`tilgan Trisemuss shifrlash jadvalidan foydalanamiz:

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

Shifrlash protsedurasi quyidagi qadamlarni o`z ichiga oladi:

1. Berilgan xabar ochiq matni harflar jufti (bigramma) ga bo`linadi. Matn juft harflar sonidan iborat bo`lishi va unda ikkita bir xil harfdan bigramma bo`lmasligi kerak. Agar bu shartlar bajarilmasa, matn ba`zi orfografik xatolarga qaramasdan o`zgartiriladi.

2. Ochiq matn ketma – ket bigrammalari shifrlash jadvallari yordamida quyidagi qoidalar bo`yicha shifr matn bigrammalariga o`tkaziladi:

a. Agar ochiq matn bigrammasining ikkala harfi ham bir qator yoki ustunga joylashmasa (masalan, yuqoridagi jadvaldagi A va E harflari singari) unda aniqlanadigan harflar jufti uchun to`rtburchak burchaklari harfi topiladi. (Bizning misolda bu AEOT harflari AE harflar juftligi OT juftida akslanadi. Shifrmatn bigrammasida harflar ketma-ketligi ochiq matn bigrammasi harflar ketma-ketligida oynali munosabatda joylashgan bo`lishi kerak).

b. Agar ochiq matn bigrammalari harfi jadvalning bir ustunida joylashsa, unda shifr matn harfli deb ular tagida joylashgan harflar olinadi. (Masalan, CM bigrammasi HU shifr matnni beradi). Agar bunda ochiq matn harfi quyi qatorda joylashgan bo`lsa, unda shifrmatn uchun shu ustunning yuqori qatori harfi olinadi. (Masalan, CZ bigramma UX shifrmatn bigrammasini beradi).

c. Agar ochiq matnning bigrammasi ikkala harfi bitta qatorda joylashgan bo`lsa, unda shifrmatn harflari sifatida ulardan o`ngda joylashgan harflar olinadi. (Masalan, XO bigramasi BR shifr matn bigrammasini beradi). Agar bunda ochiq matn harfi eng o`ng ustunda joylashgan bo`lsa, shifr uchun shu qatorning chap ustuni harfi olinadi. (masalan, VX bigrammasi WS shifrmatn bigrammasini beradi).

Ochishda ya`ni deshifrlashda harakatlar teskari tartibda omalga oshiriladi. Shuni ta`kidlash lozimki, bigrammalar bo`yicha shifrlash shifrlar chidamligini tezkor oshiradi.

2.3. Uinstonning ‘ikkililangan kvadrat’ shifri

1854 yil angliyalik Charl’z Uinston bigrammalarni shifrlashning yangi metodini o`ylab topdi va shu tariqa kriptografiya rivojiga o`z hissasini qo`shdi. U polibian shifrga o`xshash bo`lgani uchun ‘ikkilangan kvadrat’ deb nomlanadi. Uinston shifri kriptografiya tarixida yangi bosqichni ochib berdi. Polibian shifridan farqli ravishda ‘ikkilangan kvadrat’ shifrlash usulida ikkita jadvaldan foydalanilgan. Bu jadvallar gorizontal joylashgan bo`lib, shifrlash Pleyfor shifri singari bigrammalar bo`yicha shifrlanadi. Murakkab bo`lmagan modifikatsiyalar orqali qo`lda shifrlash juda qulay bo`lib, kriptografiyada ishonchli yangi kriptografik tizimini dunyoga keltirdi. Bu usul juda ishonchli bo`lgani uchun undan Germaniyada hattoki ikkinchi jahon urushida ham foydalanilgan. [15] Axborotni shifrlash uchun kirill alfaviti harflari ixtiyoriy joylashgan ikkita jadval olingan.

Ж	Щ	Н	Ю	Р
И	Т	Ь	Ц	Б
Я	М	Е	.	С
В	Ы	П	Ч	
:	Д	У	О	К
З	Э	Ф	Г	Ш
Х	А	,	Л	Ъ

И	Ч	Г	Я	Т
,	Ж	Ь	М	О
З	Ю	Р	В	Щ
Ц	:	П	Е	Л
Ъ	А	Н	.	Х
Э	К	С	Ш	Д
Б	Ф	У	Ы	

Shifrlash uchun matn harflarini juft-juft qilib bo`laklarga, ya`ni bigrammalarga bo`lingan. Har bir bigramma alohida shifrlangan. Har bir juft bo`lakning birinchi harfi uchun chap tomondagi birinchi jadvaldan, ikkinchi harf uchun esa o`ng tomondagi ikkinchi jadvaldan foydalanilgan.

Shifrlashda juft bo`lakning birinchi harfini chap jadvaldan, ikkinchi harfini esa o`ng jadvaldan olingan. Shifrmatn harflarini olish uchun matn birinchi harfni chap jadvaldan, ikkinchisini esa o`ng jadvaldan topiladi, so`ngra shu harflar burchaklari bo`lgan xayolan to`rtburchak tuziladiki, bigramma hafrlari qarama-qarshi burchaklarda tursin. Bu to`rtburchakning boshqa burchaklaridagi harflar shifr bigrammani ifodalashadi. Aytaylik, berilgan matnning ИЛ bigrammasi shifrlansin. И harfi birinchi, chap jadvalning 1-ustun va 2-qatorida joylashgan. Л harfi esa ikkinchi, o`ng jadvalning 5-ustun va 4-qatorida joylashgan. Bu to`rtburchak 2 va 4 qatorlardan hamda chap jadvalning 1- va o`ng jadvalning 5-ustunidan tuzilgan. Shunday qilib, shifrmatn bigrammasiga o`ng jadval 5-ustun va 2-qatorida joylashgan О harfi va chap jadval 1-ustun va 4-qatordagi В harflari kiradi. Shunday qilib berilgan matnning ИЛ bigrammasi uchun ОВ shifrmatn bigrammasini olamiz.

Agar bigrammaning ikkala harfi ham bir qatorda joylashgan bo`lsa, unda shifrmatn harflari ham shu qatordan olinadi. Shifrmatn bigrammasi birinchi harfi chap jadvaldan xabar bigrammasi ikkinchi harfi ustuniga mos bo`lgan harf olinadi. Ikkinchisi esa o`ng jadvaldan xabar bigrammasi birinchi harfi joylashgan ustunga mos harfi olinadi. Shuning uchun ТО bigrammasi ЖБ shifrmatn bigrammasiga aylanadi. Xuddi shu tariqa xabar bigrammalari shifrlanadi.

Misol. Quyida berilgan xabarni shifrlang:

УИНСТОННИНГ ИККИЛАНГАН КВАДРАТ ШИФРИ

Berilgan xabarni bigrammalarga bo`lamiz (Probel uchun _ belgi qo`yamiz):

УИ НС ТО НН ИН Г_ ИК КИ ЛА НГ АН _К ВА ДР АТ _Ш ИФ РИ

Berilgan xabarga Uitstonning ‘ikkilangan kvadrat’ shifrini qo`llasak quyidagi bigrammali shifrmatnni olamiz:

ЪН ГФ ЖБ ГУ Ь: ДЛ ЖЗ ЪР ФО ГН УД :Ш :: НМ Щ_ ХЖ ТЖ

Bigrammali shifrmatnni birlashtirsak quyidagi oddiy i shifrmatnni olamiz:

ЪНГФЖБГУЬ:ДЛЖЗЪРФОГНУД:Ш::НМЩ_ХЖТЖ

Ochishda ya`ni deshifrlashda harakatlar teskari tartibda omalga oshiriladi.

Uitstonning “ikkililan kvadrat” shifrini kirill alfaviti uchun qo`llasak tanlangan jadval yacheykalari soni 35 ta bo`lishi kerak. Chunki unda nuqta, vergul va ikki nuqta singari tinish belgilar ham kiritilgan.

Yozuv qatori 30 tadan kam bo`lmasligа kerak, shunda uni ochish uchun juda katta qiyinchiliklar tugdiradi.

‘Ikkilangan kvadrat’ usuli shifrlanishi juda chidamli va qo`llashda sodda shifrlash hisoblanadi. [15]

2.4. Uinstonning “ikkilangan kvadrat” usulida matnni shifrlash va deshifrlash

Matnni Uinstonning ‘ikkilangan kvadrat’ usulida shifrlash. Lotin alfaviti harflarida berilgan matnni shifrlash algoritmini misol orqali tavsiflaymiz. U quyidagi qadamlardan iborat:

1. Lotin alfaviti harflari va tinish belgilarini berilish tartibi belgilab olinadi.

ABCDEFGHIJKLMNOPQRSTUVWXYZ- .,:;

Ular 32 ta.

2. Jadvallar Trisemussning shifrlash jadvallari usulidan foydalanib tuziladi.

a. Har bir jadval uchun alohida kalit so`z tanlanadi. (Kalit so`z uzunligi katta bo`lsa, shifrlash bardoshliligi yuqori bo`ladi.)

Chap jadval uchun kalit so`zi: KRIPNOGRAFIYANING SIMMETRIK USULI

O`ng jadval uchun kalit so`zi: SHIFRLASSH VA DESHIFRLASH JADVALLARI

b. Trisemussning shifrlash jadvallari usuliga muvofiq kalit so`zlardagi navbatdagi takrorlanuvchi harflar tushirib qoldiriladi.

Chap jadval uchun takrorlanuvchi harflari tushirib qoldirilgan kalit so`zi:

KRIPNOGAFY SMETUL

O`ng jadval uchun takrorlanuvchi harflari tushirib qoldirilgan kalit so`zi:

SHIFRLA VDEJ

c. Jadval o`lchamlari belgilanadi.

Belgilar soni 32 ta, shuning uchun jadval o`lchamini 4x8 deb kelishib olamiz.

d. Jadvallarga Trisemussning shifrlash jadvallari usuliga muvofiq kalit so`z va lotin alfaviti harflari joylashtiriladi.

Chap va o`ng jadvallarga belgilarni quyidagi tartibda kiritamiz.

Kalit so`z harflarini jadvalning birinchi qatori, birinchi yacheykasidan boshlab joylashtirishni boshlaymiz. Agar birinchi qator to`lsa, harflarni ikkinchi qatordan boshlab joylashtirishni davom ettiramiz. Kalit so`z kiritilgach, alfavit harflarini boshdan boshlab jadvalga joylashtirishni boshlaymiz. Agar alfavit harfi kalit so`zda mavjud bo`lsa, u tashlab yuboriladi va navbatdagi harfni joylashtirish davom ettiriladi. Qator to`lgach navbatdagi qatordan joylashtirish boshlanadi.

K	R	I	P	N	O	G	A
F	Y	_	S	M	E	T	U
L	B	C	D	H	J	Q	V
W	X	Z	-	.	,	:	;

S	H	I	F	R	L	A	_
V	D	E	J	B	C	G	K
M	N	O	P	Q	T	U	W
X	Y	Z	-	.	,	:	;

3. Maxfiy xabar matni olinadi.

Quyida berilgan xabarni shifrlang:

UINSTONNING IKKILANGAN KVADRAT SHIFRI

4. Berilgan xabar bigrammalarga bo`linadi.

Xabarni bigrammalarga bo`lamiz (Probel uchun _ belgi qo`yamiz):

UI NS TO NN IN G_ IK KI LA NG AN _K VA DR AT _S HI FR I_

5. Xabar shifrlanadi.

a. Har bir bigramma, ya`ni juft bo`lak alohida shifrlanadi.

b. Har bir juft bo`lakning birinchi harfi uchun chap tomondagi birinchi jadvaldan, ikkinchi harf uchun esa o`ng tomondagi ikkinchi jadvaldan foydalaniladi.

c. Agar juft bo`lakning harflari jadvallarning turli qatorlarida joylashgan bo`lsa, juft bo`lakning birinchi harfini chap jadvaldan, ikkinchi harfini esa o`ng

jadvaldan topiladi. So`ngra shu harflar burchaklari bo`lgan xayoliy to`rtburchak tuziladi. Juft bo`lak hafrlari xayoliy to`rtburchakning qarama-qarshi burchaklarda turadi. Xayoliy turtburchakning o`ng jadvalida turgan xabar harfining boshqa burchagidagi harf shifr juft bo`lagining birinchi harfi, chap jadvalida turgan xabar harfining boshqa burchagidagi harf esa shifr juft bo`lagining ikkinchi harfi bo`ladi.

d. Agar juft bo`lakning ikkala harfi ham bir qatorda joylashgan bo`lsa, unda shifr harflari ham shu qatordan olinadi. Shifr juft bo`lak birinchi harfi o`ng jadvaldan, chap jadvalda xabar juft bo`lagi birinchi harfi joylashgan ustuniga mos xonadagi harfi olinadi. Shifr juft bo`lak ikkinchi harfi chap jadvaldan, o`ng jadvalda xabar juft bo`lagi ikkinchi harfi joylashgan ustuniga mos xonadagi harfi olinadi.

e. Keyin navbatdagi bigramma, ya`ni juft bo`lakka o`tiladi va shifrlash uchun b-qadamga o`tiladi. Agar barcha bigrammalar shifrlansa, shifrlash to`xtatiladi.

Berilgan xabarga Uitstonning ‘ikkilangan kvadrat’ shifrini qo`llasak quyidagi bigrammali shifrmatnni olamiz:

EA LM EQ HH HC AA __ SI UK AM HV EU UA QP LV VI ON BK IA

6. Shifr bigrammalarini birlashtirib shifrmatn olinadi.

Bigrammali shifrmatnni birlashtirsak quyidagi oddiy shifrmatnni olamiz:

EALMEQHHHCAA__SIUKAMHVEUUAQPLVVIONBKIA

Shifrlashni tahlil qilamiz:

Shifrlanadigan juft bo`lakning birinchi harfi $M_1$, ikkinchi harfi $M_2$ bo`lsin. Shifrlangan juft bo`lakning birinchi harfi $U_1$, ikkinchi harfi $U_2$ bo`lsin. Shifrlashni quyidagi jadvallar uchun ko`rib chiqamiz:

A_{11} A_{12} A_{13} A_{14} A_{15} A_{16} A_{17} A_{18}	B_{11} B_{12} B_{13} B_{14} B_{15} B_{16} B_{17} B_{18}
A_{21} A_{22} A_{23} A_{24} A_{25} A_{26} A_{27} A_{28}	B_{21} B_{22} B_{23} B_{24} B_{25} B_{26} B_{27} B_{28}
A_{31} A_{32} A_{33} A_{34} A_{35} A_{36} A_{37} A_{38}	B_{31} B_{32} B_{33} B_{34} B_{35} B_{36} B_{37} B_{38}
A_{41} A_{42} A_{43} A_{44} A_{45} A_{46} A_{47} A_{48}	B_{41} B_{42} B_{43} B_{44} B_{45} B_{46} B_{47} B_{48}

Shifrlash uchun M_1 harfni A jadvaldan, M_2 harfni esa B jadvaldan izlab topamiz. Izlab topilgan harflar jadvallar qatorlarida joylashishi bo`yicha ikki xil holatda bo`lishi mumkin:

1. (M_1M_2) juft bo`lakning harflari jadvallarning turli qatorlarida joylashgan.

2. (M_1M_2) juft bo`lakning harflari jadvallarning bir qatorida joylashgan.

1-holat. (M_1M_2) juft bo`lakning harflari jadvallarning turli qatorlarida joylashgan:

a. Birinchi juftlik $M_1=A_{ij}$ harfi ikkinchi juftlik $M_2=B_{mn}$ harfiga nisbatan yuqori qatorda joylashgan, ya`ni i<m shart bajarilsa, shifrmatn juftligi uchun $U_1= B_{in}$ va $U_2= A_{mj}$ harflari olinadi.

b. Birinchi juftlik $M_1=A_{ij}$ harfi ikkinchi juftlik $M_2=B_{mn}$ harfiga nisbatan quyi qatorda joylashgan, ya`ni i>m shart bajarilsa, shifrmatn juftligi uchun $U_1= B_{in}$ va $U_2= A_{mj}$ harflari olinadi.

Demak, (M_1M_2) juft bo`lakning birinchi $M_1=A_{ij}$ harfi va ikkinchi $M_2=B_{mn}$ harfi jadvallarning turli qatorlarida joylashgan bo`lsa, u holda birinchi va ikkinchi harflarning o`zaro qanday joylashishidan qat`iy nazar shifrmatn juftligi (U_1U_2) quyidagicha olinadi:

$U_1= B_{in}$, $U_2= A_{mj}$

2-holat. (M_1M_2) juft bo`lakning harflari jadvallarning bir qatorida joylashgan:

a. Birinchi juftlik $M_1=A_{ij}$ harfi ikkinchi juftlik $M_2=B_{mn}$ harfiga nisbatan oldingi ustunda joylashgan, ya`ni j<n shart bajarilsa, shifrmatn juftligi uchun $U_1= B_{ij}$ va $U_2= A_{mn}$ harflari olinadi.

b. Birinchi juftlik $M_1=A_{ij}$ harfi ikkinchi juftlik $M_2=B_{mn}$ harfiga nisbatan keyingi ustunda joylashgan, ya`ni j>n shart bajarilsa, shifrmatn juftligi uchun $U_1= B_{ij}$ va $U_2= A_{mn}$ harflari olinadi.

c. Birinchi juftlik $M_1=A_{ij}$ harfi va ikkinchi juftlik $M_2=B_{mn}$ harflari bir ustunda joylashgan, ya`ni j=n shart bajarilsa, shifrmatn juftligi uchun $U_1= B_{ij}$ va $U_2= A_{mn}$ harflari olinadi.

Demak, (M_1M_2) juft bo`lakning birinchi $M_1=A_{ij}$ harfi va ikkinchi $M_2=B_{mn}$ harfi jadvallarning bir qatorida joylashgan bo`lsa, u holda birinchi va ikkinchi harflarning o`zaro qanday joylashishidan qat`iy nazar shifrmatn juftligi (U_1U_2) quyidagicha olinadi:

$U_1= B_{ij}$, $U_2= A_{mn}$

Misol. Uinstonning “ikkilangan kvadrat” usuli uchun ('A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z', ' ', '.', ',', '?', '!', '=', '+', '-', ':', ';', '“',' (', ')', '%') harf va belgilardan tashkil topgan alfavitni tanlaymiz.

1, Alfavit 40 ta elementga ega. Shuning uchun jadvalni ustuni sonini 8 ta, qatorlar sonini 5 ta deb olsak bo`ladi.

2. Jadvallarni Trisemussning shifrlash jadvallari usulidan foydalanib tuzamiz. Buning uchun birinchi jadval uchun ‘Muhammad’, ikkinchi jadval uchun ‘Majidov’ kalit so`zlarni tanlaymiz.

3. Kalit so`zlardagi takrorlanuvchi harflarni tushirib qoldirsak, birinchi jadval uchun ‘Muhad’, ikkinchi jadval uchun ‘Majidov’ kalit so`z hosil bo`ladi.

4. Bu kalit so`zlarning har bir harfini jadvallarning xonalariga birinchi qatoridan boshlab navbat bilan kiritamiz. So`ngra bu kalit so`zda mavjud bo`lmagan alfavit harflari va belgilarini jadvallarning xonalariga navbat bilan kiritamiz. Natijada quyidagi jadvallarni olamiz:

M	U	H	A	D	B	C	E
F	G	I	J	K	L	N	O
P	Q	R	S	T	V	W	X
Y	Z		.	,	?	!	=
+	-	:	;	“	(	)	%

M	A	J	I	D	O	V	B
C	E	F	G	H	K	L	N
P	Q	R	S	T	U	W	X
Y	Z		.	,	?	!	=
+	-	:	;	“	(	)	%

5. Shifrlanadigan matnni beramiz:

Uinstonning ikkilangan kvadrat shifri

6. Shifrlanadigan matnni bigrammalarga, ya`ni juft bo`laklarga bo`lamiz.

UI NS TO NN IN G IK KI LA NG AN K VA DR AT S HI FR I

7. Har bir juft bo`lakni alohida-alohida shifrlaymiz.

Shifrlanadigan juft bo`lakning birinchi harfi $M_1$, ikkinchi harfi $M_2$ bo`lsin. Shifrlangan juft bo`lakning birinchi harfi $U_1$, ikkinchi harfi $U_2$ bo`lsin. Shifrlashni quyidagi jadvallar uchun ko`rib chiqamiz:

$A_{11}\ A_{12}\ A_{13}\ A_{14}\ A_{15}\ A_{16}\ A_{17}\ A_{18}$ $\qquad$ $B_{11}\ B_{12}\ B_{13}\ B_{14}\ B_{15}\ B_{16}\ B_{17}\ B_{18}$

$A_{21}\ A_{22}\ A_{23}\ A_{24}\ A_{25}\ A_{26}\ A_{27}\ A_{28}$ $\qquad$ $B_{21}\ B_{22}\ B_{23}\ B_{24}\ B_{25}\ B_{26}\ B_{27}\ B_{28}$

$A_{31}\ A_{32}\ A_{33}\ A_{34}\ A_{35}\ A_{36}\ A_{37}\ A_{38}$ $\qquad$ $B_{31}\ B_{32}\ B_{33}\ B_{34}\ B_{35}\ B_{36}\ B_{37}\ B_{38}$

$A_{41}\ A_{42}\ A_{43}\ A_{44}\ A_{45}\ A_{46}\ A_{47}\ A_{48}$ $\qquad$ $B_{41}\ B_{42}\ B_{43}\ B_{44}\ B_{45}\ B_{46}\ B_{47}\ B_{48}$

Shifrlash uchun M_1 harfni A jadvaldan, M_2 harfni esa B jadvaldan izlab topamiz, ya`ni:

$M_1=A_{ij}$ va $M_2=B_{mn}$

a. Agar matn (M_1M_2) juft bo`lakning harflari jadvallarning turli qatorlarida joylashgan bo`lsa, u holda shifrmatn (U_1U_2) juft bo`lak quyidagicha olinadi:

$U_1= B_{in}$, $U_2= A_{mj}$

b. Agar matn (M_1M_2) juft bo`lakning harflari jadvallarning bir qatorida joylashgan bo`lsa, u holda u holda shifrmatn (U_1U_2) juft bo`lak quyidagicha olinadi:

$U_1= B_{ij}$, $U_2= A_{mn}$

Bigrammalarga ajratilgan matnni Uinston ikkilangan kvadrat usuli bo`yicha har bir juftini jadvaldagi o`rnini topamiz va uni mos harfga almashtiramiz.

UI NS TO NN IN G IK KI LA NG AN K VA DR AT S HI FR I

Matn UI o`rni $A_{12}B_{14}$ bo`lsa, shifrmatn o`rni $B_{12}A_{14}$ va shifrmatn AA bo`ladi.

Matn NS o`rni $A_{27}B_{34}$ bo`lsa, shifrmatn o`rni $B_{24}A_{37}$ va shifrmatn GW bo`ladi.

Matn TO o`rni $A_{35}B_{16}$ bo`lsa, shifrmatn o`rni $B_{36}A_{15}$ va shifrmatn UD bo`ladi.

Matn NN o`rni $A_{27}B_{28}$ bo`lsa, shifrmatn o`rni $B_{27}A_{28}$ va shifrmatn LO bo`ladi.

Matn IN o`rni $A_{23}B_{28}$ bo`lsa, shifrmatn o`rni $B_{23}A_{28}$ va shifrmatn FO bo`ladi.

Matn G o`rni $A_{22}B_{43}$ bo`lsa, shifrmatn o`rni $B_{23}A_{42}$ va shifrmatn FZ bo`ladi.

Matn IK o`rni $A_{23}B_{26}$ bo`lsa, shifrmatn o`rni $B_{23}A_{26}$ va shifrmatn FL bo`ladi.

Matn KI o`rni $A_{25}B_{14}$ bo`lsa, shifrmatn o`rni $B_{24}A_{15}$ va shifrmatn GD bo`ladi.

Matn LA o`rni $A_{26}B_{12}$ bo`lsa, shifrmatn o`rni $B_{22}A_{16}$ va shifrmatn EB bo`ladi.

Matn NG o`rni $A_{27}B_{24}$ bo`lsa, shifrmatn o`rni $B_{27}A_{24}$ va shifrmatn LJ bo`ladi.

Matn AN o`rni $A_{14}B_{28}$ bo`lsa, shifrmatn o`rni $B_{18}A_{24}$ va shifrmatn BJ bo`ladi.

Matn K o`rni $A_{43}B_{26}$ bo`lsa, shifrmatn o`rni $B_{46}A_{23}$ va shifrmatn ?I bo`ladi.

Matn VA o`rni $A_{36}B_{12}$ bo`lsa, shifrmatn o`rni $B_{32}A_{16}$ va shifrmatn QB bo`ladi.

Matn DR o`rni $A_{15}B_{33}$ bo`lsa, shifrmatn o`rni $B_{13}A_{35}$ va shifrmatn JT bo`ladi.

Matn AT o`rni $A_{14}B_{35}$ bo`lsa, shifrmatn o`rni $B_{15}A_{34}$ va shifrmatn DS bo`ladi.

Matn S o`rni $A_{43}B_{34}$ bo`lsa, shifrmatn o`rni $B_{44}A_{33}$ va shifrmatn .R bo`ladi.

Matn HI o`rni $A_{13}B_{14}$ bo`lsa, shifrmatn o`rni $B_{13}A_{14}$ va shifrmatn JA bo`ladi.

Matn FR o`rni $A_{21}B_{33}$ bo`lsa, shifrmatn o`rni $B_{23}A_{31}$ va shifrmatn FP bo`ladi.

Matn I o`rni $A_{23}B_{43}$ bo`lsa, shifrmatn o`rni $B_{23}A_{43}$ va shifrmatn F bo`ladi.

Natijada matnni shifrlab, quyidagi shifrmatnni olamiz.

Shifrlanadigan matn: UINSTONNING IKKILANGAN KVADRAT SHIFRI

Shifrlangan matn: AAGWUDLOFOFZFLGDEBLJBJ?IQBJTDS.RJAFPF

Shifr matnni Uinstonning ‘ikkilangan kvadrat’ usulida deshifrlash. Lotin alfaviti harflarida berilgan shifr matnni deshifrlash algoritmini misol orqali tavsiflaymiz. U quyidagi qadamlardan iborat:

1. Lotin alfaviti harflari va tinish belgilarini berilish tartibi xabar beruvchidan qabul qilib olinadi. Deshifrlovchi bu tartibni o`zgartira olmaydi. U 32 ta belgidan iborat bo`lib, quyidagichadir:

ABCDEFGHIJKLMNOPQRSTUVWXYZ-_.,:;

2. Jadvallar Trisemussning shifrlash jadvallari usulidan foydalanib tuziladi.

a. Har bir jadval uchun alohida kalit so`z xabar beruvchidan qabul qilib olinadi. Deshifrlovchi bu so`zlarni o`zgartira olmaydi.

Chap jadval uchun kalit so`zi: KRIPNOGRAFIYANING SIMMETRIK USULI

O`ng jadval uchun kalit so`zi: SHIFRLASSH VA DESHIFRLASH JADVALLARI

b. Trisemussning shifrlash jadvallari usuliga muvofiq kalit so`zlardagi navbatdagi takrorlanuvchi harflar tushirib qoldiriladi.

Chap jadval uchun takrorlanuvchi harflari tushirib qoldirilgan kalit so`zi:

KRIPNOGAFY SMETUL

O`ng jadval uchun takrorlanuvchi harflari tushirib qoldirilgan kalit so`zi:

SHIFRLA VDEJ

c. Jadval o`lchamlari xabar beruvchidan qabul qilib olinadi. Deshifrlovchi bu o`lchamlarni o`zgartira olmaydi. Jadval o`lchami 4x8.

d. Jadvallarga Trisemussning shifrlash jadvallari usuliga muvofiq kalit so`z va lotin alfaviti harflari joylashtiriladi.

Chap va o`ng jadvallarga belgilarni quyidagi tartibda kiritamiz.

Kalit so`z harflarini jadvalning birinchi qatori, birinchi yacheykasidan boshlab joylashtirishni boshlaymiz. Agar birinchi qator to`lsa, harflarni ikkinchi qatordan boshlab joylashtirishni davom ettiramiz. Kalit so`z kiritilgach, alfavit harflarini boshdan boshlab jadvalga joylashtirishni boshlaymiz. Agar alfavit harfi kalit so`zda mavjud bo`lsa, u tashlab yuboriladi va navbatdagi harfni joylashtirish davom ettiriladi. Qator to`lgach navbatdagi qatordan joylashtirish boshlanadi.

K	R	I	P	N	O	G	A
F	Y	_	S	M	E	T	U
L	B	C	D	H	J	Q	V
W	X	Z	-	.	,	:	;

S	H	I	F	R	L	A	_
V	D	E	J	B	C	G	K
M	N	O	P	Q	T	U	W
X	Y	Z	-	.	,	:	;

3. Shifr matn olinadi.

Quyida berilgan shifr matnni deshifrlang:

EALMEQHHHCAA__SIUKAMHVEUUAQPLVVIONBKIA

4. Berilgan shifr matn bigrammalarga bo`linadi.

Shifr matnni bigrammalarga bo`lamiz (Probel uchun _ belgi qo`yamiz):

EA LM EQ HH HC AA __ SI UK AM HV EU UA QP LV VI ON BK IA

5. Shifr matn deshifrlanadi.

a. Har bir bigramma, ya`ni juft bo`lak alohida deshifrlanadi.

b. Har bir juft bo`lakning birinchi harfi uchun o`ng tomondagi ikkinchi jadvaldan, ikkinchi harf uchun esa chap tomondagi birinchi jadvaldan foydalaniladi.

c. Agar juft bo`lakning harflari jadvallarning turli qatorlarida joylashgan bo`lsa, juft bo`lakning birinchi harfini o`ng jadvaldan, ikkinchi harfini esa chap jadvaldan topiladi. So`ngra shu harflar burchaklari bo`lgan xayoliy to`rtburchak tuziladi. Juft bo`lak hafrlari xayoliy to`rtburchakning qarama-qarshi burchaklarda turadi. Xayoliy to`rtburchakning chap jadvalida turgan shifr harfining boshqa burchagidagi harf xabar juft bo`lagining birinchi harfi, o`ng jadvalida turgan shifr harfining boshqa burchagidagi harf esa xabar juft bo`lagining ikkinchi harfi bo`ladi.

d. Agar juft bo`lakning ikkala harfi ham bir qatorda joylashgan bo`lsa, unda xabar harflari ham shu qatordan olinadi. Xabar juft bo`lak birinchi harfi chap jadvaldan, o`ng jadvalda shifr juft bo`lagi birinchi harfi joylashgan ustuniga mos xonadagi harfi olinadi. Xabar juft bo`lak ikkinchi harfi o`ng jadvaldan, chap jadvalda shifr juft bo`lagi ikkinchi harfi joylashgan ustuniga mos xonadagi harfi olinadi.

e. Keyin navbatdagi bigramma, ya`ni juft bo`lakka o`tiladi va deshifrlash uchun b-qadamga o`tiladi. Agar barcha bigrammalar deshifrlansa, deshifrlash to`xtatiladi.

Berilgan shifr matnga Uitstonning ‘ikkilanga kvadrat’ shifrini qo`llasak quyidagi bigrammali xabarni olamiz:

UI NC TO NN IN G_ IK KI LA NG AN _K VA DR AT _S HI FR I_

6. Xabar bigrammalarini birlashtirib xabar olinadi.

Bigrammali xabarni birlashtirsak quyidagi oddiy xabarni olamiz:

UINCTONNING IKKILANGAN KVADRAT SHIFRI

Deshifrlashni tahlil qilamiz:

Deshifrlanadigan juft bo`lakning birinchi harfi $M_1$, ikkinchi harfi $M_2$ bo`lsin. Shifrlangan juft bo`lakning birinchi harfi $U_1$, ikkinchi harfi $U_2$ bo`lsin. Shifrlashni quyidagi jadvallar uchun ko`rib chiqamiz:

$A_{11}\ A_{12}\ A_{13}\ A_{14}\ A_{15}\ A_{16}\ A_{17}\ A_{18}$	$B_{11}\ B_{12}\ B_{13}\ B_{14}\ B_{15}\ B_{16}\ B_{17}\ B_{18}$
$A_{21}\ A_{22}\ A_{23}\ A_{24}\ A_{25}\ A_{26}\ A_{27}\ A_{28}$	$B_{21}\ B_{22}\ B_{23}\ B_{24}\ B_{25}\ B_{26}\ B_{27}\ B_{28}$
$A_{31}\ A_{32}\ A_{33}\ A_{34}\ A_{35}\ A_{36}\ A_{37}\ A_{38}$	$B_{31}\ B_{32}\ B_{33}\ B_{34}\ B_{35}\ B_{36}\ B_{37}\ B_{38}$
$A_{41}\ A_{42}\ A_{43}\ A_{44}\ A_{45}\ A_{46}\ A_{47}\ A_{48}$	$B_{41}\ B_{42}\ B_{43}\ B_{44}\ B_{45}\ B_{46}\ B_{47}\ B_{48}$

Deifrlash uchun M_1 harfni B jadvaldan, M_2 harfni esa A jadvaldan izlab topamiz. Izlab topilgan harflar jadvallar qatorlarida joylashishi bo`yicha ikki xil holatda bo`lishi mumkin:

1. (M_1M_2) juft bo`lakning harflari jadvallarning turli qatorlarida joylashgan.

2. (M_1M_2) juft bo`lakning harflari jadvallarning bir qatorida joylashgan.

1-holat. (M_1M_2) juft bo`lakning harflari jadvallarning turli qatorlarida joylashgan:

a. Birinchi juftlik $M_1=B_{mn}$ harfi ikkinchi juftlik $M_2=A_{ij}$ harfiga nisbatan yuqori qatorda joylashgan, ya`ni $m<i$ shart bajarilsa, shifrmatn juftligi uchun $U_1= A_{mj}$ va $U_2= B_{in}$ harflari olinadi.

b. Birinchi juftlik $M_1=B_{mn}$ harfi ikkinchi juftlik $M_2=A_{ij}$ harfiga nisbatan quyi qatorda joylashgan, ya`ni $m>i$ shart bajarilsa, shifrmatn juftligi uchun $U_1= A_{mj}$ va $U_2= B_{in}$ harflari olinadi.

Demak, (M_1M_2) juft bo`lakning birinchi $M_1=B_{mn}$ harfi va ikkinchi $M_2=A_{ij}$ harfi jadvallarning turli qatorlarida joylashgan bo`lsa, u holda birinchi va ikkinchi harflarning uzaro qanday joylashishidan qat`iy nazar shifrmatn juftligi (U_1U_2) quyidagicha olinadi:

$U_1= A_{mj}$, $U_2= B_{in}$

2-holat. (M_1M_2) juft bo`lakning harflari jadvallarning bir qatorida joylashgan:

a. Birinchi juftlik $M_1=B_{mn}$ harfi ikkinchi juftlik $M_2=A_{ij}$ harfiga nisbatan oldingi ustunda joylashgan, ya`ni $n<j$ shart bajarilsa, shifrmatn juftligi uchun $U_1= A_{mn}$ va $U_2= B_{ij}$ harflari olinadi.

b. Birinchi juftlik $M_1=B_{mn}$ harfi ikkinchi juftlik $M_2=A_{ij}$ harfiga nisbatan keyingi ustunda joylashgan, ya`ni j>n shart bajarilsa, shifrmatn juftligi uchun $U_1= A_{mn}$ va $U_2= B_{ij}$ harflari olinadi.

c. Birinchi juftlik $M_1=B_{mn}$ harfi va ikkinchi juftlik $M_2=A_{ij}$ harflari bir ustunda joylashgan, ya`ni j=n shart bajarilsa, shifrmatn juftligi uchun $U_1= A_{mn}$ va $U_2= B_{ij}$ harflari olinadi.

Demak, (M_1M_2) juft bo`lakning birinchi $M_1=B_{mn}$ harfi va ikkinchi $M_2=A_{ij}$ harfi jadvallarning bir qatorida joylashgan bo`lsa, u holda birinchi va ikkinchi harflarning o`zaro qanday joylashishidan qat`iy nazar shifrmatn juftligi (U_1U_2) quyidagicha olinadi:

$U_1= A_{mn}$, $U_2= B_{ij}$

Misol. Yuqorida berilgan matnni shifrladik. endi uni deshifrlaymiz. Shifrlangan matnni deshifrlash uchun:

1. Shifrlashda ishlatilgan alfavit aynan o`zgarishsiz qabul qilinadi.

2. Jadval o`lchamlari o`zgarmaydi, ustun soni 8 ta, qatorlar soni 5 ta deb olinadi.

3. Birinchi jadval uchun ‘Muhammad’, ikkinchi jadval uchun ‘Majidov’ kalit so`zlar o`zgarishsiz olinadi.

4. Kalit so`zlardagi takrorlanuvchi harflarni tushirib qoldirib, birinchi jadval uchun ‘Muhad’, ikkinchi jadval uchun ‘Majidov’ kalit so`z hosil qilinadi.

5. Bu kalit so`zlarning har bir harfini jadvallarning xonalariga birinchi qatoridan boshlab navbat bilan kiritamiz. So`ngra bu kalit so`zda mavjud bo`lmagan alfavit harflari va belgilarini jadvallarning xonalariga navbat bilan kiritamiz. Natijada quyidagi jadvallarni olamiz:

M	U	H	A	D	B	C	E
F	G	I	J	K	L	N	O
P	Q	R	S	T	V	W	X
Y	Z		.	,	?	!	=
+	-	:	;	“	(	)	%

M	A	J	I	D	O	V	B
C	E	F	G	H	K	L	N
P	Q	R	S	T	U	W	X
Y	Z		.	,	?	!	=
+	-	:	;	“	(	)	%

6. Shifrlangan matnni beramiz:

AAGWUDLOFOFZFLGDEBLJBJ?IQBJTDS.RJAFPF

7. Shifrlangan matnni bigrammalarga, ya`ni juft bo`laklarga bo`lamiz.

AA GW UD LO FO FZ FL GD EB LJ BJ ?I QB JT DS .R JA FP F

8. Har bir juft bo`lakni alohida-alohida deshifrlaymiz.

Deshifrlanadigan juft bo`lakning birinchi harfi $M_1$, ikkinchi harfi $M_2$ bo`lsin. Deshifrlangan juft bo`lakning birinchi harfi $U_1$, ikkinchi harfi $U_2$ bo`lsin. Deshifrlashni quyidagi jadvallar uchun ko`rib chiqamiz:

$A_{11}\ A_{12}\ A_{13}\ A_{14}\ A_{15}\ A_{16}\ A_{17}\ A_{18}$	$B_{11}\ B_{12}\ B_{13}\ B_{14}\ B_{15}\ B_{16}\ B_{17}\ B_{18}$
$A_{21}\ A_{22}\ A_{23}\ A_{24}\ A_{25}\ A_{26}\ A_{27}\ A_{28}$	$B_{21}\ B_{22}\ B_{23}\ B_{24}\ B_{25}\ B_{26}\ B_{27}\ B_{28}$
$A_{31}\ A_{32}\ A_{33}\ A_{34}\ A_{35}\ A_{36}\ A_{37}\ A_{38}$	$B_{31}\ B_{32}\ B_{33}\ B_{34}\ B_{35}\ B_{36}\ B_{37}\ B_{38}$
$A_{41}\ A_{42}\ A_{43}\ A_{44}\ A_{45}\ A_{46}\ A_{47}\ A_{48}$	$B_{41}\ B_{42}\ B_{43}\ B_{44}\ B_{45}\ B_{46}\ B_{47}\ B_{48}$

Shifrlash uchun M_1 harfni B jadvaldan, M_2 harfni esa A jadvaldan izlab topamiz, ya`ni:

$M_1=B_{mn}$ va $M_2=A_{ij}$

a. Agar shifrmatn (M_1M_2) juft bo`lakning harflari jadvallarning turli qatorlarida joylashgan bo`lsa, u holda matn (U_1U_2) juft bo`lak quyidagicha olinadi:

$U_1= A_{mj}$, $U_2= B_{in}$

b. Agar shifrmatn (M_1M_2) juft bo`lakning harflari jadvallarning bir qatorida joylashgan bo`lsa, u holda (U_1U_2) juft bo`lak quyidagicha olinadi:

$U_1= A_{mn}$, $U_2= B_{ij}$

Bigrammalarga ajratilgan shifrmatnni Uinston ikkilangan kvadrat usuli bo`yicha har bir juftini jadvaldagi o`rnini topamiz va uni mos harfga almashtiramiz.

AA GW UD LO FO FZ FL GD EB LJ BJ ?I QB JT DS .R JA FP F

Shifrmatn AA o`rni $B_{12}A_{14}$ bo`lsa, matn o`rni $A_{12}B_{14}$ va matn UI bo`ladi.

Shifrmatn GW o`rni $B_{24}A_{37}$ bo`lsa, matn o`rni $A_{27}B_{34}$ va matn NS bo`ladi.

Shifrmatn UD o`rni $B_{36}A_{15}$ bo`lsa, matn o`rni $A_{35}B_{16}$ va matn TO bo`ladi.

Shifrmatn LO o`rni $B_{27}A_{28}$ bo`lsa, matn o`rni $A_{27}B_{28}$ va matn NN bo`ladi.

Shifrmatn FO o`rni $B_{23}A_{28}$ bo`lsa, matn o`rni $A_{23}B_{28}$ va matn IN bo`ladi.

Shifrmatn FZ o`rni $B_{23}A_{42}$ bo`lsa, matn o`rni $A_{22}B_{43}$ va matn G bo`ladi.

Shifrmatn FL o`rni $B_{23}A_{26}$ bo`lsa, matn o`rni $A_{23}B_{26}$ va matn IK bo`ladi.

Shifrmatn GD o`rni $B_{24}A_{15}$ bo`lsa, matn o`rni $A_{25}B_{14}$ va matn KI bo`ladi.

Shifrmatn EB o`rni $B_{22}A_{16}$ bo`lsa, matn o`rni $A_{26}B_{12}$ va matn LA bo`ladi.

Shifrmatn LJ o`rni $B_{27}A_{24}$ bo`lsa, matn o`rni $A_{27}B_{24}$ va matn NG bo`ladi.

Shifrmatn BJ o`rni $B_{18}A_{24}$ bo`lsa, matn o`rni $A_{14}B_{28}$ va matn AN bo`ladi.

Shifrmatn ?I o`rni $B_{46}A_{23}$ bo`lsa, matn o`rni $A_{43}B_{26}$ va matn K bo`ladi.

Shifrmatn QB o`rni $B_{32}A_{16}$ bo`lsa, matn o`rni $A_{36}B_{12}$ va matn VA bo`ladi.

Shifrmatn JT o`rni $B_{13}A_{35}$ bo`lsa, matn o`rni $A_{15}B_{33}$ va matn DR bo`ladi.

Shifrmatn DS o`rni $B_{15}A_{34}$ bo`lsa, matn o`rni $A_{14}B_{35}$ va matn AT bo`ladi.

Shifrmatn .R o`rni $B_{44}A_{33}$ bo`lsa, matn o`rni $A_{43}B_{34}$ va matn  S bo`ladi.

Shifrmatn JA o`rni $B_{13}A_{14}$ bo`lsa, matn o`rni $A_{13}B_{14}$ va matn HI bo`ladi.

Shifrmatn FP o`rni $B_{23}A_{31}$ bo`lsa, matn o`rni $A_{21}B_{33}$ va matn FR bo`ladi.

Shifrmatn F o`rni $B_{23}A_{43}$ bo`lsa, matn o`rni $A_{23}B_{43}$ va matn I  bo`ladi.

Natijada matnni deshifrlab, qo`yidagi matnni olamiz.

Shifrlangan matn: AAGWUDLOFOFZFLGDEBLJBJ?IQBJTDS.RJAFPF

Deshifrlangan matn: UINSTONNING IKKILANGAN KVADRAT SHIFRI

2.5. Uinstonning ‘ikkililagan kvadrat’ shifrini o`rgatish metodikasi

Mavzu	**Uinstonning ‘ikkilangan kvadrat’ shifrini o`rgatish metodikasi**

Axborotli ma`ruzada o`qitish texnologiyasi.

Vaqt – 2 soat	Talabalar soni: 70-80 nafar
O`quv mashg’ulotining shakli	Axborotli ma`ruza
O`qitish texnologiyasi	Uinstonning ‘ikkilangan kvadrat’ shifri to`g’risida yaxlit tasavvur beradi.
*Ma`ruza mashg’ulotining rejasi* (O`quv jarayonining mazmuni)	• Axborotlarni kriptografik usullar orqali himoyalash. • Hozirgi zamon kriptografiyasi. • Kriptoanalitik hujumlar. • An`anaviy simmetrik kriptotizimlar. • Trisemussning shifrlash jadvallari. • Pleyferning bigrammali shifri. • Uinstonning ‘ikkilangan kvadrat’ shifri
*O`quv mashg’ulotining maqsadi:* Kriptografiya va uning vazifasi hamda kriptografik tizimlarni yaratish to`g’risida to`liq tasavvurni shakllantirish, kriptografik tizimlarni yaratish texnologiyasini o`rgatishdan iborat.	
Pedagogik vazifalar: - Axborotlarni kriptografik usullar orqali himoyalash haqida ma`lumot berish. - Hozirgi zamon kriptografiyasi to`g’risida ma`lumot berish. - Kriptoanalitik hujumlar haqida tushunchalar beradi. - An`anaviy simmetrik kriptotizimlar to`g’risida ma`lumot berish. Trisemussning shifrlash jadvallari tushuntiradi. Pleyferning bigrammali shifri haqida tushunchalar beradi. Uinstonning ‘ikkilangan kvadrat’ shifrini bayon qiladi.	*O`quv faoliyati natijalari:* *Talaba:* - Axborotlarni kriptografik usullar orqali himoyalashni tavsiflaydi. - Hozirgi zamon kriptografiyasini tavsiflaydi. - Kriptoanalitik hujumlarni haqida tushunchalarga ega bo`ladi. - An`anaviy simmetrik kriptotizimlarni tahlil qiladi. Trisemussning shifrlash jadvallarini o`rganadi. Pleyferning bigrammali shifri haqida tushunchaga ega bo`ladi. Uinstonning ‘ikkilangan kvadrat’ shifrini o`rganadi.
O`qitish uslubi va texnikasi	Ma`ruza, bayon qilish, klaster.
O`qitish vositalari	Ma`ruzalar matni, proektor, tarqatma materiallar, grafik organayzerlar.
O`qitish shakli	Jamoaviy, frontal
O`qitish shart-sharoiti	Proektor, kompyuter bilan jihozlangan auditoriya.
Monitoring va baholash	Og’zaki nazorat: fokuslangan savollar
Mustaqil ish: - BMI boblari va mavzularini o`rganish.	Talaba: Uinstonning ‘ikkilangan kvadrat’ shifrini o`rganish. Mavzudagi tayanch iboralar mazmunini o`zlashtirish, nazorat savollariga javob tayyorlash.

B.Blum taksonomiyasi asosida o`quv maqsadlarining toifalarini belgilash						
Tayanch iboralar	**O`quv maqsadlari toifalari**					
	Bilish	**Tushunish**	**Qo`llash**	**Analiz**	**Sintez**	**Baholash**
1. Kriptografiya	+	+	+			
2. Kriptografik tizim	+	+		+		
3. Kriptoanalitik hujum	+	+	+			+
4. Kriptobardoshlilik	+	+	+			+

Ishning bosqichlari	Faoliyat mazmuni	
	O`qituvchining	Talabalarning
1-bosqich Kirish (5 minut)	1.1 Mavzu, uning maqsadi, o`quv mashg'ulotidan kutilayotgan natijalar ma`lum qilinadi	1.1.Eshitadi, yozib oladi.
2-bosqich Asosiy (65 - minut)	2.1. Mavzu bo`yicha asosiy savollarga Power Point da tayyorlangan slaytlar asosida izoh berib, namoyish o`tkazadi (5-ilova). Mavzuning har bir bo`limi bo`yicha xulosa qilib, unga talabalarni jalb qilgan holda ularni e`tiborini qaratadi. 2.2. Talabalarga mavzuning asosiy tushunchalariga e`tibor qilishni va yozib olishlarini ta`kidlaydi. 2.3.Quyidagi savollardan foydalangan holda mavzu yoritiladi: - Kriptografiya tushunchalarni sharhlaydi. - Kriptografik tizim deganda nima tushuniladi? - Kriptografik tizim qanday quriladi? - Kriptoanalitik hujum deganda nima tushuniladi? - Kriptobardoshlilik qanday belgilanadi? 2.4. Talabalarga mavzuning asosiy tushunchalariga e`tibor qilishni va yozib olishlarini ta`kidlaydi.	O`UM-ni ko`radilar Eshitadilar, O`UM-ni ko`radilar Tahlil mobaynida matnlarni to`ldiradilar
3-bosqich Yakuniy (10-minut)	3.1. Mavzuga yakun yasaydi va talabalar e`tiborini asosiy masalalarga qaratadi. 3.2. Talabalarning faoliyatini tahlil qiladi va baholaydi. Faol ishtirok etgan talabalarni rag'batlantiradi. 3.3. O`z-o`zini tekshirish bo`yicha savol va topshiriqlar beradi (7-ilova). 3.4. Mustaqil ish uchun vazifa, baholaydi.	Savollar beradilar Javob beradilar va aniqlaydilar O`UM-ni ko`radilar

III. Hayot faoliyati xavfsizligida mehnat tarbiyasi
3.1. Kasb-hunar va ilm-fanni egallash

Inson kasb-hunari bilan ulug'. Kishilik jamiyatining tarixi ham mehnatdan, kasb-hunardan boshlangan. Kasb-hunar avvalam bor tirikchilik manbaidir. Hayot va turmushning qaysi burchagiga kirmang, qadamingiz mehnat bilan qutlug'. Tarbiyani ham mehnatsiz tasavvur qilish mumkin emas. Hatto, u bilimlarni egallamoq va hunar o`rganmoq uchun ham zarur. Insonning sog'lom yurishi uchun uni dangasaliqdan qutqarish foydalidir, zero yalqovlik, ishyoqmaslik odamning buzilishiga, kasalliklarga chalinishiga olib keladi.

Kasb-hunarsiz shon-shavkatga, martabaga erishgan kishi hurmatga loyiqmi degan savol tug'iladi. Bu savolga ham quyidagicha javob berish mumkin: yuqori martabaga ayrim yo`llar bilan kasb-hunarsiz erishgan kishi rohat farog'atda yashayotgandek tuyuladi, ya`ni bunday kishilar yaxshi kiyinadi, qimmatbaho mashina va uy-joylarga ega bo`ladi. Ammo ular ulug'likdan, izzat-hurmatdan mahrumdir.

Kasb-hunarning mamlakatdagi o`rni beqiyos. Hunari bilan insonlar yanada yuksaklikka ko`tarilishadi va buning uchun salohiyatli ilmlarni egallashi lozim bo`ladi. Ilm olish va o`qish eng kerakli mehnatdir.

Kasb-hunarni egallashda dastlabki omil - bu aql bilan bog'liq hodisadir. Agar bola ma`rifatli oiladan bo`lsa, uni ilm-fan bilan mashg'ul qilishga yo`llash kerak, agar hunarmand oilasidan bo`lsa, aksincha, uni albatta kosibchilik qilishga yo`naltirish yaxshi samara beradi. Bunday kasb-hunar egalari jamiyatda yuqori malakada faoliyat ko`rsatadigan soha mutaxassislari hisoblanadi. Uchinchi guruh kasb-hunar kishilarining shijoatlariga bog'liqdir. Masalan: sportchi, chavandozlik va shunga o`xshash insonlardan shijoat talab etiladigan kasblar shular jumlasiga kiradi. Yana bir turdagi shunday kasb-hunar borki, buni qabih va yaramas kasb-hunarlar deb aytishimiz mumkin. Bularga folbinlik, sehrgarlik, afsungarlik, qo`shmachilik va boshqalar kiradi.

Bu hunarlar jamiyatga katta zarar keltirganliklari uchun ular hamma vaqt qoralangan. Lekin bundan qat`iy nazar, jamiyatning har bir a`zosi mehnat qilishi, kasb-hunar egallashi lozim, zeroki, faqat mehnat bilan inson baxt saodat va kamolotga etishuvi mumkin.

Jamiyat va uning farovonligiga foyda keltiradigan har qanday kasb-hunar inson uchun munosibdir. Har bir kishi o`z ishiga halol munosabatda bo`lishi lozimdir. Bu

g’oyalar ifodasini biz ulug’ mutafakkirlarimiz, Navoiy va Jomiy asarlarida ham ko`plab kuzatishimiz mumkin. Ulardagi qahramonlar yoshlikdan yirik olim va ustozlar qo`lida tahsil ko`radilar. Navoiy qahramonlaridan biri bo`lgan Qaysga besh yoshligida otasi tajribali muallim tayinlaydi. U aqlli, dono va bilimdon ustoz yordamida ilm-fanning qonun-qoidalarini, koinot sirlarini o`rganib, o`z davrining bilimdon kishisi bo`lib etishadi. Yoki Farhodni olaylik, u yoshligidan bilim olish bilan shug’ullanib, o`n yoshida fanning ko`p sohalaridan ogoh bo`ladi, kamtarinligi, harakatchanligi, xulq-odobi va boshqa fazilatlari bilan odamlarni hayratga soladi. Demak, ilmu odobga yoshlikdan kirishmoq g’oyasi sharq mutafakkirlarining aksariyat asarlarida keng yoritilganligining guvohi bo`lamiz.

Agar yoshliqda kasb-hunarga yo`naltiruvchi bilim olish imkoniyati bo`lmagan bo`lsa, kishining ulg’ayganida ham ilm bilan shug’ullanishi kech bo`lmaydi, zero bilim egallash hech qachon qoralangan emas.

Bu xususda buyuk alloma Aflotundan so`radilar: ‘O`qish-o`rganish qay vaqtgacha izzat va hurmatda bo`ladi?’ U javob beribdi: ‘Johillik nuqson deb hisoblanguncha’. Shuning uchun jamiyatga nafi tegadigan bilimlarni egallash nihoyatda zarurdir.

Kasb-hunarni o`rganish uchun haqiqiy fanlarni egallash juda katta samara beradi. Shuning uchun ham Aflotun o`z eshigi tepasiga ‘Kimki geometriyani bilmasa, uyimizga kirmasin’-degan so`zlarni yozib qo`ygan ekan.

Ma`lumki, hozirgi vaqtda ijtimoiy hayotning barcha jabhalarida, shu jumladan, ma`naviy hayotda ham chuqur o`zgarishlar sodir bo`lmoqda. O`tgan davrlardan bizning davrimizgacha saqlanib kelayotgan umuminsoniy qadriyatlar yangicha talqin etilmoqda, an`ana va marosimlarimizga yondashilmoqda.

Jamiyatning axloqiy g’oyalari va talablariga javob beradigan o`tmish ahloqiy qadriyatlarini tiklash, ularni kishilar, ayniqsa, o`sib kelayotgan yoshlarning ongiga singdirish muhim ahamiyat kasb etadi. Mutafakkirlarning boy adabiy-axloqiy merosi, o`tmishdan saqlanib kelayotgan xulq odob qoidalari, o`gitlari-yu, pand-nasihatlari hanuzgacha o`zining tarbiyaviy ahamiyatini yo`qotmagan. Demak, kasb-hunar va ilm-fanni egallash to`g’risidagi o`tgan allomalarimizning qimmatli fikrlari -donolik, adolat, shijoatdir.

3.2. Mehnat bandligi va samaradorligi

Mustaqillik yo`lida dadil borayotgan yurtimizda aholini ish bilan ta`minlash va ishsizlikni oldini olish masalalariga alohida e`tibor berilmoqda. Inson qobiliyati, uni ishga solish, natijada o`z ehtiyojlarini qondirish uchun zarur shart-sharoitlar yaratilmoqda. Mamlakatda tashabbuskorlik va tadbirkorlikka keng yo`l ochib berilgan. Bozor iqtisodiyotiga o`tishning 'O`zbek modeli' ko`pgina hamdo`stlik mamlakatlaridagidek ishsizlikning birdaniga oshib ketishiga yo`l qo`ymaydi. Ushbu modelning yana bir ustivor yo`nalishi shundan iboratki, mamlakatimizning jadal rivojlanishida qishloq xo`jaligining mavqeini oshirishni to`g'ri belgilab dehqonlar uchun tomorqa va dehqon fermer xo`jaliklari uchun er berilishi qishloqdagi aholini ish bilan band qilish muammosini deyarli barham toptirdi. Hozirda respublikamiz qishloqlarida yashayotgan har bir xo`jalik yoki oila to`liq tomorqasi uchun er bilan ta`minlanganligining guvohi bo`lamiz. Shuning uchun ham bozorlarimiz qishu yoz meva - sabzavotga to`la.

Iqtisodiyotdagi chuqur tarkibiy o`zgarishlar, kichik va o`rta tadbirkorlikning rivojlanishi, tashqi investitsiya siyosatini to`g'ri olib borilishi aholini ish bilan ta`minlashni yaxshilashga, faolligining o`sishiga asos bo`lmoqda. Aholini ish bilan ta`minlash maqsadida ularni kasbga tayyorlash va qayta o`qitish, aholini ijtimoiy himoyalash va har bir kasbga mehr uyg'otish uchun ularda avvalom bor ma`naviy kamolotni shakllantirish lozim bo`ladi.

Ma`naviyati yuksak inson birovning haqiga; davlat, jamoat mulkiga xiyonat qilmaydi, sadoqatli bo`ladi. Vatan, el-yurt, xalqi uchun jonini fido etishda o`zini ayamaydi. Ma`naviy barkamol, ma`rifatli, yaxshi niyatli, tadbirkor, fozil inson eng oliy faoliyat-mehnat, yaratuvchanlik, bunyodkorlik bilan mashg'ul bo`lishi uchun, uning ishlashi va sharoitini tubdan yaxshilash taraqqiyotimizning ob`ektiv qonuniyati bo`lib qolayotganligi quvonarli holdir.

Kasbiga yuqori darajada mehrli va ma`naviyatli bo`lish avvalom bor avloddan-avlodga o`tib kelayotgan hunarmandchilikni davom ettirgan shaxslarda yaxshi shakllanadi.

Ish bilan bandlik O`zbekistonda iqtisodiyotning nodavlat sektoriga to`g'ri kelishi ta`kidlanib, hozirgi paytda ushbu sohada band bo`lgan ishchi va xizmatchilarning ulushi qariyib 75% ni tashkil qiladi. Aholining soni 1995-2000 yillarda 5,6% oshgan

bir paytda, xususiy korxonalarda ishga joylashganlar soni 60%, hissadorlik jamiyatlarida 30%, qo`shma korxonalarda 10% ko`paydi. Ma`lumotlar ham ko`rsatib turibdiki, O`zbekistonda bozor munosabatlarining shakllanishi jarayoni bevosita nodavlat sektorining o`sishi bilan bogliqdir. Biroq, ta`kidlash joizki, O`zbekistonda kichik va o`rta biznesning ulushi jahon mamlakatlariga nisbatan juda kam. Masalan, Italiyada ish bilan band aholining taxminan 80%i ni, buyuk Britaniya va Yaponiyada 70%i dan ortiqrog'ini, Frantsiya va Olmoniyada taxminan 66 % ni, AQSH da -55% ni kichik va o`rta biznes bilan mashg'ul odamlar tashkil qiladi. O`zbekistonda esa ushbu ko`rsatkich atiga 7% ni tashkil qilishi hali bu borada bizda juda katga imkoniyatlar mavjudligidan dalolat beradi.

Shuni e`tirof etish kerakki, hozirgi sharoitda O`zbekistonda kichik va o`rta biznesni rivojlantirish uchun qonun etarli darajada yaratildi. Bu borada 2000 yil 25 mayda qabul qilingan 'Tadbirkorlik faoliyati erkinligining kafolatlari to`g'risida' gi qonun ayni muddao bo`ldi. Ammo ma`muriy buyruqbozlikdan qolgan juda ko`p asoratlar ularning rivojlanishiga hamon to`sqinlik qilmoqda. Bunga kichik va o`rta biznes faoliyatiga davlatning aralashuvi, turli davlat idoralarining tekshiruv funktsiyasini mustahkam saqlab turishdan manfaatdorligi, bank va soliq sohasida amalga oshirilayotgan islohotlarning ayrim hollarda sust ketayotganligi kabilar sabab bo`lmoqda. Lekin mazkur qonunning amaliyotga to`liq joriy qilinishi juda ko`p to`siqlarning barham berishiga olib keladi.

Ko`rinib turibdiki, O`zbekistonda xususiy tadbirkorlikka asoslangan kichik va o`rta biznesni rivojlantirish uchun ham katta imkoniyatlar mavjud. O`zbekistonning iqtisodiyoti kelajakda kichik va o`rta tadbirkorlikka tayanishi muqarrar. Ularning ulushi barcha sohalarda 50% dan kam bo`lmasligi kerak. Zero, ushbu soha bozor talablariga mos bo`lib tez o`zgarishlarga moslanuvchan bo`ladi. Bu esa bozor munosabatlari sharoitida iqtisodiyotni rivojlantirishning asosiy omillaridan biridir.

Ushbu muammolarni hal etish uchun huquqiy manbalarni yaxshi yo`lga qo`yish lozim. Shundagina tadbirkorlikka keng imkoniyatlar ochiladi. Fan va texnika taraqqiyoti yutuqlaridan aholini ish bilan ko`proq ta`minlash, ular uchun qulay hamda havfsiz mehnat sharoitlarini yaratish, ish vaqtidan unumli foydalanish, og'ir jismoniy va malakasiz ishlarni qisqartirishda katta ahamiyat kasb etadi.

Har bir inson mehnatni majbur bo`lib emas, balki o`z ixtiyori bilan bajarishi lozim. Shundagina mehnat unumli samara beradi. Lekin har kim hamisha o`z ixtiyori bilan samarali mehnat qilavermaydi. Uning uchun insonda eng avvalo shunday mehnat qilishga da`vat etuvchi tuyg'u uyg'otilishi kerak. Bunday tuyg'u turli rag'batlantirish yo`llari bilan amalga oshiriladi.

Rag'batlantirish asosan ikki yo`nalishda ya`ni moddiy va ma`naviy rag'batlantirish orqali olib boriladi. Mehnat qiluvchining moddiy va ma`naviy ehtiyojini qondirish uchun, his-tuyg'ularni uyg'otish yo`li mehnat motivizatsiyasi tushunchasi bilan tushuniladi. Shu boisdan mehnat motivatsiyasining ikkita turi alohida ahamiyat kasb etishini ta`kidlash joiz. Bunga quyidagilar kiradi: birinchidan, his-tuyg'u uyg'otuvchi tadbirlar majmuasi, ikkinchisi esa, aql-idrok bilan qilinadigan ishlardir.

Kishilarning samarali mehnat qilishi uchun ikkalasi ham muhim ahamiyatga ega. Ba`zi tadbirlar borki aql-idrok bilan qilinib kishilarda yaxshi mehnat qilish uchun kuchli his-tuyg'u uyg'otadi.

Masalan, millatparvar, fidoiy, jonkuyar inson uchun yaxshi mehnat qilish his-tuyg'usini uyg'otishga O`zbekistonning mustaqillikka erishganligi juda katta omil bo`lib xizmat qiladi. Yoki ishxonasining ravnaqi uchun ahil bo`lgan mehnat jamoaning bir tan, bir jon bo`lib kechayu kunduz uni yuksaltirish uchun qilingan ishlari kabi hamma-hammasida insonlardagi aql-idrok, his-tuyg'u hamohangdir.

Xodimning mehnat qilishi uchun bir qancha motivlar qatorida mehnatga haq to`lash jarayoni quyidagicha bo`lishi mumkin:

• mehnat haqi shakli va tizimlari, mukofotlar, qo`shimcha to`lovlar, ustamalar, rag'batlantirish tarzidagi to`lovlar jamoa shartnomalarida belgilanishi;

• byudjet hisobidan moliyaviy jihatdan ta`minlanadigan muassasalar va tashkilotlarning xodimlari mehnatiga haq to`lash shartlarining eng kam darajasi qonun hujjatlarida belgilab qo`yilishi;

• tabiiy-iqlim va turmush sharoitlari noqulay bo`lgan joylarda mehnat haqiga mintaqa koeffitsientlari va ustamalar belgilanishi;

• m*ehnatga haq to`lash kafolatlari:*

• ish beruvchi o`zining moliyaviy holatidan qat`i nazar, xodimga bajargan ishi uchun haqni belgilangan mehnat haqi shartlarida ko`rsatilgan muddatlarda to`lashi;

• muayyan davr uchun belgilangan mehnat me`yori va mehnat vazifalarini to`liq bajargan xodimning oylik mehnat haqi qonun hujjatlari bilan belgilab qo`yilgan eng kam mehnat haqi miqdoridan oz bo`lmasligi lozim;

• mehnat haqining eng kam miqdoriga qo`shimcha to`lovlar, ustamalar, rag'batlantirish tarzidagi to`lovlar, me`yoriy ish vaqtidan chetga chiqqan holda bajarilgan ishlar uchun amalga oshirilish;

• bir necha kasbda (lavozimda) va o`rindoshlik asosida ishlaganlik uchun;

• xizmat ko`rsatish doirasi kengayganligi, bajariladigan ishlar hajmi ortganligi, o`zining asosiy ishi bilan bir qatorda ishda vaqtincha bo`lmagan xodimlarning vazifalarini bajarganlik uchun, shuningdek o`rindoshlik asosida ish bajarilganda (xodim o`zining asosiy ishini bajarishidan tashqari asosiy ishidan bo`sh vaqtida mehnat shartnomasi asosida boshqa haq to`lanadigan ishni bajarganda), xodimlarning mehnat haqi miqdori mehnat shartnomasining taraflari o`rtasida kelishuvga binoan amalga oshirilishi;

• haq to`lanadigan kun dam olish kuni yoki bayram kuniga to`g'ri kelib qolsa, mehnat haqi shu kun arafasida to`lanishi.

3.3. Mehnatga oid munosabat va rag'batlantirish

Bugungi kunda davlatimizning ustuvor yo`nalishlaridan biri bu - barkamol bunyodkor avlodni tarbiyalash, kadrlarni to`g'ri tanlash, ularni joy-joyiga qo`yish, xalqimizning turmush darajasini oshirish va boshqa ijobiy ishlarga qaratilgandir. Kelajagi buyuk davlatni qurish, barcha orzu umidlarimizga erishish o`z-o`zidan bo`lmaydi, uning asosida mehnat va yana mehnat yotadi. Bugungi kunda joylarda hamma ham bir xil mehnat qilayapti deb bo`lmaydi. Mehnatga, ishga munosabat har kimda har xil bo`lganligi uchun mehnatga oid munosabat bir necha toifa guruhlarga mansub bo`ladi:

Oliyjanob xodimlar - bilim saviyasi, intizomi mehnatga nisbatan yuqori darajada bo`ladi.

Murakkab xususiyatli xodimlar - ishga vaqtida keladi, vaqtida ketadi, nima desangiz 'labbay' deydi, lekin ishni uddalay olmaydi, uddalashni ham xohlamaydi.

*Tarbiyalash mumkin bo`lgan xodimlar -,* ma`lumoti yaxshi, ammo, qiziqish yo`q, uni ustiga qiziqqon, betgachopar, lekin ayrim kunlari yaxshi kayfiyat bilan ishlab qoladi, shunda ancha ishni uddalay oladi.

*Tashkiliy ishlarga suyagi yo`q kishilar* - chalasavod, mehnatga nisbatan munosabati bir xil emas, o`zgaruvchan, lekin yoqimli tili, odamgarchiligi bor.

Og'ir holat - ishga doimo kechikib keladi, iloji boricha erta ketadi, ko`p javob so`raydi, bahonasi ko`p, tanqid qilsangiz surbetlarcha boshini egib turaveradi. Uning ustiga g'iybatchilik qiladi.

Ishga nisbatan chinoq xodimlar - hammasi yaxshi ammo bu xodim keraksiz ishni qilmaydi, jamoaning ayrim boshqa yumushlari uning uchun yot narsa, shuning uchun bo`lsa kerak, bu toifadagi xodimlarga ortiqcha yuklama rahbariyat tomonidan berilmay qo`yiladi.

*O`tkinchi holat* - xodimning ishga bo`lgan munosabati o`rtacha yoki yaxshi, ammo u muhitni buzishi, mish-mish tarqatish, yomonlash, rahbar yoki alohida xodimlarga nisbatan tuhmat, bo`hton qilish va shunga o`xshash g'ayritabiiy illatlarga juda moyildir.

Ishidagi yutuqlar uchun xodimga nisbatan rag'batlantirish choralari qo`llanilishi mumkin. Rag'batlantirish turlari, ularni qo`llanish tartibi, afzallik va imtiyozlar berish jamoa shartnomalari, ichki mehnat tartib qoidalari va boshqa lokal hujjatlarda, jamoa kelishuvlarida, intizom to`g'risidagi Nizomlarda belgilab qo`yiladi.

Xodimlar mehnat sohasida davlat va jamiyat oldidagi alohida xizmatlari uchun davlat mukofotlariga taqdim etilishi mumkin.

Ish haqi, mukofotlar, qo`shimcha to`lovlar, ustamalar va mehnat haqi tizimida nazarda tutilgan boshqa to`lovlar rag'batlantirish turlariga kirmaydi.

Intizomiy jazo amal qilib turgan muddat mobaynida xodimga nisbatan rag'batlantirish choralari qo`llanilmaydi.

Mehnatning natijasi qancha tez rag'batlantirilib borilsa, u shuncha unumli bo`ladi. Ayniqsa har haftada, ba`zan har kuni maosh to`lanishi evaziga yuqori mehnat unumdorligiga erishadilar. Xo`jalikni yuritishda mehnatning bu motivini inobatga olish yuqori samaradorlikka erishish uchun juda muhimdir.

Tahlil jarayonida mehnat samaradorligi uning ish haqining muddatida to`lanishiga bog'liqligi muhim ahamiyatga ega.

*Mehnat samaradorligiga shahar transportining ta`siri.* - Bu mehnatkash uchun juda katta ahamiyatga ega. Mehnat sharoiti xodimlarni ishga olib kelish, ishlash jarayonini ta`minlash va ishdan uygacha kuzatib qo`yishni o`z ichiga oladi. Hozir

transport xarajatlari qimmat. Xodimlarning ishga borib kelishi uchun oylik maoshining asosiy qismi ketib qoladi. Shu tufayli odamlar ozroq ish haqi bo`lsa ham yashash joyiga yaqinroq joydagi korxonalarda ishlashni hohlaydi. Albatta bu xodimning malakasiga ham, mutaxassisligiga ham to`g'ri kelmasligi mumkin. Lekin u yo`l haqini tejash evaziga ko`proq moddiy manfaatdor. Ammo bundan mehnatkash ham, uzoqroqda joylashgan korxona ham, jamiyat ham katta zarar ko`radi. Shu tufayli har bir korxona o`z xodimini ishlatish bilan birga uni ishga olib kelish va ishdan uyigacha kuzatib qo`yish chorasini ham ko`rishi kerak.

Korxonada yaxshi muhitning yaralishi. - Bu ham mehnat samaradorligini oshirish uchun eng muhim omillardan biridir. Chunki har bir kishi ma`naviy jihatdan mustaqil. U mehnat jamoasida o`z o`rniga, mavqeiga ega bo`lishni xohlaydi. SHu tufayli har bir shaxs o`z o`rnida etarli darajada ob`ektiv ravishda baholanishi lozim. Uning izzat obruyi o`z o`rniga qo`yilishi kerak. Korxonaning umumiy mavaffaqiyati uchun shu korxonada ishlayotgan birorta kishi o`zini ortiqcha yoki jamoadan chetda his qilmasligi kerak. Jamoadan hammaning, ya`ni farroshdan tortib to boshliqqa qadar o`z o`rni bor. Hamma o`z o`rnida qilgan mehnati natijasiga qarab munosib baholanishi lozim.

Rejali iqtisodiyotda amal qilgan juda ko`p ma`muriy buyruqbozlik usullari bozor iqtisodiyoti uchun yot unsurlardir. Kishilar tazyiq bilan, majbur bo`lib ishlamasligi kerak. Ularda ishlash uchun ichki tuyg'ular, imkoniyatlar ishga tushib mehnat qilish ixtiyoriy ehtiyojga aylanishi lozim. Bunga o`z-o`zidan erishib qolinmaydi, balki insonga juda katta e`tibor berish bilan erishishi mumkin. Bu holat ko`p holda ortiqcha kapital talab qilmasa-da, lekin ko`p samara, naf keltirishi mumkin bo`lgan tadbirdir.

Boshliqning ovozi ko`tarilgan joyda ishning samarasi pasayishi, uning ovozi muloyim bo`lgan joyda ish jadallashishi mumkin. Muloyimlik yaxshi rag'batlantiruvchi tadbirlar bilan amalga oshirilishi lozim. Har bir mehnat qilayotgan kishi eng avvalo o`zi uchun, o`z manfaati uchun mehnat qilayotganligini his qilishi kerak. Shundagina uning mehnati ehtiyojga aylanadi. Mehnatkash rejaning boshqarilishi uchun yoki rahbarning obro`sining ortishi uchun ishlayotganligini his qilib ishlasa, birov uchun ishlayotgandek bo`ladi.

Har bir kishining o`z o`rniga ega bo`lishini ta`minlash.- Bu borada ma`naviy-ruhiy muhitning yaratilishi alohida ahamiyatga ega. Chunki bu omillar bir-biri bilan

uzviy bog’liqdir. Har bir kishiga o`zining mehnati bilan jamoaning umumiy muvaffaqiyatiga ozmi-ko`pmi hissa qo`shadi. Shu jihatdan u o`zi ishlayotgan mehnat jamoasida o`z o`rnim bor, deb his qiladi. Odamlarda shakllangan shu tuyg’uni poymol qilmaslik kerak. Shuningdek, u jamoaning muvaffaqiyati bevosita unga bog’liq ekanligini va o`zining jamiyatga, jamoaga kerakligini his qiladi. Bunday his-tuyg’u bilan bog’liq mehnat motivatsiyasi uning samarali, unumli ishlashi uchun asos bo`ladi. Har bir kishida shu korxonaning egasi, xo`jayini va uning bu erda zarur ekanligini his qilishni ta`minlash kerak. Ishlaganiga qarab, ya`ni ish natijasining hajmiga qarab ish haqini oshirib borish, yil oxirida olingan foydaning bir qismini dividend tariqasida bo`lib berish orqali erishiladi. Bu tuyg’u har bir xizmatchida shu xo`jalik mulkini saqlashga, tejamli bo`lishga, yilni ko`proq foyda bilan yakunlashga da`vat etadi. Shuningdek, har bir kishi samarali mehnat qilishga harakat qiladi.

Shunday qilib xodimning mehnat motivatsiyasi shakli, turlari va omillari juda ko`p ekanligiga amin bo`lamiz. Uning juda ko`p omillari borki ularning sonini aniq vaziyatdan kelib chiqib ko`paytirish yoki kamaytirish mumkin.

XULOSA

Jahon kompyuter tarmog’i axborotlarni yig’ish, saqlash, qayta ishlash va axborot almashuvi tezligini keskin oshirdi hamda davlat boshqaruvini tubdan o`zgartirmoqda. Axborotlar dunyosiga sayohat qilishda davlat chegaralari degan tushuncha yo`qolib, globallashgan axborotlashgan jamiyat tezlik bilan shakllanib bormoqda. Mavjud axborot resurslarini boshqara olish, ularning xavfsizligini ta`minlash va undan samarali foydalanish mamlakat xavfsizligini hamda demokratik axborotlashgan jamiyatni muvaffaqiyatli shakllantirishni ta`minlaydi. Mavjud axborotlarga noqonuniy kirilishi, ularni o`g’irlanishi, yo`qotilishi, buzib ko`rsatilishi va uni o`zgartirilishi singari muammolarga yo`l qo`yilishi shaxs, jamiyat va davlatning axborot xavfsizligi darajasining pasayishiga olib keladi. Shu sababli axborot xavfsizligini ta`minlash muammosi davlat milliy xavfsizligini ta`minlashning asosiy va ajralmas qismi bo`lib qolmoqda hamda u eng muhim dolzarb masala hisoblanadi.

Axborot xavfsizligini ta`minlashning usullaridan biri kriptografik usullardir. Bu usullarni qo`llash orqali ma`lumotlar ishonchli himoyalanadi. Barchamiz kriptografik usullar haqida etarlicha ma`lumotga ega bo`lishimiz lozim. Shuning uchun, ushbu ‘Uinstonning ‘ikkilangan kvadrat’ shifri tahlili va uni dasturini yaratish’ mavzusidagi bitiruv malakaviy ishida ta`lim jarayoni uchun axborot xavfsizligi muammosini yorituvchi ma`lumotlar berildi va dasturiy mahsulot yaratildi.

FOYDALANILGAN ADABIYOTLAR

1. I.Karimov O`zbekiston XXI – asr bo`sag'asida: xavfsizlikka tahdid, barqarorlik shartlari va taraqiyot kafolatlari. Toshkent. 1997 y.
2. Брюс Шнайер. Секреты и ложь. Безопасность данных в цифровом мире. Триумф-2002.
3. Майкл Ховард, Девид Лебланк. Защищенный код. Москва 2004.
4. Д. Скляров. Искусство, защиты и взлома информации. Санкт-Петербург. БХВ-Петербург. 2004.
5. Роберт Чёрчхаус. Коды и шифры. Москва 2006.
6. В. В. Ященко. Введения в криптография. Москва 2006.
7. Ж. Брассар. Современная криптология. Москва 2006.
8. В. Громов, Г.А. Васильев Энциклопедия компютерной безопасносты. Москва 2007.
9. Баричев С., Гончаров В.В., Серов Р.Е. Основы современной криптологии. Москва. Горячая линия. Телесом 2001 г/
10. Ғаниев С.К., Каримов М.М. Ҳисоблаш тизимлари ва тармоқларида информация ҳимояси: Олий ўқув юрт. талаб. учун ўқув қўлланма. - Тошкент давлат техника университети, 2003. 77б.
11. Шеннон К. Работы по теории информации и кибернетики / Пер. с англ. – М.: Иностранная литература, 1963. – 829с.
12. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии.–М.: Гелиус АРВ, 2001.– 480 с.
13. Кан Д. Взломщики кодов. –М.: Издательство "Центрполиграф", 2000. – 473 с.
14. Завгородний В.И. Комплексная защита информации в компютерных системах. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.
15. Нильс Фергюсон, Брюс Шнайер «Практическая криптография», М.: Издательский дом «Вильямс», 2005г.-424с.
16. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», М.: ДМК, 2000г. -448с.

17. Коблиц Н. Курс теории чисел в криптографии. – М., Научное издательство ТВП, 2001й.

18. Масленников А. Практическая криптография BHV – СПб 2003й.

19. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф-2002й.

20. A. Ismoilov, Q. Usmonov. Hayot faoliyati xavfsizligi. O`quv qo`llanma. Samarqand – 2010

21. O.Qudratov, T. G'aniev. Hayotiy faoliyat xavfsizligi. Toshkent, 2004 y.

22. X.Rahimova va boshqalar. Mehnatni muhofaza qilish. Toshkent, 2004 y.

23. M.A.Qudratov va boshqalar. Hayotiy faoliyat xavfsizligi (ma'ruza kursi). Toshkent, 2005y.

24. ftp://ftp.kiae.su/msdos/crypto/pgp

25. http://drago.centerline.com:8080/franl/pgp/…

26. Yahoo - Computers, Security-and-Encryption

27. http://gov.uz

Matnni Uinstonning ikkilangan kvadrat usulida shifrlash va deshifrlash dasturi matni

```
uses crt;
  Const d=40;
  Const S:array[1..d] of char=('A','B','C','D','E','F','G','H','I','J','K',
                               'L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z',
                               ' ',',','.',';','?','!','=','+','-',':',';','"','(',')','%');
  var
   i,j,qator,ustun,bigson: byte;
   Text,suz,suz1,suz2: string;
   J1,J2: array[1..50,1..50] of char;
   Bigram: array[1..200] of string;
   qator1,ustun1,qator2,ustun2: byte;
   c:char;
 {== Tresimuss jadvali ulchovini tanlash =====}
 procedure Jadval;
  var i:byte;
   begin
    repeat
     write('Jadval qatori sonini kiriting: '); readln(qator);
     write('Jadval ustuni sonini kiriting: '); readln(ustun);
     i:= qator*ustun;
     if i<d+5 then
      begin
       writeln;
       writeln('Sizning jadvalingiz yacheykalari soni ',qator*ustun,' ta.');
       writeln('Jadval yacheykalari soni eng kamida ',d,' ta bolishi kerak.');
      end;
     if i>d+15 then
      begin
       writeln;
       writeln('Sizning jadvalingiz yacheykalari soni ',qator*ustun,' ta.');
       writeln('Jadval yacheykalari soni ',d+1,' tadan oshmasligi kerak.');
      end;
     writeln;
    until (i>=(d)) and (i<=(d+1));
 end;
 {=== Matnni bosh harflar bilan yozish ======}
 function BoshHarf(Matn: string): string;
  var
    i: integer;
    tmps:string;
    xarf:char;
 begin
   tmps:='';
   for i:=1 to length(Matn) do
    begin
      xarf:=chr(ord(Matn[i]));
      tmps:=tmps+upcase(xarf);
    end;
   BoshHarf:= tmps;
 end;
 {=== Matnda harflarni takrorlamaslik ======}
 function UnikalHarf(Matn: string): string;
  var
```

```
   i,j,k: byte;
   tmps:string;
   suz:array[1..200] of char;
 begin
  for i:=1 to length(Matn) do suz[i]:=chr(ord(Matn[i]));
  tmps:=suz[1];
  for i:=2 to length(Matn) do
    begin
     j:=1; k:=0;
     repeat
       if suz[i]=suz[j] then begin j:=i; k:=1; end;
       j:=j+1;
     until j>=i;
     if k=0 then tmps:=tmps+suz[i];
    end;
  UnikalHarf:= tmps;
 end;
{=== Jadval harflarni takrorlamaslik ======}
function JadvalHarf(Matn: string): string;
 var
   i,j,k: byte;
   tmps:string;
   suz:array[1..200] of char;
 begin
  tmps:='';
  for i:=1 to D do tmps:=tmps+S[i];
  tmps:=matn+tmps;
  Matn:=tmps;
  {writeln(Matn);}
  for i:=1 to length(Matn) do suz[i]:=chr(ord(Matn[i]));
  tmps:=suz[1];
  for i:=2 to length(Matn) do
    begin
     j:=1; k:=0;
     repeat
       if suz[i]=suz[j] then begin j:=i; k:=1; end;
       j:=j+1;
     until j>=i;
     if k=0 then tmps:=tmps+suz[i];
    end;
  JadvalHarf:= tmps;
 end;
{== Tresimuss jadvali takrorlanmas harflari ======}
procedure TresimussHarf(qator, ustun: byte; Matn: string);
 var
   i,j,k: byte;
   tmps:string;
 begin
   k:=1;
   for i:=1 to qator do
     for j:=1 to ustun do
       begin
        if k<=length(Matn)then J2[i,j]:=chr(ord(Matn[k]))
        else J2[i,j]:=' ';
        k:=k+1;
       end;
```

```
 end;
{== Matnni bigrammalarga ajratish ======}
procedure BigramHarf(Matn: string);
 var
   i,k: byte;
 begin
   writeln('Bigrammalarga ajratilgan matn:');
   if (Length(Matn) mod 2)<>0 then Matn:=Matn+' ';
   j:=length(Matn)+1;
   i:=0; k:=1;
   repeat
     i:=i+1;
     Bigram[i]:=copy(Matn,k,2);
     write(Bigram[i],' ');
     k:=k+2;
   until k>=j;
   if length(Bigram[i])=1 then Bigram[i]:=Bigram[i]+' ';
   bigson:=i;
 end;
{=== Matn bigrammani jadvallardagi urni ======}
 procedure MatnBigramKoor(Juft: string);
 var
   a,b:string;
   i,j: byte;
 begin
   a:=copy(Juft,1,1);
   b:=copy(Juft,2,1);
   i:=0;j:=0;
   repeat
    i:=i+1;
    repeat
     j:=j+1;
     if j>ustun then j:=1;
    until (J1[i,j]=a) or (j=ustun);
   until (J1[i,j]=a) or (i=qator);
   qator1:=i;
   ustun1:=j;
   i:=0;j:=0;
   repeat
    i:=i+1;
    repeat
     j:=j+1;
     if j>ustun then j:=1;
    until (J2[i,j]=b) or (j=ustun);
   until (J2[i,j]=b) or (i=qator);
   qator2:=i;
   ustun2:=j;
   write(a,'(',qator1,',',ustun1,')');
   write(b,'(',qator2,',',ustun2,')',  ');
 end;
{=== Shifr bigrammani jadvallardagi urni ======}
 procedure ShifrBigramKoor(Juft: string);
 var
   a,b:string;
   i,j: byte;
 begin
```

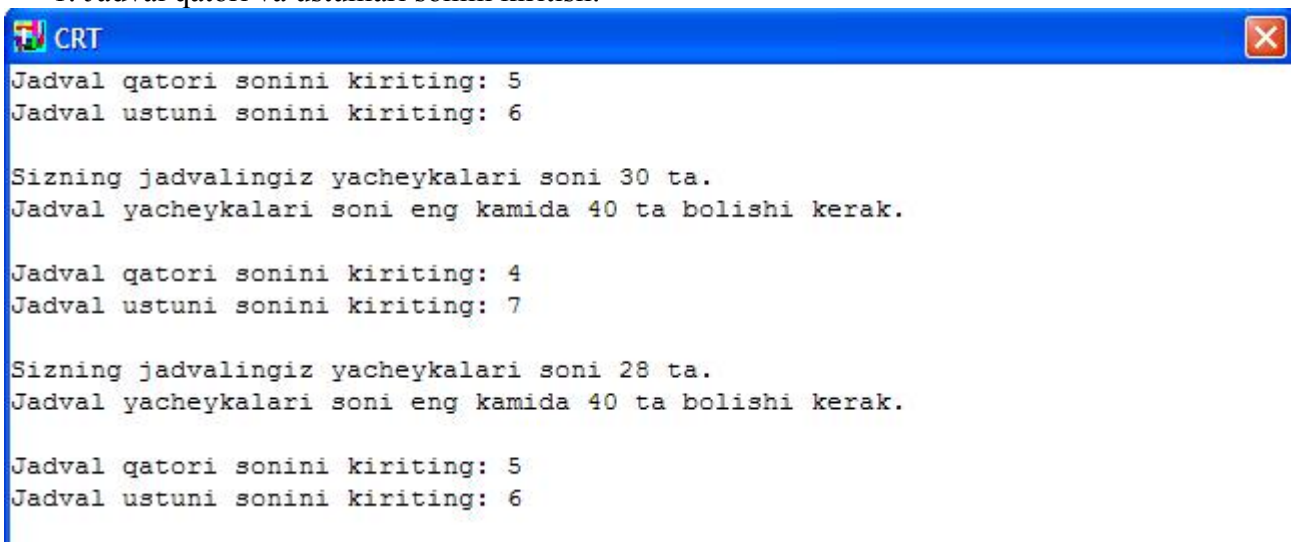
```
   a:=copy(Juft,1,1);
   b:=copy(Juft,2,1);
   i:=0;j:=0;
   repeat
    i:=i+1;
    repeat
     j:=j+1;
     if j>ustun then j:=1;
    until (J2[i,j]=a) or (j=ustun);
   until (J2[i,j]=a) or (i=qator);
   qator2:=i;
   ustun2:=j;
   i:=0;j:=0;
   repeat
    i:=i+1;
    repeat
     j:=j+1;
     if j>ustun then j:=1;
    until (J1[i,j]=b) or (j=ustun);
   until (J1[i,j]=b) or (i=qator);
   qator1:=i;
   ustun1:=j;
   write(a,'(',qator2,',',ustun2,')');
   write(b,'(',qator1,',',ustun1,'),  ');
  end;
{++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++}
BEGIN
 clrscr;
 Jadval;
 clrscr;
 writeln; write('Birinchi jadval kalit suzini kiriting: '); readln(suz1);
 writeln; write('Ikkinnchi jadval kalit suzini kiriting: '); readln(suz2);
{==== Birinchi Tresimuss jadvalini yaratish ==========}
 suz:=suz1;
 suz:=BoshHarf(suz);
 suz:=UnikalHarf(suz);
 suz:=JadvalHarf(suz);
 TresimussHarf(qator,ustun,suz);
 for i:=1 to qator do
   for j:=1 to ustun do J1[i,j]:=J2[i,j];
{==== Ikkinchi Tresimuss jadvalini yaratish ==========}
 suz:=suz2;
 suz:=BoshHarf(suz);
 suz:=UnikalHarf(suz);
 suz:=JadvalHarf(suz);
 TresimussHarf(qator,ustun,suz);
{======= Yaratilgan Tresimuss jadvallari =======}
 clrscr;
 writeln('UINSTONNING IKKILANGAN KVADRAT USULIDA SHIFRLASH.');
 writeln(' Jadvalning ustunlari soni = ',ustun,' ta, qatorlari soni = ',qator,' ta');
 {writeln;}
 write('Birinchi jadval kalit suzi ( ',suz1);
 write(' ) va jadvalga joylashtirilgan harflar:');
 for i:=1 to qator do
  begin
   writeln;
```

```
        for j:=1 to ustun do write(J1[i,j],' ');
       end;
      writeln;
      write('Ikkinchi jadval kalit suzi (',suz2);
      write(' ) va jadvalga joylashtirilgan harflar:');
      for i:=1 to qator do
       begin
        writeln;
        for j:=1 to ustun do write(J2[i,j],' ');
       end;
     {======= Shifrlash =======}
      writeln;
      writeln('Shifrlanadigan matnni kiriting:'); readln(Text);
      {writeln('UINSTONNING IKKILANGAN KVADRAT USULIDA MATNNI
SHIFRLASH.');}
      Text:=BoshHarf(Text);
      BigramHarf(Text);
      writeln;writeln('Bigramma harflarining jadvallardagi urni');
      Text:='';
      for i:=1 to bigson do
       begin
        MatnBigramKoor(Bigram[i]);
        if qator1<>qator2 then Text:=Text+J2[qator1,ustun2]+J1[qator2,ustun1];
        if qator1=qator2 then Text:=Text+J2[qator1,ustun1]+J1[qator2,ustun2];
       end;
       writeln;
       writeln('Shifrlangan matn:');
       writeln(Text);
       readln(c);
     {======= Yaratilgan Tresimuss jadvallari =======}
      clrscr;
      writeln('UINSTONNING IKKILANGAN KVADRAT USULIDA DESHIFRLASH.');
      writeln(' Jadvalning ustunlari soni = ',ustun,' ta, qatorlari soni = ',qator,' ta');
      {writeln;}
      write('Birinchi jadval kalit suzi ( ',suz1);
      write(' ) va jadvalga joylashtirilgan harflar:');
      for i:=1 to qator do
       begin
        writeln;
        for j:=1 to ustun do write(J1[i,j],' ');
       end;
      writeln;
      write('Ikkinchi jadval kalit suzi (',suz2);
      write(' ) va jadvalga joylashtirilgan harflar:');
      for i:=1 to qator do
       begin
        writeln;
        for j:=1 to ustun do write(J2[i,j],' ');
       end;
     {======= DeShifrlash =======}
      writeln;
      writeln('Shifrlangan matn:');
      writeln(Text);
      {writeln('UINSTONNING IKKILANGAN KVADRAT USULIDA MATNNI
DESHIFRLASH.');}
      Text:=BoshHarf(Text);
```

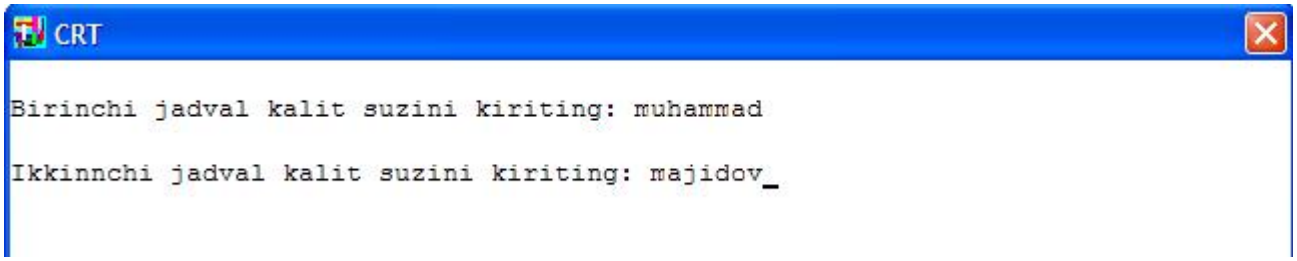
```
 BigramHarf(Text);
 writeln;writeln('Bigramma harflarining jadvallardagi urni');
 Text:='';
 for i:=1 to bigson do
  begin
   ShifrBigramKoor(Bigram[i]);
   if qator1<>qator2 then Text:=Text+J1[qator2,ustun1]+J2[qator1,ustun2];
   if qator1=qator2 then Text:=Text+J1[qator2,ustun2]+J2[qator1,ustun1];
  end;
  writeln;
  writeln('Deshifrlangan matn:');
  writeln(Text);
  readln(c);
END.
```

Matnni Uinstonning ikkilangan kvadrat usulida shifrlash dasturi oyna ko`rinishi

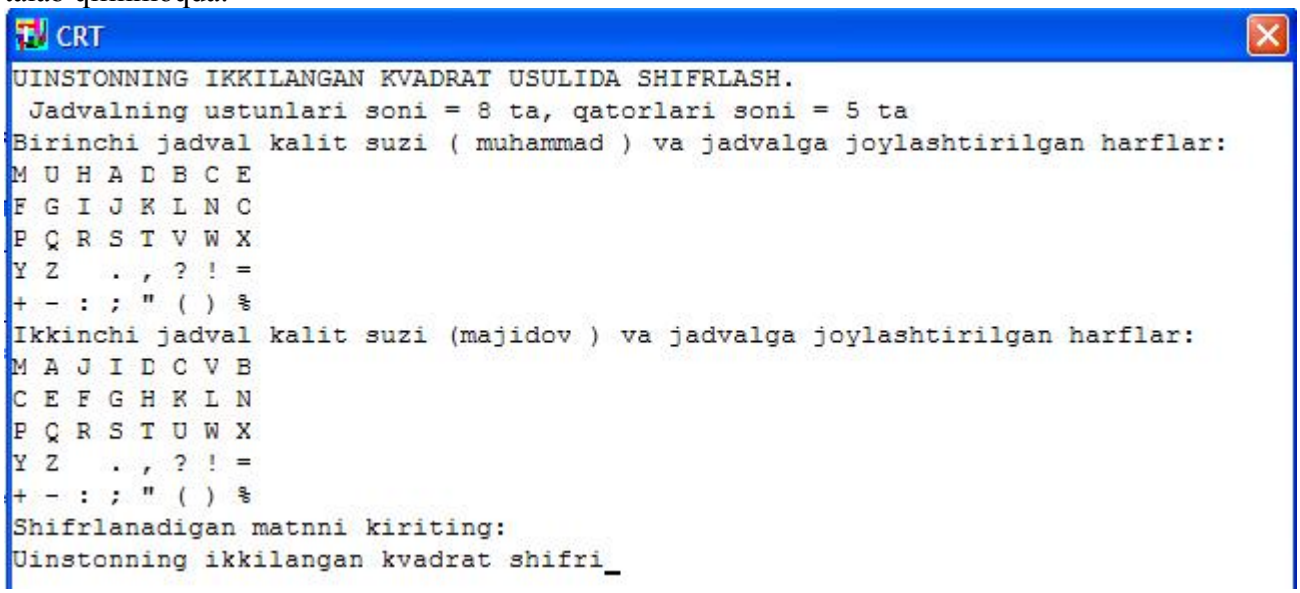
1. Jadval qatori va ustunlari sonini kiritish:



2. Jadvallar kalit so`zlarini kiritish:

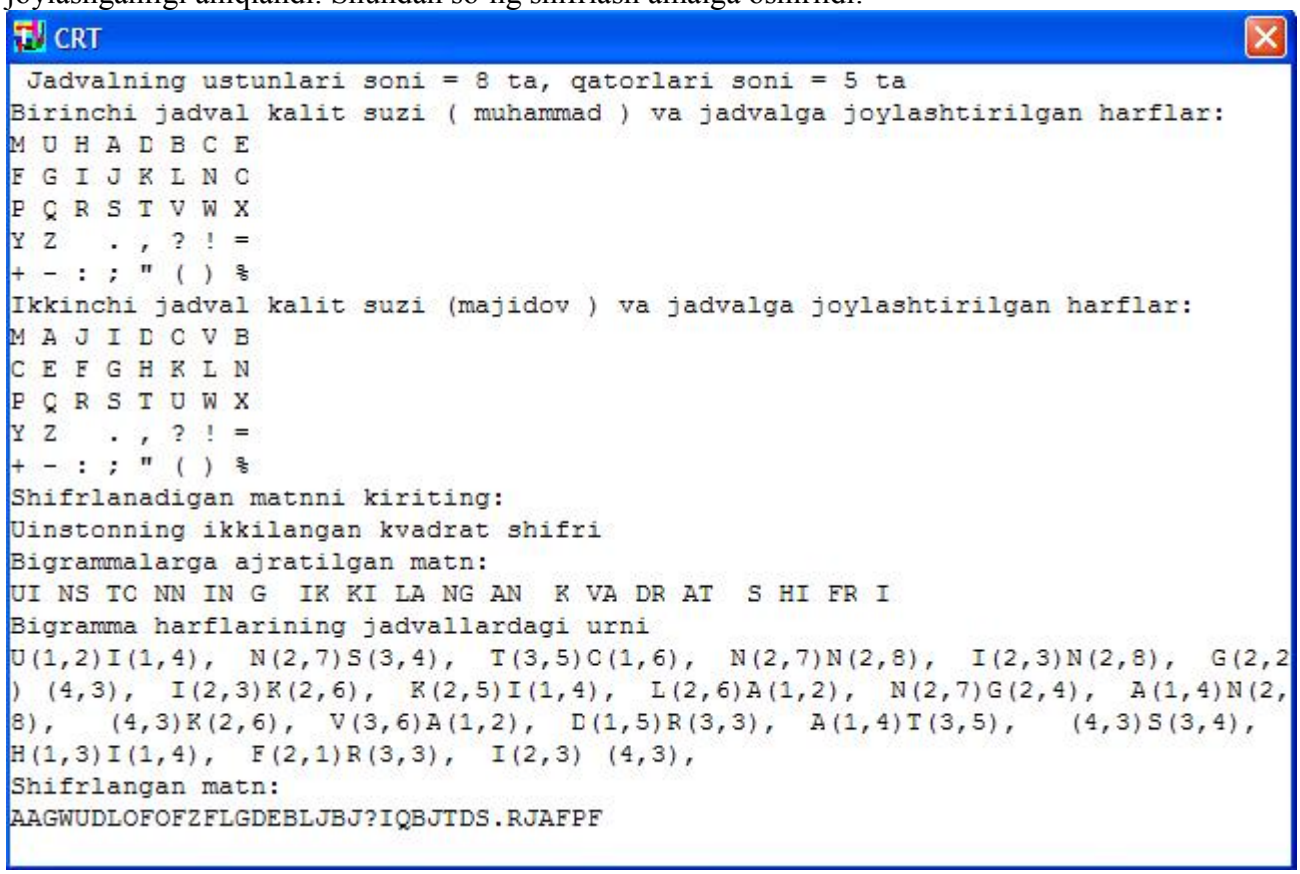


3. Jadvallar yaratildi va unga takrorlanmas harflarga ega bo`lgan kalit so`z harflari va alfavitning kalit so`zda mavjud bo`lmagan harflari joylashtirildi. endi shifrlanadigan matnni kiritish talab qilinmoqda:



Shifrlanadigan matn: Uinstonning ikkilangan kvadrat shifri

4. Shifrlanadigan matn bigrammalarga ajratildi va har bir juftlikning birinchi harfi birinchi jadvalning qaysi yacheykasida, ikkinchi harfi esa ikkinchi jadvalning qaysi yacheykasida joylashganligi aniqlandi. Shundan so`ng shifrlash amalga oshirildi.

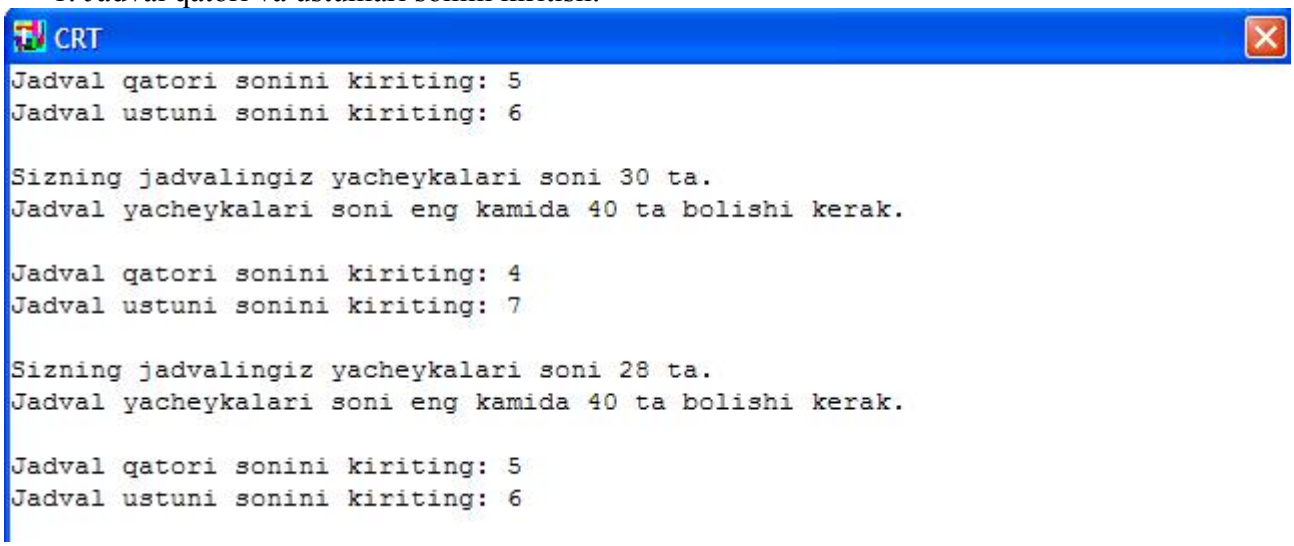


Shifrlanadigan matn: UINSTONNING IKKILANGAN KVADRAT SHIFRI

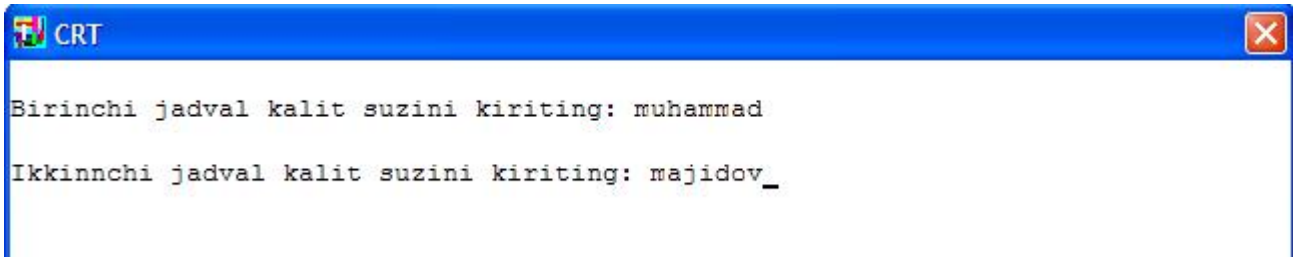
Shifrlangan matn: AAGWUDLOFOFZFLGDEBLJBJ?IQBJTDS.RJAFPF

Shifrmatnni Uinstonning ikkilangan kvadrat usulida deshifrlash dasturi oyna ko`rinishi

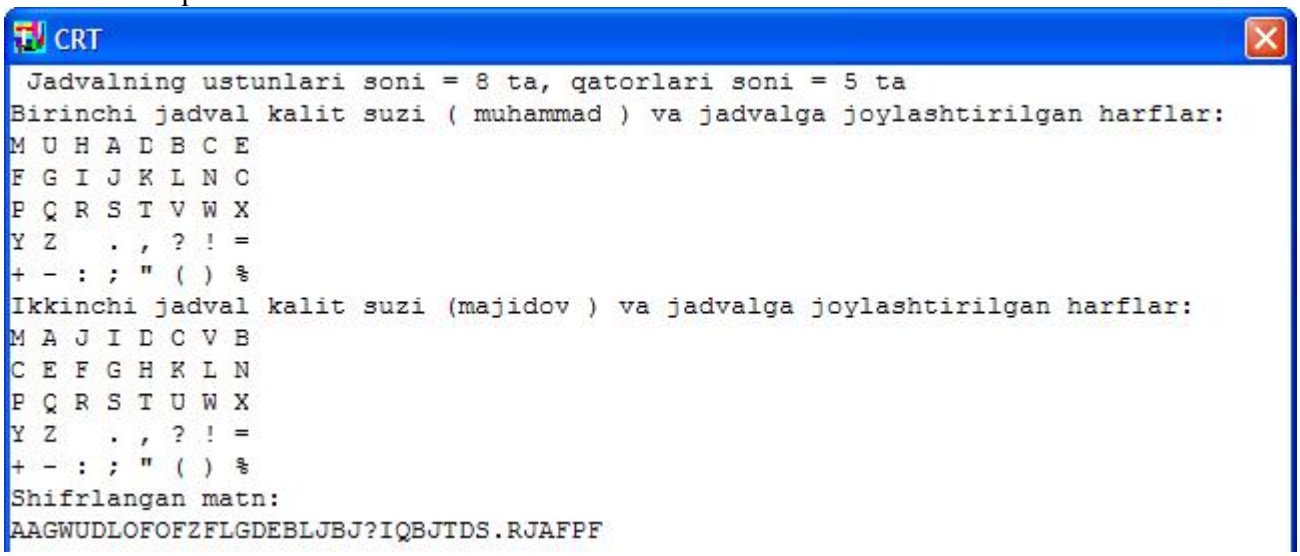
1. Jadval qatori va ustunlari sonini kiritish:



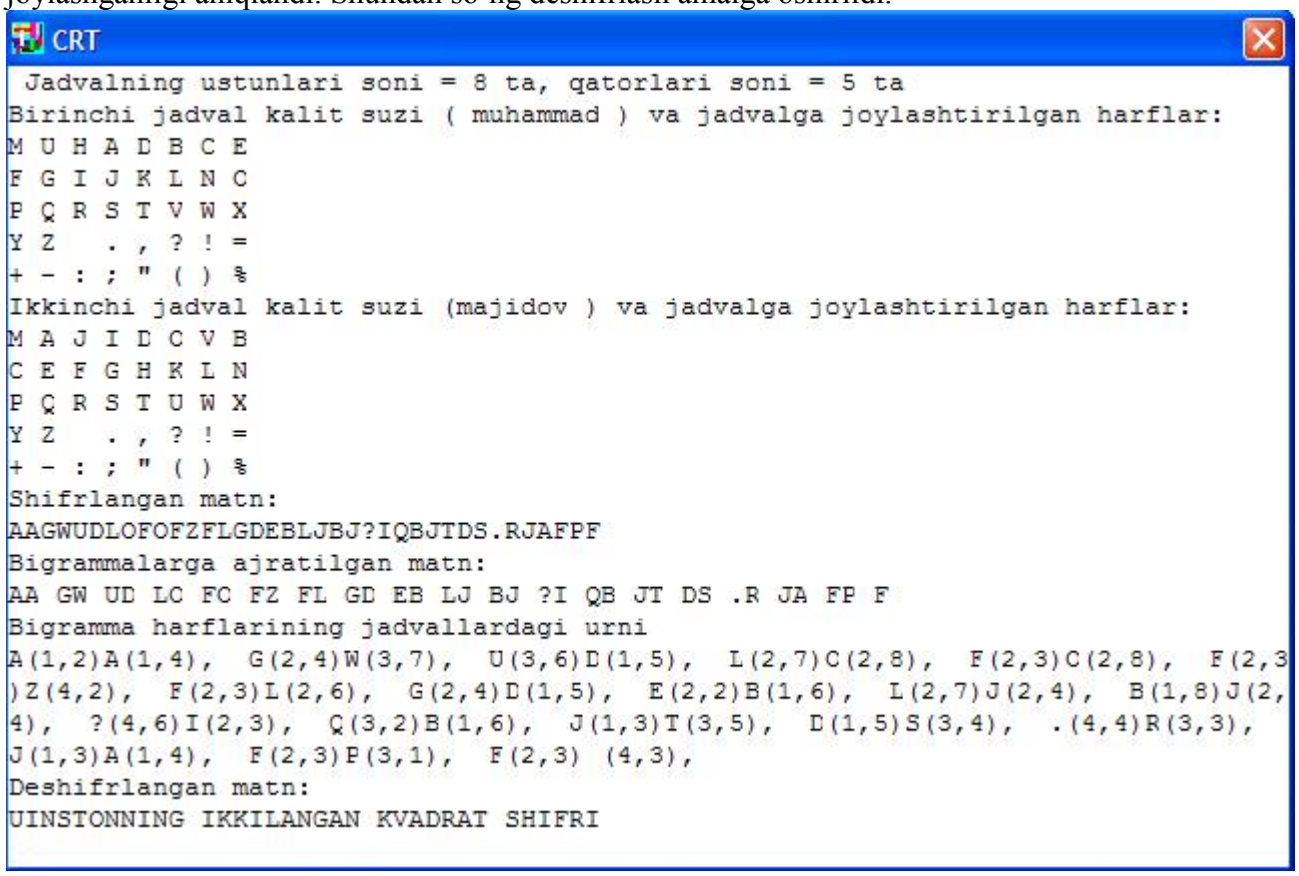
2. Jadvallar kalit so`zlarini kiritish:



3. Jadvallar yaratildi va unga takrorlanmas harflarga ega bo`lgan kalit so`z harflari va alfavitning kalit so`zda mavjud bo`lmagan harflari joylashtirildi. Keyin deshifrlanadigan matnni kiritish talab qilinadi va u ham kiritiladi.



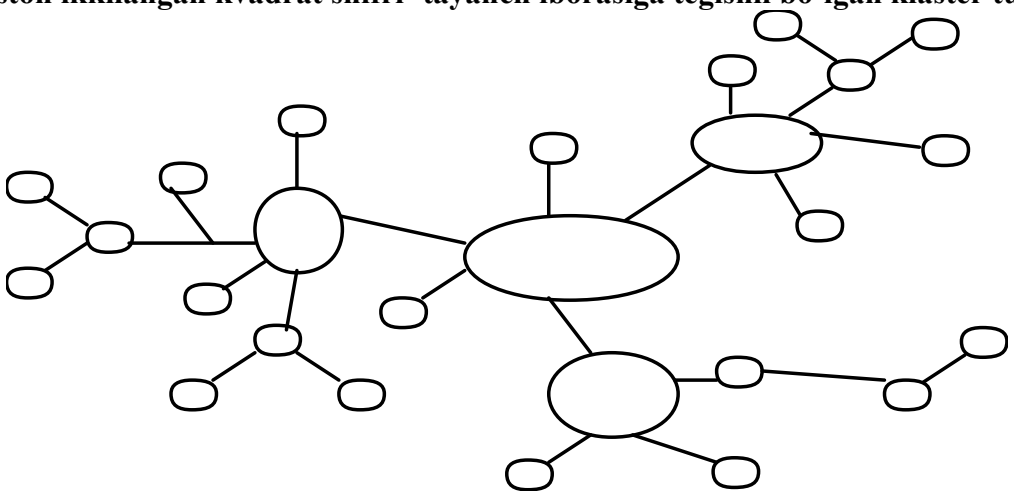
4. Deshifrlanadigan matn bigrammalarga ajratildi va har bir juftlikning birinchi harfi ikkinchi jadvalning kaysi yacheykasida, ikkinchi harfi esa birinchi jadvalning qaysi yacheykasida joylashganligi aniqlandi. Shundan so`ng deshifrlash amalga oshirildi.



Shifrlangan matn: AAGWUDLOFOFZFLGDEBLJBJ?IQBJTDS.RJAFPF
Deshifrlangan matn: UINSTONNING IKKILANGAN KVADRAT SHIFRI

Ilova 4

‘Uinston ikkilangan kvadrat shifri’ tayanch iborasiga tegishli bo`lgan klaster tuzing



Ilova 5

Guruhda ishlash tartibi

- har kim o`z o`rtoqlari nutqini xushmuomalalik bilan tinglashi zarur;
- har kim faol, birgalikda ishlashi, berilgan topshiriqqa mas`uliyatli yondashishi zarur;
- har kim yordamga muxtoj bo`lganda uni so`rashi zarur;
- har kimdan yordam so`ralsa, yordam qilishi zarur;
- har kim guruh ishi natijalarini baholashda ishtirok etishi zarur.

Guruhlar ishida tarqoqsizlikni oldini olish yo`llari:

- Guruhlar ishini har doim boshqarib turish kerak: mavzudan chetga chiqish ta`lim oluvchilar uchun yo`ldan chiqish.
- Guruh sardorlariga e`tibor berish kerak.
- Ishni bajarish uchun zarur bo`lgan, barcha materiallar tushunarli bo`lganligiga ishonch hosil qilish.

Ilova 6

MA`RUZANING O`QUV-VIZUAL MATERIALLARI

Kriptografiya - axborotlarni aslidan o`zgartirilgan holatga o`tkazishlarning matematik uslublarini topish va takomillashtirish bilan shug’ullanadi.

Hozirgi zamon kriptografiyasi

- Simmetrik (yopiq kalitli) kriptotizimlar
- Asimmetrik (ochiq kalitli) kriptotizimlar
- Elektron imzo tizimlari
- Kriptotizimlarda kalitlardan foydalanish

Kriptografik uslublardan foydalanishning asosiy yo`nalishlari

- maxfiy ma`lumotlarni aloqa kanali (masalan, elektron pochta) bo`yicha uzatish
- uzatilgan ma`lumotlarning haqiqiyligini ta`minlash
- axborotlarni (hujjatlarni) kompyuterlar tizimi xotiralarida shifrlangan holda saqlash

Kriptografik uslublar axborotlar matnini asli holidan o`zgartirib, faqat kalitni bilgan holdagina uni asli holatini olish imkoniyatini beradi.

Axborotlar matnini asli holidan o`zgartirishga shifrlash, shifrlangan axborotni asli holiga keltirishga esa deshifrlash deyiladi.

Shifrlash – ochiq matn deb ataluvchi dastlabki matnni shifrlangan matn holatiga o`tkazish jarayonidir.

Deshifrlash – shifrlashga teskari bo`lgan jarayon, ya`ni kalit yordamida shifrlangan matnni dastlabki matn holatiga o`tkazishdir.

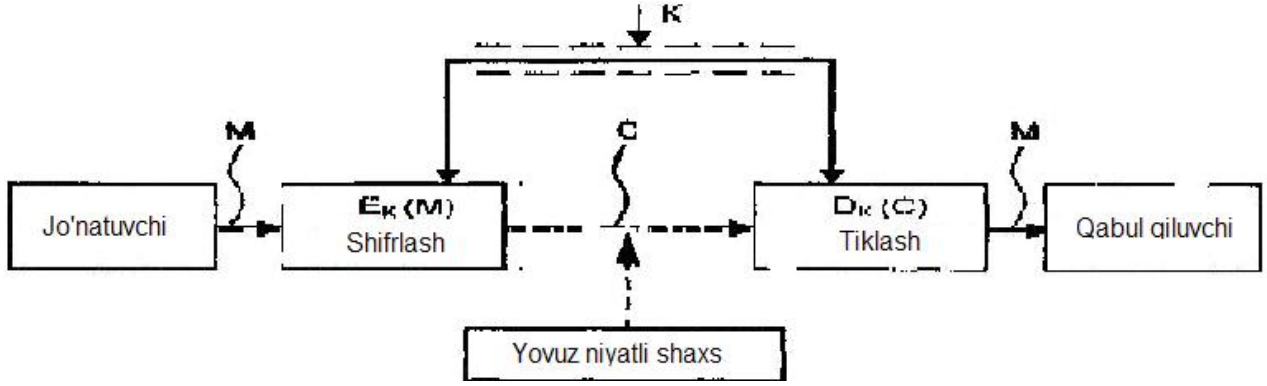
Kalit – bevosita dastlabki matnni shifrlash va deshifrlash uchun zarur bo`lgan ma`lumotdir.

Kriptoanaliz yoki kriptotahlil esa shifrlash uslubini (kalitini yoki algoritmini) bilmagan holda shifrlangan matnning asli holatini topish uslublari masalalari bilan shug'ullanadi.

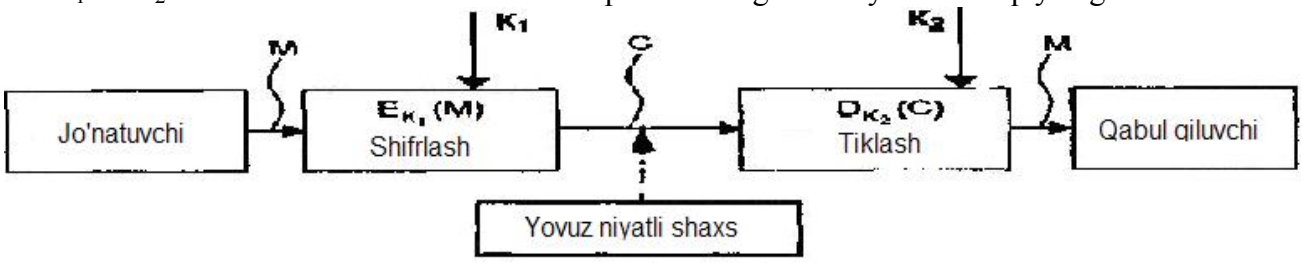
Kriptografik tizim yoki kriptotizim – ochiq matnni shifrlash (deshifrlash) jarayonini tashkil etuvchi amallar majmui bo`lib, matn belgilarini biror bir usulda almashtirishlar ketma-ketligidan iborat.

Kriptochidamlilik yoki kriptomustahkamlik - kriptotahlil orqali shifrlangan matnning asli holatini topishning qiyinlik darajasi.

Uzatiladigan axborotni kriptografik tizim orqali himoyalashning umumiy sxemasi

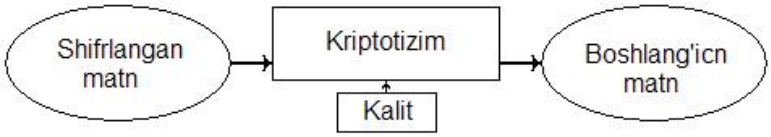


K_1 va K_2 ikki har xil kalitli assimmetrik kriptotizimning umumiy sxemasi quyidagicha.

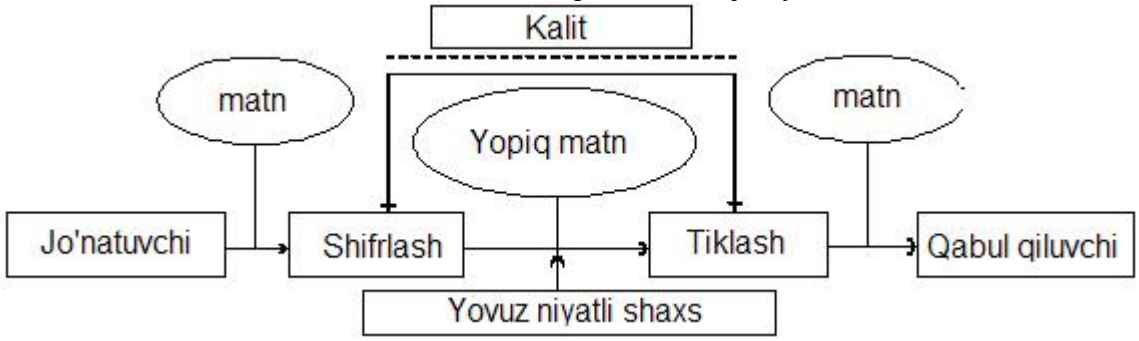


Shifrlash jarayoni quyidagicha amalga oshiriladi:

Tiklash yoki deshifrlash jarayoni quyidagicha amalga oshiriladi:



Simmetrik kriptotizim ish jarayoni



Uinstonning “ikkilangan kvadrat” usuli yordamida matnni shifrlash

Uinstonning “ikkilangan kvadrat” usuli uchun ('A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z', ' ', '.', ',', '?', '!', '=', '+', '-', ':', ';', '“',' (', ')', '%') harf va belgilardan tashkil topgan alfavitni tanlaymiz.

1, Alfavit 40 ta elementga ega. Shuning uchun jadvalni ustuni sonini 8 ta, qatorlar sonini 5 ta deb olsak bo`ladi.

2. Jadvallarni Trisemussning shifrlash jadvallari usulidan foydalanib tuzamiz. Buning uchun birinchi jadval uchun ‘Muhammad’, ikkinchi jadval uchun ‘Majidov’ kalit so`zlarni tanlaymiz.

3. Kalit so`zlardagi takrorlanuvchi harflarni tushirib qoldirsak, birinchi jadval uchun ‘Muhad’, ikkinchi jadval uchun ‘Majidov’ kalit so`z hosil bo`ladi.

4. Bu kalit so`zlarning har bir harfini jadvallarning xonalariga birinchi qatoridan boshlab navbat bilan kiritamiz. So`ngra bu kalit so`zda mavjud bo`lmagan alfavit harflari va belgilarini jadvallarning xonalariga navbat bilan kiritamiz.

Natijada quyidagi jadvallarni olamiz:

M	U	H	A	D	B	C	E
F	G	I	J	K	L	N	O
P	Q	R	S	T	V	W	X
Y	Z		.	,	?	!	=
+	-	:	;	“	(	)	%

M	A	J	I	D	O	V	B
C	E	F	G	H	K	L	N
P	Q	R	S	T	U	W	X
Y	Z		.	,	?	!	=
+	-	:	;	“	(	)	%

5. Shifrlanadigan matnni beramiz:
Uinstonning ikkilangan kvadrat shifri

6. Shifrlanadigan matnni bigrammalarga, ya`ni juft bo`laklarga bo`lamiz.
UI NS TO NN IN G IK KI LA NG AN K VA DR AT S HI FR I

7. Har bir juft bo`lakni alohida-alohida shifrlaymiz.

Shifrlanadigan juft bo`lakning birinchi harfi $M_1$, ikkinchi harfi $M_2$ bo`lsin. Shifrlangan juft bo`lakning birinchi harfi $U_1$, ikkinchi harfi $U_2$ bo`lsin. Shifrlashni quyidagi jadvallar uchun ko`rib chiqamiz:

$A_{11}\ A_{12}\ A_{13}\ A_{14}\ A_{15}\ A_{16}\ A_{17}\ A_{18}$ $\quad$ $B_{11}\ B_{12}\ B_{13}\ B_{14}\ B_{15}\ B_{16}\ B_{17}\ B_{18}$

$A_{21}\ A_{22}\ A_{23}\ A_{24}\ A_{25}\ A_{26}\ A_{27}\ A_{28}$ $\quad$ $B_{21}\ B_{22}\ B_{23}\ B_{24}\ B_{25}\ B_{26}\ B_{27}\ B_{28}$

$A_{31}\ A_{32}\ A_{33}\ A_{34}\ A_{35}\ A_{36}\ A_{37}\ A_{38}$ $\quad$ $B_{31}\ B_{32}\ B_{33}\ B_{34}\ B_{35}\ B_{36}\ B_{37}\ B_{38}$

$A_{41}\ A_{42}\ A_{43}\ A_{44}\ A_{45}\ A_{46}\ A_{47}\ A_{48}$ $\quad$ $B_{41}\ B_{42}\ B_{43}\ B_{44}\ B_{45}\ B_{46}\ B_{47}\ B_{48}$

Shifrlash uchun M_1 harfni A jadvaldan, M_2 harfni esa B jadvaldan izlab topamiz, ya`ni:
$M_1=A_{ij}$ va $M_2=B_{mn}$

a. Agar matn (M_1M_2) juft bo`lakning harflari jadvallarning turli qatorlarida joylashgan bo`lsa, u holda shifrmatn (U_1U_2) juft bo`lak quyidagicha olinadi:

$U_1= B_{in}$, $U_2= A_{mj}$

b. Agar matn (M_1M_2) juft bo`lakning harflari jadvallarning bir qatorida joylashgan bo`lsa, u holda u holda shifrmatn (U_1U_2) juft bo`lak quyidagicha olinadi:

$U_1= B_{ij}$, $U_2= A_{mn}$

Bigrammalarga ajratilgan matnni Uinston ikkilangan kvadrat usuli bo`yicha har bir juftini jadvaldagi o`rnini topamiz va uni mos harfga almashtiramiz.

UI NS TO NN IN G IK KI LA NG AN K VA DR AT S HI FR I

Matn UI o`rni $A_{12}B_{14}$ bo`lsa, shifrmatn o`rni $B_{12}A_{14}$ va shifrmatn AA bo`ladi.
Matn NS o`rni $A_{27}B_{34}$ bo`lsa, shifrmatn o`rni $B_{24}A_{37}$ va shifrmatn GW bo`ladi.
Matn TO o`rni $A_{35}B_{16}$ bo`lsa, shifrmatn o`rni $B_{36}A_{15}$ va shifrmatn UD bo`ladi.
Matn NN o`rni $A_{27}B_{28}$ bo`lsa, shifrmatn o`rni $B_{27}A_{28}$ va shifrmatn LO bo`ladi.
Matn IN o`rni $A_{23}B_{28}$ bo`lsa, shifrmatn o`rni $B_{23}A_{28}$ va shifrmatn FO bo`ladi.
Matn G o`rni $A_{22}B_{43}$ bo`lsa, shifrmatn o`rni $B_{23}A_{42}$ va shifrmatn FZ bo`ladi.
Matn IK o`rni $A_{23}B_{26}$ bo`lsa, shifrmatn o`rni $B_{23}A_{26}$ va shifrmatn FL bo`ladi.
Matn KI o`rni $A_{25}B_{14}$ bo`lsa, shifrmatn o`rni $B_{24}A_{15}$ va shifrmatn GD bo`ladi.
Matn LA o`rni $A_{26}B_{12}$ bo`lsa, shifrmatn o`rni $B_{22}A_{16}$ va shifrmatn EB bo`ladi.
Matn NG o`rni $A_{27}B_{24}$ bo`lsa, shifrmatn o`rni $B_{27}A_{24}$ va shifrmatn LJ bo`ladi.
Matn AN o`rni $A_{14}B_{28}$ bo`lsa, shifrmatn o`rni $B_{18}A_{24}$ va shifrmatn BJ bo`ladi.
Matn K o`rni $A_{43}B_{26}$ bo`lsa, shifrmatn o`rni $B_{46}A_{23}$ va shifrmatn ?I bo`ladi.
Matn VA o`rni $A_{36}B_{12}$ bo`lsa, shifrmatn o`rni $B_{32}A_{16}$ va shifrmatn QB bo`ladi.
Matn DR o`rni $A_{15}B_{33}$ bo`lsa, shifrmatn o`rni $B_{13}A_{35}$ va shifrmatn JT bo`ladi.
Matn AT o`rni $A_{14}B_{35}$ bo`lsa, shifrmatn o`rni $B_{15}A_{34}$ va shifrmatn DS bo`ladi.
Matn S o`rni $A_{43}B_{34}$ bo`lsa, shifrmatn o`rni $B_{44}A_{33}$ va shifrmatn .R bo`ladi.
Matn HI o`rni $A_{13}B_{14}$ bo`lsa, shifrmatn o`rni $B_{13}A_{14}$ va shifrmatn JA bo`ladi.
Matn FR o`rni $A_{21}B_{33}$ bo`lsa, shifrmatn o`rni $B_{23}A_{31}$ va shifrmatn FP bo`ladi.
Matn I o`rni $A_{23}B_{43}$ bo`lsa, shifrmatn o`rni $B_{23}A_{43}$ va shifrmatn F bo`ladi.

Natijada matnni shifrlab, quyidagi shifrmatnni olamiz.

Shifrlanadigan matn: UINSTONNING IKKILANGAN KVADRAT SHIFRI
Shifrlangan matn: AAGWUDLOFOFZFLGDEBLJBJ?IQBJTDS.RJAFPF

Uinstonning ‘ikkilangan kvadrat’ usuli yordamida shifrmatnni deshifrlash

Shifrlangan matnni deshifrlash uchun:

1. Shifrlashda ishlatilgan alfavit aynan o`zgarishsiz qabul qilinadi.
2. Jadval o`lchamlari o`zgarmaydi, ustun soni 8 ta, qatorlar soni 5 ta deb olinadi.
3. Birinchi jadval uchun ‘Muhammad’, ikkinchi jadval uchun ‘Majidov’ kalit so`zlar o`zgarishsiz olinadi.
4. Kalit so`zlardagi takrorlanuvchi harflarni tushirib qoldirib, birinchi jadval uchun ‘Muhad’, ikkinchi jadval uchun ‘Majidov’ kalit so`z hosil qilinadi.
5. Bu kalit so`zlarning har bir harfini jadvallarning xonalariga birinchi qatoridan boshlab navbat bilan kiritamiz. So`ngra bu kalit so`zda mavjud bo`lmagan alfavit harflari va belgilarini jadvallarning xonalariga navbat bilan kiritamiz.

Natijada quyidagi jadvallarni olamiz:

M	U	H	A	D	B	C	E
F	G	I	J	K	L	N	O
P	Q	R	S	T	V	W	X
Y	Z		.	,	?	!	=
+	-	:	;	“	(	)	%

M	A	J	I	D	O	V	B
C	E	F	G	H	K	L	N
P	Q	R	S	T	U	W	X
Y	Z		.	,	?	!	=
+	-	:	;	“	(	)	%

6. Shifrlangan matnni beramiz:
AAGWUDLOFOFZFLGDEBLJBJ?IQBJTDS.RJAFPF
7. Shifrlangan matnni bigrammalarga, ya`ni juft bo`laklarga bo`lamiz.
AA GW UD LO FO FZ FL GD EB LJ BJ ?I QB JT DS .R JA FP F

Deshifrlanadigan juft bo`lakning birinchi harfi $M_1$, ikkinchi harfi $M_2$ bo`lsin. Deshifrlangan juft bo`lakning birinchi harfi $U_1$, ikkinchi harfi $U_2$ bo`lsin. Deshifrlashni quyidagi jadvallar uchun ko`rib chiqami:

$A_{11}\ A_{12}\ A_{13}\ A_{14}\ A_{15}\ A_{16}\ A_{17}\ A_{18}$ $\quad$ $B_{11}\ B_{12}\ B_{13}\ B_{14}\ B_{15}\ B_{16}\ B_{17}\ B_{18}$
$A_{21}\ A_{22}\ A_{23}\ A_{24}\ A_{25}\ A_{26}\ A_{27}\ A_{28}$ $\quad$ $B_{21}\ B_{22}\ B_{23}\ B_{24}\ B_{25}\ B_{26}\ B_{27}\ B_{28}$
$A_{31}\ A_{32}\ A_{33}\ A_{34}\ A_{35}\ A_{36}\ A_{37}\ A_{38}$ $\quad$ $B_{31}\ B_{32}\ B_{33}\ B_{34}\ B_{35}\ B_{36}\ B_{37}\ B_{38}$
$A_{41}\ A_{42}\ A_{43}\ A_{44}\ A_{45}\ A_{46}\ A_{47}\ A_{48}$ $\quad$ $B_{41}\ B_{42}\ B_{43}\ B_{44}\ B_{45}\ B_{46}\ B_{47}\ B_{48}$

Shifrlash uchun M_1 harfni B jadvaldan, M_2 harfni esa A jadvaldan izlab topamiz, ya`ni:
$M_1=B_{mn}$ va $M_2=A_{ij}$

a. Agar shifrmatn (M_1M_2) juft bo`lakning harflari jadvallarning turli qatorlarida joylashgan bo`lsa, u holda matn (U_1U_2) juft bo`lak quyidagicha olinadi:
$U_1= A_{mj}$, $U_2= B_{in}$

b. Agar shifrmatn (M_1M_2) juft bo`lakning harflari jadvallarning bir qatorida joylashgan bo`lsa, u holda (U_1U_2) juft bo`lak quyidagicha olinadi:
$U_1= A_{mn}$, $U_2= B_{ij}$

Bigrammalarga ajratilgan shifrmatnni Uinston ikkilangan kvadrat usuli bo`yicha har bir juftini jadvaldagi o`rnini topamiz va uni mos harfga almashtiramiz.
AA GW UD LO FO FZ FL GD EB LJ BJ ?I QB JT DS .R JA FP F
Shifrmatn AA o`rni $B_{12}A_{14}$ bo`lsa, matn o`rni $A_{12}B_{14}$ va matn UI bo`ladi.
Shifrmatn GW o`rni $B_{24}A_{37}$ bo`lsa, matn o`rni $A_{27}B_{34}$ va matn NS bo`ladi.
Shifrmatn UD o`rni $B_{36}A_{15}$ bo`lsa, matn o`rni $A_{35}B_{16}$ va matn TO bo`ladi.
Shifrmatn LO o`rni $B_{27}A_{28}$ bo`lsa, matn o`rni $A_{27}B_{28}$ va matn NN bo`ladi.
Shifrmatn FO o`rni $B_{23}A_{28}$ bo`lsa, matn o`rni $A_{23}B_{28}$ va matn IN bo`ladi.
Shifrmatn FZ o`rni $B_{23}A_{42}$ bo`lsa, matn o`rni $A_{22}B_{43}$ va matn G bo`ladi.
Shifrmatn FL o`rni $B_{23}A_{26}$ bo`lsa, matn o`rni $A_{23}B_{26}$ va matn IK bo`ladi.
Shifrmatn GD o`rni $B_{24}A_{15}$ bo`lsa, matn o`rni $A_{25}B_{14}$ va matn KI bo`ladi.
Shifrmatn EB o`rni $B_{22}A_{16}$ bo`lsa, matn o`rni $A_{26}B_{12}$ va matn LA bo`ladi.
Shifrmatn LJ o`rni $B_{27}A_{24}$ bo`lsa, matn o`rni $A_{27}B_{24}$ va matn NG bo`ladi.
Shifrmatn BJ o`rni $B_{18}A_{24}$ bo`lsa, matn o`rni $A_{14}B_{28}$ va matn AN bo`ladi.
Shifrmatn ?I o`rni $B_{46}A_{23}$ bo`lsa, matn o`rni $A_{43}B_{26}$ va matn K bo`ladi.
Shifrmatn QB o`rni $B_{32}A_{16}$ bo`lsa, matn o`rni $A_{36}B_{12}$ va matn VA bo`ladi.
Shifrmatn JT o`rni $B_{13}A_{35}$ bo`lsa, matn o`rni $A_{15}B_{33}$ va matn DR bo`ladi.
Shifrmatn DS o`rni $B_{15}A_{34}$ bo`lsa, matn o`rni $A_{14}B_{35}$ va matn AT bo`ladi.
Shifrmatn .R o`rni $B_{44}A_{33}$ bo`lsa, matn o`rni $A_{43}B_{34}$ va matn S bo`ladi.
Shifrmatn JA o`rni $B_{13}A_{14}$ bo`lsa, matn o`rni $A_{13}B_{14}$ va matn HI bo`ladi.
Shifrmatn FP o`rni $B_{23}A_{31}$ bo`lsa, matn o`rni $A_{21}B_{33}$ va matn FR bo`ladi.
Shifrmatn F o`rni $B_{23}A_{43}$ bo`lsa, matn o`rni $A_{23}B_{43}$ va matn I bo`ladi.

Natijada matnni deshifrlab, qo`yidagi matnni olamiz.

Shifrlangan matn: AAGWUDLOFOFZFLGDEBLJBJ?IQBJTDS.RJAFPF

Deshifrlangan matn: UINSTONNING IKKILANGAN KVADRAT SHIFRI

Ilova 7

Nazorat savollari

1. Ma`lumotlarni himoyalash deganda nimani tushunasiz?
2. Kriptografiya kanday vazifalarni bajaradi
3. Kriptografik tizim nima?
4. Hozirgi zamon kriptografiyasi qanday yo`nalishlarga ega?
5. Kriptografik uslublardan foydalanishning asosiy yo`nalishlarini ayting?
6. Kriptografiya qanday vazifalarni bajaradi?
7. Kriptografik uslublarning vazifalari nimadan iborat?
8. SHifrlash nima?
9. Deshifrlash nima?
10. Kalit nima?
11. MBBT tavsifi nima?
12. Kriptoanaliz yoki kriptotahlil deganda nimani tushunasiz?
13. Kriptochidamlilik yoki kriptomustahkamlik deganda nimani tushunasiz?
14. Uzatiladigan axborotni kriptografik tizim orqali himoyalashning umumiy sxemasini tavsiflang.
15. Ikki har xil kalitli assimmetrik kriptotizimning umumiy sxemasini tavsiflang.
16. Shifrlash jarayoni qanday amalga oshiriladi?
17. Tiklash yoki deshifrlash jarayoni qanday amalga oshiriladi?
18. Simmetrik kriptotizim ish jarayonini tavsiflang.
19. Uinstonning ‘ikkilangan kvadrat’ usuli yordamida matnni shifrlashni tavsiflang.
20. Uinstonning ‘ikkilangan kvadrat’ usuli yordamida shifrmatnni deshifrlashni tavsiflang.