**O‘ZBEKISTON RESPUBLIKASI RAQAMLI TEXNOLOGIYALAR VAZIRLIGI**

**MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI SAMARQAND FILIALI**

**TELEKOMMUNIKATSIYA TEXNOLOGIYALARI VA KASB TA’LIMI FAKULTETI**

**“Axborot xavfsizligi” kafedrasi**

5330300 – “Axborot xavfsizligi” ta’lim yo‘nalishi bo‘yicha bakalavr akademik darajasini olish uchun

“Himoyaga ruxsat”

kafedra mudiri:

dots. N.R. Zaynalov \_\_\_\_\_\_\_\_\_\_

2023-yil “\_\_” \_\_\_\_\_\_\_\_\_\_

**“OpenSSL kutubxonasidan foydalangan holda xavfsiz malumot almashinuvini hosil qilish”**

mavzusida

**BITIRUV MALAKAVIY ISHI**

Bitiruvchi: \_\_\_\_\_\_\_\_\_\_ 407-guruh talabasi Xudoyberdiyev D.

Ilmiy rahbar: \_\_\_\_\_\_\_\_\_\_ ass. Shakarov A

Taqrizchi: \_\_\_\_\_\_\_\_\_\_ dots.Nazarov U.

HFX maslahatchi: \_\_\_\_\_\_\_\_\_\_ ass. Rajabov J.

**Samarqand – 2023**

|  |  |  |
| --- | --- | --- |
|  | **Kirish…………………………………………………………………………** | **3** |
| **I BOB** | **XAVFSIZ MA’LUMOT ALMASHISH TIZIMLARIDA KRIPTOGRAFIYANING O’RNI……………………………………….** | **6** |
| 1.1. | Kriptografiya va uning axborotni muhofaza qilish masalalarini yechishda qo‘llanilishi ………………………… | **6** |
| 1.2. | Simmetrik kriptotizmlarda axborot almashish bosqichlari ………………. | **11** |
| 1.3 | Kriptotizmlarni elektron raqam tizimida ishlatilishi .…………………….. | **16** |
| 1.4 | Xesh kunfsiyalar.......................................................................................... | **21** |
| **II BOB** | **MA’LUMOTLARNI XAVFSIZ ALMASHISH JARAYONIDA OPENSSL KUTUBXONASIDAN FOYDALANISH ……………….** | **25** |
| 2.1. | Axborot almashish tizimlarida assimmetrik kriptotizimlar ahamiyati ........ | **25** |
| 2.2. | Openssl kutubxonasi shifrlash algoritmlari tahlili………………………… | **30** |
| 2.3. | Openssl kutubxonasi imkoniyatlari asosida ishlab chiqilgan kriptografik vositalar .........……………………………………………………………. | **31** |
| **III BOB** | **OPENSSL KUTUBXONASIDAN FOYDALANGAN HOLDA XAVFSIZ MA’LUMOT ALMASHISHNI JORIY QILISH ………….** | **34** |
| 3.1. | Openssl kutubxonasi imkoniyatlari asosida xavfsiz ma`lumot almashish jarayonini tashkil etish bosqichlari ………………………………………… | **34** |
| 3.2. | Openssl kutubxonasidan foydalangan holda xavfsiz ma’lumot almashishni joriy qilish……………….………………………………………………… | **42** |
| 3.3 | Dasturiy ta’minotni yaratishda mehnat muhofazasi va texnika xavfsizligi…. | **45** |
|  | **XULOSA…………………………………………………………………....** | **51** |
|  | **ADABIYOTLAR RO‘YXATI…………………………………………….** | **52** |

**KIRISH**

**Mavzuning asoslanishi va uning dolzarbligi.** O‘zbekiston Respublikasi mustaqillikka erishishi tufayli ijtimoiy-iqtisodiy tizimning barcha sohalarida ijobiy o‘zgarishlar yuz berdi. Malumki, axborot-komunikatsiya texnologiyalari davlatimiz iqtisodiy-ijtimoiy rivojlanishini ta’minlashda asosiy sektorlardan biri hisoblanadi.

Mamlakatimizda o‘tkazilayotgan iqtisodiy xalq xo‘jaligining yetakchi sohalarida axborot-komunikatsiya texnologiyalarini keng joriy etishga qaratilagan bo‘lib davlat hokimiyati va boshqaruv organlarida ish yuritish faoliyatini electron shaklda amalga oshirishni talab etmoqda. Davlat hokimiyati va boshqaruv organlari hamda fuqarolarning o‘zaro axborot almashinishida elektron ma‘lumotlardan foysalanishga o‘tish buning yaqqol dalili hisiblanadi. Bu jarayonning huquqiy asoslarini mustahkamlash maqsadida Respublikamizda bir qator Qonunlar, Prezedent Farmon va qarorlari qabul qilingan. Jumladan O‘zbekiston Respublikasining «Axborotlashtirish tog‘risida»gi, “Telekomunikatsiyalar to‘g‘risisda”gi Qonunlari [1] hamda O‘zbekiston Respublikasi Prezedentining «O‘zbekiston Respublikasining jamoat ta’lim axborot tarmog‘ini tasgkil etish to‘g‘risida»gi [3], “Zamonaviy axborot-komunikatsiya tizimini yanada rivojlantirish chora-tadbirlari to‘g‘risida”gi [4], «O‘zbekiston Respublikasi Milliy axborot-komunikatsiya tizimini yanada rivojlantirish chora-tadbirlari to‘risida» gi [5] Qarorlari va ushbu qaror ijrosini ta’minlash borasida ishlab chiqilgan me‘yoroy-huquqiy hujjatlar O‘zbekiston Respublikasi axborot komunikatsiya texnologiyalarini hozirgi kun talablari darajasida rivojlantirish, joriy etish masalalariga qaratilgan.

O‘zbekiston Respublikasining «Ta‘lim tog‘risida»gi Qonuni va kadrlar tayyorlash milliy dasturi [2] asosida uzluksiz ta’limi tizimida yuqori malakali kadrlarni tayyorlash, ularda ilmiy dunyoqarashni, mehnatga ijodiy munosabatni tarkib toptirish,yuksak mehnat intizomini shakllantirish vazifasini qo‘yadi. Ushbu Qonunlar va qonunosti hujjatlarini amaliyotga joriy etishda respublikamizda telekomunikatsiya tizimlarini rivojlantirish va axborotlashtirish sohasida olib borilayotgan ilmiy tadqiqot ishlari muhim ahamiyat kasb etmoqda.

**Masalaning qo‘yilishi.** Openssl kutubxonasidan foydalangan holda xavfsiz ma’lumot almashinuvini hosil qilish. Shu bilan birga kriptografik shifrlash algoritmlarini o’rganish.

Elektron xizmatlar va elektron tijoratning jadal rivojlanishi korparativ tarmoqda, umumiy foydalanish tarmog‘i bo‘lmish – internetda axborot xavfsizligi muammosini hal etish *muhim va dolzarb masalalar* sirasiga kiradi. Hozirgi paytda axborotni kriptografik himoya qilish eng ishonchli himoya usullaridan biridir.

Tarmoqda ma‘lumotlarni himoyalashning ko‘plab usullari (dasturiy, apparatli, huquqiy va boshqalar) ishlab chiqilgan. Shunga qaramasdan bugungi kunda tarmoqdagi ma‘lumotlarni himoyalashning yangidan yangi usul va uslublarini ishlab chiqish, yangi algoritm va dasturiy vositalar yaratish extiyoji sezilmoqdi.

**Bitiruv malakaviy ishining maqsadi.** Ushbu bitiruv malakaviy ishida kompyuter tarmoqlarida ishchi stantsiyalararo ma’lumotlar uzatishda, shifrlash algoritmlaridan foydalanib, xavfsiz ma’lumotlarni almashishni hosil qilish maqsad qilib olingan. Xavfsiz ma’lumot almashish tizimini hosil qilishda openssl kutubxonasidan foydalanilgan.

**Bitiruv malakaviy ishining vazifalari.** Yuqoridagilardan kelib chiqib bitiruv malakaviy ishining asosiy vazifalari sifatida quyidagilar olindi:

* Adabiyotlar va internet manbalari yordamida tarmoq texnologiyalari, internet asoslari va unda ma‘lumotlarni himoyalash usullarining umumiy va xususiy muammolari bilan tanishish;
* Mavzu bo‘yicha nazariy va amaliy manbalarni to‘plash;
* Bir tomonlama funksiyalarni o‘rganish;
* Kriptografik shifrlash algoritmlari haqida bilim va ko’nikmalarga ega bo’lish;
* Openssl kutubxonasidan foydalanishni o’rganish ;
* Openssl kutubxonasidan foydalangan holda shifrlash algoritmlari yordamida xavfsiz ma’lumot almashishni joriy qilish;
* Joriy qilingan xavfsiz ma’lumot almashish tizimini electron raqamli imzo yordamida tekshirish;

**Bitiruv malakaviy ishining ilmiy ahamiyati.** Ishning ilmiy yangiligi, ishda kriptobardoshli algoritmlaridan foydalanilganligidir.

**Bitiruv malakaviy ishining amaliy ahamiyati.** Ishning natijalari kelgusi tadiqiqotlar, shifrlash kriptobardoshligini oshirish usullarini o‘ziga xos yondashuvlarini izlash uchun ilmiy amaliy ahamiyatga egadir. Mavjud algoritmlarini qo‘llash bo‘yicha takliflar shifrlash algoritmlarini yaratish jarayonida foydali bo‘lishi mumkin.

**Bitiruv malakaviy ishining ilmiy-tadqiqot usullari.** Bitiruv malakaviy ishining obyekti, uning asosiy maqsadlarida ko‘rsatilgan vazifalar nazariy ahamiyatga ega bo‘lganligi sababli uning tadqiqot usullari sifatida nazariy va kompyuterli sinov (test) tanlandi.

**Bitiruv malakaviy ishining tuzilishi.** Bitiruv malakaviy ishi kirish, uchta bob, dasturiy ta‘minot va undan foydalanish, xulosa, foydalanilgan adabiyotlar ro‘yxati va ilovadan iborat.

Bitiruv malakaviy ishining «Kirish» qismida masalaning qo‘yilishi uning dolzarbligi, ishning asosiy maqsadi, uning imliy-amaliy ahamiyati hamda ish strukturasi keltirilgan.

Bitiruv malakaviy ishining birinchi bobida “Xavfsiz ma’lumot almashish tizimlarida kriptografiyaning o’rni” bo’yicha umumiy nazariy asoslari yoritilgan.

Ikkinchi bobida «Ma’lumotlarni xavfsiz almashish jarayonida openssl kutubxonasidan foydalanish» bo’yicha nazariy jihatdan tushuntirib o‘tilgan va openssl kutubxonasining imkoniyatlari keltirilib o’tilgan.

Uchinchi bobida «Dasturiy ta‘minot va undan foydalanish» da algoritmlarining tarmoqda himoyalashni tahlil qiluvchi dasturiy vositaning interfeysi va undan foydalanish keltirilgan.

Bitiruv malakaviy ishining xulosa qismida tadqiqotlar natijalari, bajarilgan ishlar umumlashtirib umumiy xulosalar kabi shakllantirilgan.

**I BOB. XAVFSIZ MA’LUMOT ALMASHISH TIZIMLARIDA KRIPTOGRAFIYANING O’RNI**

**1.1. Kriptografiya va uning axborotni muhofaza qilish masalalarini yechishda qo‘llanilishi.**

Bugungi kunda axborot xavfsizligini ta’minlashda an’anaviy qo‘llanilib kelgan yondoshuvlar va vositalar etarli bo’lmay qoldi. Bunday sharoitda axborot himoyasining eng ishonchli va sinalgan usuli bo‘lgan kriptografiyaning ahamiyati yanada oshdi. Quyida Internet va Intranetda axborot himoyasining kriptologiya yo’nalishi haqida batafsil to’xtalamiz.

Kriptologiya-axborotni kriptologiyaviy o‘zgartishning ilmiy-uslubiy usullari, uslub va vositalarini yaratish hamda o’rganish bilan shug‘ullanuvchi fan. Kriptologiya ikki ilmiy irmoqga ajraladi. Bular -kriptografiya va kriptotaxlildir.

Kriptografiya – kriptografiya amallari asosida axborot xavfsizligini ta’minlash fani bo‘lib, asosan turt xil xavfsizlik muammosi yechimlarini topish bilan shug‘ullanadi. Bular:

* Pinxoniylik (Confidentiality).
* Axborot butunligi (Data Integrity).
* Autentifikatsiya:

Axborot egasini autentifikatsiyasi (User Authentication)-axborot yuborgan shaxs asl shaxsligini tekshirish.

Axborot asl nusxasini autentifikatsiyasi (Data Origin Authentication)-olingan axborot o’z asliga aylanligini tekshirish.

Aloqa qatnashchilari nazorati:

Inkor eta olmaslik (Non-repudiation) - axborot yo‘llaganlikni yo uni (umuman yo uz vaqtida) qabul qilib olganlikni bo‘yniga olmaslikni oldini olish.

Kriptografiya amallarining eng asosiylari shifrlash va shifrni ochishdir. Shifrlash (inglizcha- enciphering)- shifrlash kaliti ishtirokida berilgan (dastlabki) axborotni begona olib tushunmaydigan shaklga, ya’ni shifrlangan axborotga aylantirishdir. Shifrni ochish (inglizcha- deciphering) - shifrlangan axborotni uni ochish kaliti yordamida dastlabki axborotga aylantirishdir. Shifrni buzib ochish - shifrlangan axborotni shifrni ochish kalitini bilmagan holda dastlabki axborotga aylantirishdir.

Shifrlash pinxoniylikni ta’minlab axborotni begonalardan maxfiy saqlash imkonini beradi. Shifrlanadigan axborot, umuman olganda matn, ovoz yozuvi va tasvir shaklida yo bo‘lmasa aralash shaklda berilishi mumkin. Amaliyotda shifrlanadigan axborot asosan matn (inglizcha-plaintext) shaklida beriladi va shifrlangan matn (inglizcha-ciphertext)ga aylantiriladi.

Ilmiy kriptografiya davrining muhim muvaffaqiyatlari ro’yxati boshida Klod Elvud Shennonning *«Maxfiy tizimlarda aloqa nazariyasi»* (1949) asari turadi [15, 20]. Unda axborot muhofazasining nazariy tamoillari shakllantirib berilgan.

K.E. Shennon tomonidan qilingan bunday kashfiyot, albatta, uning elektrotexnika va matematika bo’yicha chuqur bilimlari va bundan bir yil oldin u yaratgan axborot nazariyasi fani tufayli yuzaga kelgan edi. U nafaqat Vernamning tasodifiy shifrini buzib ochib bo’lmasligini, balki himoyalangan kanal orqali uzatiladigan maxfiy kalit miqdori (bitlar soni) chegaralarini ham aniq ko’rsatib berdi. U cheklanmagan resurslarga ega bo’lgan kriptotahlilchi biror «tasodifiy shifr»ni ochishida maxfiy kalitni topishi uchun zarur bo’lgan shifrlangan matndagi simvollar soni *s* quyidagicha ifodalanishini ko’rsatdi:

*S = H(k)/(r\*Log n)*

bu yerda: *H(k)*- kalit entropiyasi, ya’ni kalitning har bitta simvoliga to’g’ri keladigan axborot miqdori, *r* - ochiq matnning seriboraligi (ruscha, izbыtochnost), *n* - alifbo hajmi.

Keltirilgan ifoda umumiy holda isbotlanmagan bo’lsa-da ma’lum xususiy hollar uchun to’g’ri. Bundan quyidagi muhim xulosa kelib chiqadi: kriptotahlilchining ishini nafaqat kriptotizimni mukammallashtirish orqali, balki shifrlanadigan matnning seriboraligi nolgacha pasaytirilsa, kriptotahlilchi kichik kalit bilan shifrlangan matnni ham ocha olmaydi. Demak, shifrlash oldidan axborotni statistik kodlash (zichlashtirish, arxivlash) lozim. Bunda axborotning hajmi va seriboraligi kamayadi, entropiyasi oshadi. Chunki, ixchamlashgan matnda qaytariluvchi so’zlar va harflar kamayib shifrni buzib ochish qiyinlashadi.

K. Shennon kriptotizimlar bardoshliligini *nazariy* va *amaliy* turlarga ajratadi. Nazariy bardoshlilik deganda raqib tomonning tahlilchisi u qo’lga tushirgan kriptogrammalarni tahlillashda cheklanmagan vaqtga va barcha zarur vositalarga ega bo’lgan holda kriptotizimning bardoshliligi tushuniladi. Amaliy bardoshlilik deganda kriptotahlilchining vaqti va hisoblash imkoniyatlari cheklangan holga oid bardoshlilik tushuniladi. K. Shennon amaliy shifrlarda ishlatiladigan ikki tamoyilni ajratadi. Bular *yoyish va aralashtirishdir*. Yoyish deganda, ochiq matnning bitta simvolini shifrlangan matnning ko’p simvollariga ta’sir etishi tushuniladi. Bu ochiq matnning statistik xossalarini yashirishga imkon beradi. Bu tamoyil kalit simvollariga nisbatan ham qo’llaniladi. Aralashtirish deganda, K. Shennon shifrlanadigan va shifrlangan matnlar statistik xossalarining bir-biriga bog’lanishini tiklashni qiyinlashtiruvchi shifrlashga oid o’zgartirishlarni nazarda tutgan.

K. Shennonning ilmiy kriptologiya asoslarini o’zida mujassamlashtirgan maqolasi bu sohada ochiq tadqiqotlarning sezilarli o’sishiga turtki bo’la olmadi. Chunki, birinchidan, maxfiy aloqa tizimlarining nazariy bardoshlilik nazariyasi o’z mohiyatiga ko’ra to’la edi. Unga ko’ra nazariy jihatdan bardoshli maxfiy tizimlarni hosil qilish uchun himoyalangan kanallar bo’ylab haddan tashqari katta hajmdagi kalitlarni uzatish lozim bo’lardi. Ikkinchidan, amaliy bardoshlilik masalalarini yechish mavjud kriptografiya usullarini takomillashtirish bilangina cheklanib qoldi.

K. Shennonning «yaxshi» shifr yaratish muammosi ma’lum shartlarni qondiruvchi eng murakkab masalalarni topishga keltiriladi. «Bizning shifrimizni shunday tuzish mumkinki, uni buzib ochish yechilishi katta hajmdagi ishlarni talab qilishi ma’lum bo’lgan muammoni o’z ichiga olsin yoki unga ekvivalent bo’lsin» luqmasi yana chorak asr e’tiborsiz qoldi.

Devid Kanning «Kriptograflar» asari kriptografiya tarixi bo’yicha mumtoz asar bo’lib qolgan. Bu asar XX asrning 70 yillari oxirigacha ham Davlat Xavfsizligi Nazoratining maxsus kutubxonasida saqlanib undan foydalanishga ruxsati bo’lgan kimsalar davrasi «ideologik mulohazalar asosida» jiddiy cheklangan. Unda Rossiya haqidagi bo’limda «Maxfiy polisiyaning vazifalaridan biri bo’lib yo’qsillar diktaturasini yo’qsillarning o’zidan muhofaza qilish bo’lgan» deyiladi. Bu XX asrning 70 yillarida ham qo’rqinchli sir bo’lgan [16, 20].

Ikkinchi jahon urushi tugagach, sovet kriptograflaridan undan kam bo’lmagan kuchlarni sarflashni talab etgan «sovuq urush» davri boshlandi.

Bu davrda harbiy kriptografik xizmatning ko’plab ilmiy xodimlari harbiy xizmatdan bo’shatilgan edi. Bu sharoitlarda harbiy chaqiriq yoshida bo’lgan yuqori malakali kriptograflar «xalqlar otasi»ga to’g’ridan-to’g’ri murojaat etishga o’zlarida jasurlik topdilar va ularning murojaatiga e’tibor berildi.

Kriptografiya usullari aloqa tizimining xavfsizligini ta’minlash uchun qo‘llanilganda u aloqa mazmuninigina, ya’ni uzatilayotgan axborotning o’zinigina himoyalaydi, aloqa mavjudligini, shu jumladan aloqaning kimlar orasida va qanday intensivlikda sodir bo‘layotganini esa himoya qilolmaydi. Aloqa mavjudligini steganografiya usullari himoyalash imkonini beradi. Bunda ayrim hollarda kanaldagi trafikning doimiy (masalan, bir xil shovqin tarzida) bo‘lishiga, ya’ni trafikning uzatilayotgan axborotga bog‘lik bo‘lmasligiga erishish kifoya qiladi.

Axborot uzatish va saqlash jarayonlarining raqamlashtirilishi uzlukli (nutq) va uzluksiz (matn, faks, teleks, tasvir, animatsiya) axborotlarni himoyalash uchun yagona algoritmlardan foydalanish imkonini beradi. Bundan buyon Shifrlanadigan axborot matn shaklida berilishi nazarda tutiladi.

Shifrlash algoritmlariga quyidagi talablar qo‘yiladi:

Shifrlangan axborotni o‘zgartirib qo‘yish yo uni Shifrini buzib ochishga yo’l qoldirmaslik;

* axborot himoyasi faqat kalitning ma’lumligiga bog‘lik bo‘lib, algoritmning ma’lum yo noma’lumligiga bog‘lik emas (Kerkgoff qoidasi);
* dastlabki (Shifrlanadigan) axborotni yoki kalitni biroz o‘zgartirish Shifrlangan matnning butunlay o‘zgartirib yuborishi lozim ("o‘pirilish" xodisasi);
* kalitning qiymatlar sohasi shunday katta bo‘lishi kerakki, undan kalit qiymatlarini bir boshdan ko‘rib-chiqish asosida shifrni buzib ochish imkoni bo‘lmasligi lozim;
* algoritm iqtisodiy jihatdan tejamli va etarli tezkorlikka ega bo‘lishi lozim;

Shifr matnini buzib ochishga ketadigan sarf-xarajaatlar axborot bahosidan yuqori bo‘lishi lozim.

Kriptotizm shifrlash ham shifrni ochish algoritmlari, bu algoritmlarda ishlatiladigan kalitlar, shu kalitlarni boshqaruv tizimi hamda shifrlanadigan va shifrlangan matnlarning o‘zaro bog‘langan majmuasidir.

Kriptotizmdan foydalanishda matn egasi shifrlash algoritmi va shifrlash kaliti vositasida avvalo dastlabki matnni shifrlangan matnga o‘giradi. Matn egasi uni o‘zi foydalanishi uchun shifrlagan bo‘lsa (bunda kalitlarni boshkaruv tizimiga hojat ham bo‘lmaydi) saqlab qo‘yadi va kerakli vaqtda shifrlangan matnni ochadi. Ochilgan matn asli (dastlabki matn)ga aynan bo‘lsa saqlab qo‘yilgan axborotning butunligiga ishonch xosil bo‘ladi. Aks xolda axborot butunligi buzilgan bo‘lib chiqadi.

Agar shifrlangan matn uni yaratgan kimsadan o‘zga qonuniy foydalanuvchiga (oluvchiga) muljallangan bo‘lsa, u tegishli manzilga junatiladi. So‘ngra Shifrlangan matn oluvchi tomonidan unga avvaldan ma’lum bo‘lgan Shifr ochish kaliti va algoritmi vositasida dastlabki matnga aylantiriladi.

Bundan tashqari shifrlash algoritmlari dastlabki (shifrlanadigan yo kodlanadigan) axborot xamda kriptografik yopilgan (shifrlangan yo kodlangan) axborotga mos qilib olingan to‘plamlar elementlari va ular orasidagi munosabatlar turi (x.1) turi buyicha shifrlar (ciphers)ga va kodlar (codes)ga bo‘linadilar. Shifrlar alohida bitlar, harflar, simvollar to‘plamlari bilan ish ko‘rsa, kodlar alohida lingvistik elementlar to‘plamlari bilan ish ko‘radilar.

Barcha nosimmetrik kriptotizmlarni kriptotahlil qilish asosan kalitlarni bir boshdan ko‘rib chiqish asosida amalga oshiriladi. Shuning uchun ularning simmetrik kriptotizmlarga teng bardoshliligini ta’minlash maqsadida ancha uzun (bitlar soni bo‘yicha) kalitlardan foydalaniladi. Bryus Shneer uzining "Amaliy kriptografiya: Ci da protokollar, algoritmlar i dastlabki matn" kitobida kalitlarning ekvivalent uzunliklari uchun qo‘yidagi raqamlarni keltiradi.

Simmetrik kalit uzunligi, bit 56, 64, 80, 112, 128

Nosimmetrik kalit uzunligi, bit 384, 512, 768, 1792, 2304

**1.2. Simmetrik kriptotizmlarda axborot almashish bosqichlari**

Axborot uzatish va saqlash jarayonlarining raqamlashtirilishi uzlukli (nutq) va uzluksiz (matn, faks, teleks, tasvir, animasiya) axborotlarni muhofazalash uchun yagona algoritmlardan foydalanish imkonini beradi. Shifrlash algoritmlariga quyidagicha asosiy talablar qo’yiladi:

- shifrlangan axborotni o’zgartirib qo’yish yoki uning shifrini buzib – ochishga yo’l qoldirmaslik;

- axborot muhofazasi faqat kalitning ma’lumligiga bog’liq bo’lib, algoritmning ma’lum yo noma’lumligiga bog’liq emas (O.Kerkgoff qoidasi);

- dastlabki axborot (ma’lumot)ni yoki kalitni biroz o’zgartirish shifrlangan matnning butunlay o’zgartirib yuborishi lozim (K. Shennon tamoyili, “o’pirilish” hodisasi);

- kalit qiymatlari sohasi shunday katta bo’lishi kerakki, undan kalit qiymatlarini bir boshdan ko’rib chiqish asosida shifrni buzib ochish imkoni bo’lmasligi lozim;

- algoritm iqtisodiy jihatdan tejamli va yetarli tezkorlikka ega bo’lishi lozim;

- shifrmatnni buzib ochishga ketadigan sarf-xarajatlar axborot bahosidan yuqori bo’lishi lozim.

Kriptografik tizim, yo qisqacha, kriptotizim, shifrlash hamda shifrni ochish algoritmlari, bu algoritmlarda ishlatiladigan kalitlar, shifrlanadigan hamda shifrlangan matnlar va bularning o’zaro moslashish qoidalarini o’zida mujassamlantirgan protokol (bayonnoma)dan iborat majmuadir.

Kriptotizimdan foydalanishda matn muallifi shifrlash algoritmi va shifrlash kaliti vositasida avvalo dastlabki matnni shifrlangan matnga o’giradi. Matn muallifi uni o’zi foydalanishi uchun shifrlagan bo’lsa (bunda kalitlarni boshqaruv tizimiga hojat ham bo’lmaydi) uni saqlab qo’yadi va kerakli vaqtda shifrlangan matnni ochadi. Ochilgan matn asli (dastlabki matn)ga aynan bo’lsa, saqlab qo’yilgan axborotning yaxlitligiga ishonch hosil bo’ladi. Aks holda axborot butunligi buzilgan bo’lib chiqadi (1.1-rasm). Bu yerda *k* – yuboruvchi va qabul qiluvchining simmetrik maxfiy kaliti.

Shifrlangan axborot

**k**

**k**

**Shifrlangan axborotni dastlabkiga o’g’rish**

**Axborotni shifrlash**

Dastlabki axborot

Dastlabki axborot

1.1-rasm. Simmetrik kriptotizimlarda axborot almashish

Agar shifrlangan matn uni yaratgan kimsadan o’zga qonuniy foydalanuvchiga (oluvchiga) mo’ljallangan bo’lsa, u tegishli manzilga jo’natiladi. So’ngra shifrlangan matn oluvchi tomonidan unga avvaldan ma’lum bo’lgan shifrni ochish kaliti va algoritmi vositasida dastlabki matnga o’giriladi.

Kriptograflar orasida mashhur bo’lgan ma’lumotlarni shifrlash algoritmlari guruhiga AQSh davlat standartlari – DES [11, 25], AES [26], Rossiya Federasiyasi davlat standarti GOST 28147-89 [27], IDEA [11, 25], FEAL [11, 25] kiradi.

**DES** IBM firmasining butun bir kriptograflari guruhi tomonidan ishlab chiqilgan [11, 25]. Ma’lumotlarni shifrlash standarti 1976 yil 23 noyabrda Milliy Standartlar Byurosi tomonidan AQShning davlat standarti sifatida qabul qilingan va u 1977 yil iyul oyidan 2000 yil oktyabr oyigacha raqamli ma’lumotlarni shifrlash uchun standart bo’lib xizmat qilgan. Hozirgi vaqtda u faqat nazariy ahamiyatga ega. DES zanjirsimon tuzilmali muvozanatlangan Feystal tarmog’i arxitekturasiga ega. Mutaxassislarning fikriga ko’ra bu standart yoyish va aralashtirish tamoyillariga asoslangan eng yaxshi kriptoalgoritmlardan biridir. Shifrlash algoritmida shifrmatnning har bir biti dastlabki matn va kalit barcha bitlarining funksiyasi bo’ladi. Standartda o’rniga qo’yish, o’rin almashtirish va 2 modul bo’yicha qo’shish amallarining kombinasiyasidan foydalaniladi.

**GOST 28147-89** - sobiq Sovet Ittifoqida ishlab chiqilgan DES kabi muvozanatlangan Feystal tarmog’i [27] arxitekturali *64*-bit blokli va kalit uzunligi *256* bit bo’lgan kriptografik o’zgartirish algoritmidir [27]. Algoritm bosqichlari soni *32* ga teng bo’lsa-da, u DESga nisbatan tezkordir.

Shifrmatnni dastlabki matnga o’girish ham xuddi dastlabki matnni shifrmatnga o’girish kabi bajariladi, faqat bunda kalitlar ketma-ketligi o’zgartiriladi.

GOST 28147-89da DES, AESga xos elektron kod kitobi rejimiga juda o’xshash oddiy almashtirish rejimi, DES, AESga xos rejimlardan biroz farqli bo’lgan gammalashtirish, teskari bog’lanishli gammalashtirish rejimlari va ulardan tamoyilli farqli imitoqistirma ishlab berish rejimidan foydalanadi.

GOST 28147-89 algoritmi DESga nisbatan ancha yuqori kriptobardoshlilikni ta’minlaydi. Bu kungacha u eng samarali hisoblangan differensial va chiziqli kriptotahlil usullariga nisbatan yetarli darajada kriptobardoshli sanaladigan algoritmlardan biridir. Bu asosan, DESga nisbatan uzun, ya’ni 256 bitli kalitdan va S-bloklarga tegishli deyarli 354 bit (S-blok generasiyalovchilar va foydalanuvchilar guruhidan o’zgalar uchun) maxfiy ma’lumotdan foydalanilishi bilan izohlanadi.

**AES** algoritmida kirish va chiqish bloklari uzunligi *128* bit shifrlash kalitining uzunligi *128*, *192* yoki *256* bit etib belgilandi.

Shifrlashda qo’llaniladigan barcha almashtirishlar yoyilish va tarqalish tamoyillarini amalga oshirishga qaratilgan. Standartda blok va kalitning uzunligiga bog’liq ravishda bosqich (raund)lar soni 10 dan 14 gacha belgilab qo’yildi.

Shifrlash prosedurasi bosqich kalitlarini generasiyalash prosedurasini ham, bosqichlar soniga mos uzunlikdagi shifrmatnga o’girish (dastlabki matnga o’girish) uchun bosqich kalitlarini yuklashni ham o’z ichiga oladi.

Shifrmatnni dastlabki matnga o’girish amallarni inversiya (teskari) tarzida bajarish orqali amalga oshiriladi.

Hozirgi kungacha AES yuqori kriptobardoshlilikka ega bo’lgan shifrlar qatoriga kiradi.

**IDEA** – yana bir *64*-bitli blokli shifrlash algoritmi bo’lib, kalitining uzunligi *128* bitga teng [11, 25]. IDEA shifrining birinchi varianti Ksuyedji Lay va Djeyms Massi tomonidan *1990* yilda taklif etilgan. U tezligi bo’yicha DES algoritmidan qolishmaydi, kriptotahlilga bardoshliligi jihatidan esa undan ham ustun.

IDEAda dastlabki matnni shifrmatnga o’girish va shifrmatnni dastlabki matnga o’girishda yagona algoritmdan foydalaniladi.

IDEA algoritmida ham boshqa blokli shifrlash algoritmlaridagi kabi aralashtirish va yoyish tamoyillari yetarli darajada amalga oshirilgan. Uning asosida “turli algebraik gruppalarning amallarini birlashtirish” falsafasi yotadi. Unda uch algebraik gruppa aralashtirilgan va ularning barchasi ham qurilma, ham dastur ko’rinishida oson amalga oshiriladi.

Shifrni ochish amali ham xuddi shifrlash amali kabi bajariladi, bunda faqat qism kalitlar biroz o’zgartiriladi.

**FEAL** algoritmi yapon mutaxassislari Akixiro Shimuzu va Shodji Miyaguchi tomonidan taklif etilgan bo’lib, unda kirish va chiqishda *64*-bitli bloklardan va *64*-bitli kalitdan foydalaniladi [11, 25]. Uning maqsadi DESga nisbatan kuchli algoritm yaratishdan iborat bo’lgan, lekin pirovardida bu algoritm boshlang’ich maqsaddan uzoqlashib ketgan.

**FEAL** algoritmi differensial va chiziqli kriptotahlilga nisbatan yetarli kriptobardoshlilikni ta’minlay olmaganligi ma’lum [11, 25]. Shu bois, uasosan kriptotahlilchilar orasida mashhur, chunki kimda-kim yangi kriptotahlil usulini yaratsa, uni avvalo **FEAL** algoritmi uchun sinab ko’rishi odat tusiga kirgan.

**O‘z DSt 1105:2005** va **O‘z DSt 1105:2009** «Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Ma’lumotlarni shifrlash algoritmi» (MShA)da modul arifmetikasining diamatrisalar algebrasidan foydalaniladi, bunda hisoblashning qiyinlik darajasi matrisalar algebrasidagi singari bajariladi [23, 28].

Shifrmatnga o’girish va dastlabki matnga o’girish proseduralarida foydalaniladigan diamatrisalar algebrasining asosiy amali diamatrisani *p* modul bo’yicha diamatrisaga teskarilash amali hisoblanadi. Bu amallarda ikki o’lchamli seans kaliti massivining maxsus tuzilmali *4*x*4* tartibli kvadrat diamatrisa bilan aks ettiriluvchi qismlari ishtirok etadi. Maxsus tuzilmali diamatrisaning muhim xossasi diamatrisaning diaaniqlovchisini hisoblash formulasining soddaligidir, bu esa diamatrisani teskarilash shartlarini tekshirish ishlarini soddalashtiradi.

Maxsus tuzilmali diamatrisani teskarilash shartlarini tekshirish MShA parametrlariga qo’yiladigan asosiy talab hisoblanadi. MShAda shuningdek butun sonlarni parametrli ko’paytirish, teskarilash va darajaga oshirish deb atalgan parametrli gruppa amallaridan ham foydalaniladi. MShA belgilab qo’yilgan ikki xil - *256* va *512* bit uzunlikdagi kalitlar yordamida amalga oshiriladi.

Barcha yuqorida bayon etilgan GOST 28147-89dan boshqa algoritmlar bo’yicha ma’lumotlarni shifrlashda 5 xil ish rejimini qo’llash mumkin [27]: elektron kod kitobi; shifr bloklarning ilashishi; chiqish orqali teskari bog’lanish; shifrmatn orqali teskari bog’lanish (teskari bog’lanishli gammalashtirish); sanoqchi. Tabiiyki, har bir ish rejimining o’ziga xos afzalligi va kamchiligi bo’ladi. Masalan, kalitlarni shifrlashda elektron kod kitobi ish rejimini, alohida belgilar uchun shifr matn orqali teskari bog’lanish ish rejimini, aloqa tizimida (odatda, biror shifrmatnni takror uzatish imkoniyati bo’lmaganda) chiqish orqali teskari bog’lanish ish rejimini qo’llash qulay hisoblanadi.

Simmetrik kriptotizimlarda, shifrlashning ikki tarmog’i: *oqimli* va *blokli* simmetrik shifrlash algoritmlari mavjud. Har ikkala turdagi simmetrik shifrlash algoritmlari ham ma’lumotlarni shifrlashda va deshifrlashda yagona kalitdan foydalanadi. Ularning o’zaro farqi esa ma’lumotlarni shifrlash va deshifrlash jarayonini amalga oshirish tartibida bo’lib, foydalanilayotgan tizim xususiyatidan kelib chiqqan holda tanlanadi.

Simmetrik kriptotizimlar bilan batafsil tanishishdan oldin, quyidagi belgilanishlarni bilish zarur:

* Ochiq matn ni simmetrik kalit bilan shifrlash:
* Shifrmatn ni simmetrik kalit bilan deshifrlash:

Bu yerda, va lar mos ravishda simmetrik kriptotizimdagi shifrlash va deshifrlash funksiyalari.

**Oqimli simmetrik shifrlash tizimlari**

Simmetrik oqimli shifrlash algoritmining yaratilishi bir martali bloknotga asoslangan bo’lib, undan farqli jihati – bardoshligi yetarlicha kichik (va boshqariladigan) kalitga asoslanishigadir. Ya’ni, kichik uzunlikdagi kalitdan ochiq matn uzunligiga teng bo’lgan ketma-ketlik hosil qilinadi va bir martali bloknot sifatida foydalaniladi.

Oqimli shifr bitli kalit ni qabul qiladi va ochiqmatnni uzunligiga teng bo’lgan ga uzaytiradi. Ketma – ketlik esa ochiq matn bilan amalida qo’shiladi va shifrmatn hosil qilinadi. Bu o’rinda ketma-ketlikni qo’shish bir martali bloknotni qo’shish kabi bir xil bo’ladi.

Oqimli shifrni quyidagicha sodda ko’rinishda yozish mumkin:

,

Bu yerda, kalit va esa natijaviy ketma-ketlik. Shuni esda saqlash zarurki, bu yerda ketma-ketlik shifrmatn emas, balki bir martali bloknotga o’xshash oddiy qator.

Agar berilgan ketma-ketlik va ochiq matn berilgan bo’lsa, mos bitlarni XOR amalida qo’shish orqali shifrmatn bitlari ni quyidagicha hosil qilamiz:

Shifrmatn ni deshifrlash uchun, yana ketma-ketlik dan foydalaniladi:

Yuboruvchi va qabul qiluvchini bir xil oqimli shifrlash algoritmi va kalit bilan ta’minlash orqali, ikkala tomonda bir xil ketma-ketliklarni hosil qilish mumkin. Biroq, natijaviy shifr kafolatli xavfsizlikka ega bo’lmaydi va bunda asosiy e’tibor amaliy tomondan qo’llashga qaratiladi.

**Blokli simmetrik shifrlash algoritmlari**

Takroriy amalga oshiriluvchi blokli shifrlash ochiq matnni fiksirlangan (o’zgarmas uzunlikdagi) bloklarga ajratadi va shifrmatnning fiksirlangan uzunlikdagi bloklarini hosil qiladi. Aksariyat blokli simmetrik shifrlar loyihasida, shifrmatn - ochiq matnni funksiya orqali biror miqdordagi *raund*lar soni davomida takroran bajarish orqali olinadi. Oldingi raunddan chiqqan natija va kalit ga asoslangan funksiya – *raund funksiyasi* deb nomlanadi. Bunday nomlanishiga asosiy sabab, uni ko’plab raundlar davomida bajarilishidir.

Blokli simmetrik shifrlarni yaratishdagi asosiy maqsad – bu xavfsizlik va samaradorlikga erishishdir. Xavfsiz yoki samarali bo’lgan blokli shifrlarni yaratish murakkab muammo emas, biroq, ham xavfsiz ham samarali bo’lgan simmetrik blokli shifrlarni yaratish – bu *san’atdir*.

Simmetrik blokli shifrlarni yaratishda ko’plab *tarmoqlardan* foydalaniladi. Ular orasida quyidagi tarmoqlar amalda keng qo’llaniladi:

1. Feystel tarmog’i.

2. SP (Substitution – Permutation network) tarmoq.

3. Lai-Messey tarmog’i.

Ma’ruzaning davomida Feystel tarmog’i va unga asoslangan sodda blokli simmetrik shifr bilan tanishib o’tiladi.

Feystel tarmog’i - bu aynan bir blokli shifr hisoblanmay, simmetrik blokli shifrni loyihalashning umumiy prinsipi sanaladi. Feystel tarmog’iga ko’ra ochiq matn bloki teng ikki chap va o’ng qismlarga bo’linadi:

,

va har bir raund uchun yangi chap va o’ng tomonlar quyidagi qoidaga ko’ra hisoblanadi:

Bu yerda, kalit – raund uchun *qismkalit* (raund kaliti) hisoblanadi. Qism kalitlar esa o’z navbatida kalit dan biror *kalit generatori* algoritmi orqali hisoblanadi. Yakuniy, shifrmatn bloki esa oxirgi raund natijalariga teng bo’ladi, ya’ni:

.

Feystel tarmog’ida deshifrlash XOR amalining “sehrgarligi”ga asoslanadi. Ya’ni, lar uchun quyidagi tenglik amalga oshiriladi:

Oxirgi raund natijasi, deshifrlangan matnni beradi:

Har bir raundda foydalaniluvchi Feystel tarmog’ining funksiyasi qaytuvchi (teskari funksiyasiga ega) bo’lishi talab etilmaydi. Biroq, olingan har qanday funksiya to’liq xavfsiz bo’la olmaydi.

Simmetrik kriptotizmlar. Simmetrik kriptotizmlarda axborot almashish uch bosqichda yuz beradi:

* axborot junatuvchi uni oluvchiga o‘zaro mahfiy kalitni, ya’ni ikkovlaridan o‘zga hech kimga ma’lum bo‘lmagan kalitni topshiradi;
* jo‘natuvchi o‘zaro maxfiy kalit bilan axborotni shifrlab uni oluvchiga jo‘natadi;
* qabul qilib oluvchi axborotni olib uning shifrini o‘zaro maxfiy kalit bilan ochadi.

Umuman olganda ikkala tomon bu kalitdan bir necha bor qayta foydalanishlari mumkin.

Shu kalitdan aloqa uchun qayta foydalanilganda yoki kalit axborot egasining o‘zi ishlatadigan matnni shifrlash uchun tuzilgan bo‘lsa, albatta, shifrlanadigan axborot miqdori bilan teng kalitdan foydalanish har doim ham qulay bo‘lavermaydi, birinchi bosqichga hojat bo‘lmaydi. Agar har kuni va har bir aloqa seansi uchun yangi noyob kalit ishlatilsa, kriptotizmning xavfsizligi yuqoriroq bo‘ladi.

Nosimmetrik kriptotizmlar algoritmlari. Nosimmetrik kriptotizmlarda axborot almashish qo‘yidagi bosqichlarda yuz beradi:

* axborot qabul qilib oluvchi tomon uni tayyorlab junatuvchiga o‘zining shaxsiy oshkora kaliti ma’lum bo‘lishiga erishadi;
* bu kalit boshqa kimsalarga ham ma’lum qilinishi mumkin;
* junatuvchi tomon axborotni uni qabul qilib oluvchining shaxsiy oshkora kaliti bilan Shifrlab uni oluvchiga junatadi;
* qabul qilib oluvchi tomon shifrlangan axborotni olib, uning shifrini uzining shaxsiy maxfiy kaliti bilan ochadi.

Bu shifrlangan axborotni oshkora kalit egasidan o‘zga xech kim ocha olmaydi, chunki ularda bunga mos mahfiy kalit yo‘q.

Umuman olganda, bitta oshkora kalitdan bir necha kishi ko‘p marotaba foydalanib, yagona manzilga-shu oshkora kalit egasiga turli axborotlar jo‘natishlari mumkin. Ko‘pchilik shu oshkora kalitdan uning egasi raqamli imzo chekkan xujjatlarning unga tegishli ekaniga ishonch hosil qilish maqsadida ham foydalanishi mumkin. Chunki, bu oshkora kalit bilan faqatgina uning egasi o‘z mahfiy kaliti bilan imzolagan xujjatlardagi imzolarnigina Shifrini ochish mumkin.

**1.3. Kriptotizmlarni elektron raqam tizimida ishlatilishi**

Elektron raqamli imzo axborot-kommunikasiya tarmog’ida almashinadigan hujjatli ma’lumotlar va ularning manbalarini haqiqiy yoki haqiqiy emasligini aniqlash masalasini, ya’ni ma’lumotlar autentifikasiyasi masalasining yechimini ta’minlovchi kriptografik vosita hisoblanadi.

Har qanday qog’ozli yozma xat yoki hujjatning oxirida shu hujjatni tuzuvchisi yoki tuzish uchun javobgar bo’lgan shaxsning imzosi bo’lishi tabiiy holdir. Imzo quyidagi ikkita maqsaddan kelib chiqib qo’yiladi. Birinchidan, ma’lumotni olgan tomon o’zida mavjud imzo namunasiga olingan ma’lumotdagi imzoni solishtirib, imzoning haqiqiy yoki soxtaligiga ko’ra shu ma’lumotning haqiqiy yoki soxta ekanligini aniqlaydi. Ikkinchidan, shaxsiy imzo ma’lumot hujjatining yuridik maqomini ta’minlaydi. Bunday kafolat esa savdo–sotiq, ishonchnoma, majburiyat va shu kabi bitimlarda alohida muhimdir.

Qog’ozli hujjatlarga qo’yilgan shaxsiy imzolarni soxtalashtirish nisbatan murakkab. Chunki shaxsiy imzo faqat uning muallifi tafakkurining o’ziga xos bo’lgan ko’pqirrali tomonlari mahsulidir. Shuning uchun bunday imzo muallifini hozirgi zamonaviy ilg’or kriminalistika uslublaridan foydalanish orqali aniqlash mumkin.

Axborot-kommunikasiya tarmog’ida almashinadigan elektron hujjatli ma’lumotlar ham qog’ozli hujjat almashinuvidagi an’anaviy shaxsiy imzo vazifasini bajaruvchi kabi elektron raqamli imzo bilan ta’minlanib, elektron hujjat va uning manbasini haqiqiy yoki haqiqiy emasligini aniqlash masalasi yechimini hal etilishini talab etadi.

**Elektron raqamli imzo algoritmlarining umumiy kriptografik xossalari**

Elektron raqamli imzo qog’ozli hujjat almashinuvidagi an’anaviy shaxsiy imzo xususiyatlaridan farqli bo’lib, ikkilik sanoq tizimi xususiyatlari bilan belgilanadigan xotira registrlari bitlariga bog’liq. Xotira bitlarining ma’lum bir ketma-ketligidan iborat bo’lgan elektron imzoni ko’chirib biror joyga qo’yish yoki o’zgartirish kompyuterlar asosidagi aloqa tizimlarida murakkablik tug’dirmaydi.

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

Elektron raqamli imzo aloqa tizimlarida bir necha tur qoida buzilishlaridan muhofaza qilinishni ta’minlaydi, ya’ni:

- foydalanuvchi (B) tomonidan qabul qilib olingan elektron hujjatga qo’yilgan raqamli imzoning haqiqiy yoki haqiqiy emasligini faqat (A) - foydalanuvchining ochiq kaliti bilan ta’minlangan shaxsiy kalit faqat o’zidan boshqa shaxsga ma’lum bo’lmasligi, ma’lumotni faqat (A) - foydalanuvchi tomonidan jo’natilganligini rad etib bo’lmaydi;

- qonunbuzar (raqib tomon) shaxsiy kalitni bilmagan holda modifikasiyalash, soxtalashtirish, faol modifikasiyalash, niqoblash va boshqa shu kabi aloqa tizimi qoidalarining buzilishiga imkoniyat tug’dirmaydi;

- aloqa tizimidan foydalanuvchilarning o’zaro bog’liq holda ish yuritishi munosabatidagi ko’plab kelishmovchiliklarni bartaraf etadi va bunday kelishmovchiliklar kelib chiqqanda vositachisiz aniqlik kiritish imkoniyati tug’iladi.

Ko’p hollarda uzatilayotgan ma’lumotlarni shifrlashga hojat bo’lmay, uni elektron raqamli imzo bilan tasdiqlash kerak bo’ladi. Bunday holatlarda ochiq matn jo’natuvchining yopiq kaliti bilan shifrlanib, olingan shifrmatn ochiq matn bilan birga jo’natiladi. Ma’lumotni qabul qilib olgan tomon jo’natuvchining ochiq kaliti yordamida shifrmatnni deshifrlab, ochiq matn bilan solishtirishi mumkin.

1991 yilda AQShdagi Standartlar va Texnologiyalar Milliy Instituti DSA raqamli imzo algoritmining standartini DSS yuqorida keltirilgan El Gamal va RSA algoritmlari asosida yaratib, foydalanuvchilarga taklif etgan.

ERI axborot-kommunikasiya tarmog’ida elektron hujjat almashinuvi jarayonida quyidagi uchta masalani yechish imkonini beradi:

- elektron hujjat manbasining haqiqiyligini aniqlash;

- elektron hujjat yaxlitligini (o’zgarmaganligini) tekshirish;

- elektron hujjatga raqamli imzo qo’ygan subyektni mualliflikdan bosh tortmasligini ta’minlash.

Har qanday ERI algoritmi ikkita qismdan iborat bo’ladi:

* imzo qo’yish;
* imzoni tekshirish.

Imzo qo’yish muallif tomonidan, faqat unga ma’lum bo’lgan shaxsiy kalit bilan amalga oshiriladi. Imzoning haqiqiyligini tekshirish esa istalgan shaxs tomonidan, imzo muallifining ochiq kaliti bilan amalga oshirilishi mumkin.

**1.4. Xesh funksiyalar**

Xeshlash funktsiyasi (xesh-funktsiyasi) shunday o’zgartirishki, kirish yo’liga uzunligi o’zgaruvchan xabar M berilganida chiqish yo’lida belgilangan uzunlikdagi qator h(M) hosil bo’ladi. Boshqacha aytganda, xesh-funktsiya h(.) argument sifatida uzunligi ixtiyoriy xabar (xujjat) M ni qabul qiladi va belgilangan uzunlikdagi xesh-qiymat (xesh) H=h(M)ni qaytaradi.

Xeshlash funktsiyasi quyidagi xususiyatlarga ega bo’lishi lozim:

- Xesh-funktsiya ixtiyoriy o’lchamli argumentga qo’llanishi mumkin.

- Xesh-funktsiya chiqish yo’lining qiymati belgilangan o’lchamga ega.

- Xesh-funktsiya  h(x) ni ixtiyoriy "x" uchun yetarlicha oson hisoblanadi. Xesh funktsiyani hisoblash tezligi shunday bo’lishi kerakki, xesh-funktsiya ishlatilganida elektron raqamli imzoni tuzish va tekshirish tezligi xabarning o’zidan foydalanilganiga qaraganda anchagina katta bo’lsin.

4.     Xesh-funktsiya matn M dagi orasiga qo’yishlar (vstavki), chiqarib tashlashlar (vыbrosы), joyini o’zgartirishlar va h. kabi o’zgarishlarga sezgir bo’lishi lozim.

5.     Xesh-funktsiya qaytarilmaslik xususiyatiga ega bo’lishi lozim.

6.     Ikkita turli xujjatlar (ularning uzunligiga boђliq bo’lmagan holda) xesh-funktsiyalari qiymatlarining mos kelishi ehtimolligi juda kichkina bo’lishi shart, ya’ni hisoblash nuqtai nazaridan h(x')=h(x) bo’ladigan x'≠ xni topish mumkin emas.

Elektron raqamli imzo va uning zamonaviy turlari

Elektron xujjatlarni tarmoq orqali almashishda ularni ishlash va saqlash xarajatlari kamayadi, qidirish tezlashadi.Ammo, elektron xujjat muallifini va xujjatning o’zini autentifikatsiyalash, ya’ni muallifning xaqiqiyligini va olingan  elektron xujjatda o’zgarishlarning yo’qligini aniqlash muammosi paydo bo’ladi.

Elektron xujjatlarni auentifikatsiyalashdan maqsad ularni mumkin bo’lgan jinoyatkorona xarakatlardan himoyalashdir. Bunday xarakatlarga quyidagilar kiradi:

-         faol ushlab qolish - tarmoqqa ulangan buzg’unchi xujjatlarni (fayllarni) ushlab qoladi va o’zgartiradi.

-         Maskarad-abonent S xujjatlarni abonent V ga abonent A nomidan yuboradi;

-         renegatlik-abonent A abonent V ga xabar yuborgan bo’lsada, yubormaganman deydi;

-         almashtirish-abonent V xujjatni o’zgartiradi, yoki yangisini shakillantiradiva uni abonent A dan olganman deydi;

-         takrorlash - abonent A abonent V ga yuborgan xujjatni abonent S takrorlaydi.

Jinoyatkorona xarakatlarning bu turlari o’z faoliyatida kompyuter axborot texnologiyalaridan foydalanuvchi bank va tijorat tuzilmalariga, davlat korxona va tashkilotlariga  xususiy shaxslarga ancha- muncha zarar yetkazishi mumkin.

Elektron raqamli imzo metodologiyasi xabar yaxlitligini va xabar muallifining xaqiqiyligini tekshirish muammosini samarali hal etishga imkon beradi.

Elektron raqamli imzo telekommunikatsiya kanallari orqali uzatiluvchi matnlarni autentifikatsiyalash uchun ishlatiladi. Raqamli imzo ishlashi bo’yicha oddiy qo’lyozma imzoga o’xshash bo’lib, quyidagi afzalliklarga ega:

- imzo chekilgan matn imzo qo’ygan shaxsga tegishli ekanligini tasdiqlaydi;

- bu shaxsga imzo chekilgan matnga bog’liq majburiyatlaridan tonish imkoniyatini bermaydi;

  - imzo chekilgan matn yaxlitligini kafolatlaydi.

Elektron raqamli imzo-imzo chekiluvchi matn bilan birga uzatiluvchi qo’shimcha raqamli xabarning nisbatan katta bo’lmagan  sonidir.

  Elektron raqamli imzo asimmetrik shifrlarning qaytaruvchanligiga hamda xabar tarkibi, imzoning o’zi va kalitlar juftining o’zaro bog’liqligiga asoslanadi. Bu elementlarning xatto birining o’zgarishi raqamli imzoning haqiqiyligini tasdiqlashga imkon bermaydi. Elektron raqamli imzo shifrlashning asimmetrik algoritmlari va xesh-funktsiyalari yordamida amalga oshiriladi.

Elektron raqamli imzo tizimining qo’llanishida bir- biriga imzo chekilgan elektron xujjatlarni jo’natuvchi abonent tarmog’ining mavjudligi faraz qilinadi. Har bir abonent uchun juft - mahfiy va ochiq kalit generatsiyalanadi.  Mahfiy kalit abonentda sir saqlanadi va undan abonent elektron  raqamli imzoni shakllantirishda foydalanadi.

Ochiq kalit boshqa barcha foydalanuvchilarga ma’lum bo’lib, undan imzo chekilgan elektron xujjatni qabul qiluvchi elektron raqamli imzoni tekshirishda foydalanadi.

Elektron raqamli imzo tizimi ikkita asosiy muolajani amalga oshiradi:

-raqamli imzoni shakllantirish muolajasi;

-raqamli imzoni tekshirish muolajasi.

Imzoni shakllantirish muolajasida xabar jo’natuvchisining maxfiy kaliti ishlatilsa, imzoni tekshirish muolajasida jo’natuvchining ochiq kalitidan foydalaniladi.

Elektron raqamli imzo tizimining printsipial jihati— foydalanuvchining elektron raqamli imzosini uning imzo chekishdagi maxfiy kalitini bilmasdan qalbakilashtirishning mumkin emasligidir. SHuning uchun imzo chekishdagi maxfiy kalitni ruxsatsiz foydalanishdan ximoyalash zarur. Elektron raqamli imzoning maxfiy kalitini, simmetrik shifrlash kalitiga o’xshab, shaxsiy kalit elituvchisida, himoyalangan  holda saqlash tavfsiya etiladi.

Imzo chekiluvchi faylga joylashtiriluvchi elektron raqamli imzo imzo chekilgan xujjat muallifini identifikatsiyalovchi qo’shimcha axborot-ga ega. Bu axborot xujjatga elektron raqamli imzo hisoblanmasidan oldin qo’shiladi. Har bir imzo quyidagi axborotni o’z ichiga oladi:

- imzo chekilgan sana;

- ushbu imzo kaliti ta’sirining tugashi muddati;

- faylga imzo chekuvchi shaxs xususidagi axborot (F.I.SH., mansabi, ish joyi);

- imzo chekuvchining indentifikatori (ochiq kalit nomi);

- raqamli imzoning o’zi.

Elektron raqamli imzoning qator algoritmlari ishlab chiqilgan. 1977 yilda AQSH da yaratilgan RSA tizimi  birinchi va dunyoda mashhur elektron raqamli imzo tizimi hisoblanadi va yuqorida keltirilgan printsiplarni amalga oshiradi. Ammo raqamli imzo algoritmi  RSA  jiddiy kamchilikka  ega. U niyati buzuq odamga maxfiy kalitni bilmasdan, xesh-lash natijasini imzo chekib bo’lingan xujjatlarning xeshlash  natijalarini ko’paytirish orkali hisoblash mumkin bo’lgan xujjatlar imzosini shakllantirishga imkon beradi.

**II BOB MA’LUMOTLARNI XAVFSIZ ALMASHISH JARAYONIDA OPENSSL KUTUBXONASIDAN FOYDALANISH**

**2.1. Axborot almashish tizimlarida assimmetrik kriptotizimlar ahamiyati**

Assimetrik shifrlash algoritmi, ma'lumotni shifrlash va de-shifrlash uchun ikki farqli kalitdan foydalanishni ta'minlaydi. Bu algoritmda, bir xil kalitdan foydalanish bilan ishlovchi xavfsizlik algoritmlariga nisbatan yuqori darajada xavfsizlik ta'minlanadi.

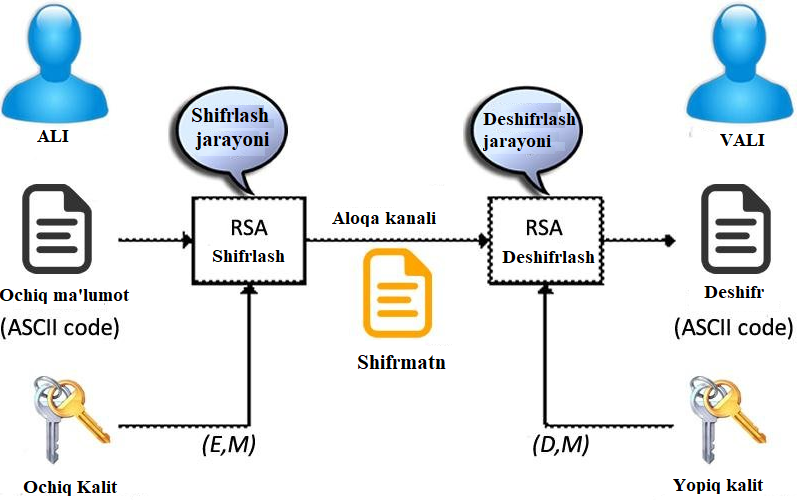
Assimetrik shifrlashning ikki asosiy elementi bor: shaxsiy xususiyatlarga ega bo'lgan kalitlardan biri "asosiy kalit" (private key) deb ataladi, ikkinchisi esa "ochiq kalit" (public key) deb ataladi.

Asosiy kalit shaxsiy va maxfiy bo'lib, shifrlash va de-shifrlash jarayonida foydalaniladi. Ochiq kalit esa xavfsiz bo'lishi lozim bo'lgan ma'lumotlarni shifrlash uchun foydalaniladi va ommaviy ravishda tarqatiladi.

Assimetrik shifrlashning eng mashhur algoritm turlari quyidagilardir:

1. RSA (Rivest-Shamir-Adleman): eng ko'p ishlatiladigan algoritmlardan biridir. Xavfsizlik kaliti uzunligi va shifrlash jarayonida ishlatiladigan matn uzunligi to'g'risidagi bog'lovchi sanoq yuqori darajada.
2. Diffie-Hellman: mahalliy tarmoqlar o'rtasida xavfsiz kalit almashinuvi yaratish uchun ishlatiladi.
3. Elliptik kengaytma algoritmi (Elliptic Curve Cryptography, ECC): avvalgi algoritmlarga nisbatan xavfsizlik darajasi yuqori, va shifrlash uchun ishlatiladigan xavfsizlik kalitlarining uzunligi juda kam.

Assimetrik shifrlash algoritmlari bir qancha tizimlar va protokollar uchun xavfsizlikni ta'minlashda ishlatiladi, masalan: SSL/TLS, SSH, S/MIME, PGP tizimlarda ishlatiladi.Quyida assimmetrik shifrlash algoritmi sxemasi ko’rsatilgan



*2.1-rasm. Assimmetrik shifrlash algoritmi ko’rinishi*

**RSA shifrlash algoritmi**

Assimetrik shifrlash algoritmi, 1970-yillarda James H. Ellis, Clifford Cocks va Malcolm J. Williamson tomonidan ishlab chiqilgan. Lekin, eng mashhur algoritmlardan biri olan RSA algoritmi 1977-yilda Ron Rivest, Adi Shamir va Leonard Adleman tomonidan ishlab chiqilgan.

Bu algoritm ilk uchta, matematikning bir qancha bo'limlaridan foydalanadi, masalan: arifmetik, algebra, nisbiylik va ma'lumotlar teorisi.

RSA algoritmi asosan hukumat va banklar kabi tashkiliyotlar tomonidan ma'lumotlarni xavfsiz ravishda o'tkazish uchun ishlatilgan. Shu bilan birga, SSL/TLS, SSH, PGP, S/MIME kabi tizimlar va protokollar ham RSA algoritmini ishlatishadi.

RSA (Rivest-Shamir-Adleman) shifrlash algoritmi, ikki foydalanuvchi orasidagi maxfiy xabarlar almashinuvini maxfiy tarzda amalga oshirish uchun ishlatiladigan bir shifrlash usuli hisoblanadi. Bu algoritm 1977 yilda Ron Rivest, Adi Shamir va Leonard Adleman tomonidan yaratilgan. Bu algoritmning asosida maxfiylikning ochiq kalitlarni ishlatish (public key cryptography) va maxfiy kalitlarni ishlatish(private key cryptography) uchun ikki farqli kalitlarni ishlatish asosida ishlaydi.

RSA shifrlash algoritmi quyidagi bosqichlarga ega:

1. Ikki tub son tanlash: p va q. Bu tub sonlar juda katta bo'lishi kerak. p va q bilan n = p \* q hisoblanadi.
2. Ф(n) hisoblanadi: Ф(n) = (p-1) \* (q-1)
3. E ni tanlash: E - sonini topamiz, bu son Ф(n) bilan 1 dan farqli biror umumiy bo’luvchiga ega bo’lmaganson.
4. D ni topish: E\*D(mod Ф(n))=1 shartni qanoatlantiruvchi *D* soni, Bu tenglikdan D soni topiladi.
5. Public key va Private key hosil qilish: Public key (E, n) kalitlar juftligi va Private key (D, n) kalitlar juftligiga ega bo'lish kerak.
6. Maxfiy xabarlar shifrlash: Xabarining har bir harfi ASCII kodida sonlarga aylanadi, keyin C = MEmod(N) formula orqali shifrlash amalga oshiriladi, bu yerda M ASCII kodida aylantirilgan ma’lumot.
7. Maxfiy xabarlar deshifrlash: D = CDmod(N) formula orqali deshifrlash amalga oshiriladi

Misol: Uchta harfdan iborat bo’lgan “ABC” ma’lumotini shifrlaymiz.

Biz qulaylik uchun kichik tub sonlardan foydalanamiz Amalda esa mumkin qadar katta tub sonlar bilan ish ko’riladi.

1. Tub bo’lgan p=17 va *q*=11 sonlarini tanlab olamiz.
2. Ushbu *n=p\*q*=17\*11=187 sonini aniqlaymiz.

So’ngra, sonini topamiz, hamda bu son bilan 1 dan farqli biror umumiy bo’luvchiga ega bo’lmagan *e* sonini, misol uchun *e*=19 sonini, olamiz.

1. Yuqorida keltirilgan e\*d(mod)=1 shartni qanoatlantiruvchi *d* sonini 19\**d*=1 (mod 160) tenglikdan topamiz. Bu son *d*=59
2. Shifrlanishi kerak bo’lgan «YIL» ma’lumotini tashkil etuvchi harflarni: A→89, B→73, C→79 mosliklar bilan sonli ko’rinishga o’tkazib olib, bu ma’lumotni musbat butun sonlarning, ketma-ketligidan iborat deb qaraymiz. U holda ma’lumot (89,73,79)ko’rinishda bo’ladi va uni {e;n}={19;187} ochiq kalit bilan  bir tomonli funksiya bilan shifrlaymiz:

*x*=89 da C1=(8919)(mod187)=166

*x*=73 da C2=(7319) (mod187)=74,

*x*=79 da C3=(7919) (mod187)=87.

1. Bu olingan shifrlangan (166,74,87) ma’lumotni mahfiy {*d;n*}={59;187} kalit bilan  ifoda orqali deshifrlaymiz:

*u*=166 da D1=(16659) (mod187)=89,

*u*=74 da D2=(7459) (mod187)=73,

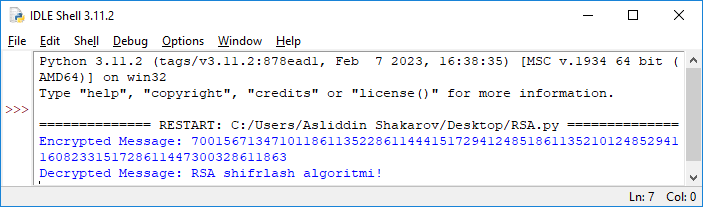
*u*=87 da D3=(8759) (mod187)=79.

RSA algoritmi maxfiylikning ochiq kalitni ishlatadi, bu xabar tarqatuvchi tomon tomonidan amalga oshiriladi. Xabar ochiq kalitli maxfiylik bilan shifrlanadi, keyin xabar qabul qiluvchi tomon uning maxfiy kaliti bilan shifrlanganini maxfiylikni ochiq qilish yordamida ochib ko'radi.

RSA shifrlash algoritmi dasturi ko'p tilli dasturlash tilida yozilgan bo'lib, bu masalada Python tilida yozilgan oddiy dasturni ko'rib chiqamiz:

|  |
| --- |
| import random  # Funksiyalar  def gcd(a, b):  while b != 0:  a, b = b, a % b  return a  def xgcd(a, b):  x0, x1, y0, y1 = 1, 0, 0, 1  while b != 0:  q, a, b = a // b, b, a % b  x0, x1 = x1, x0 - q \* x1  y0, y1 = y1, y0 - q \* y1  return a, x0, y0  def generate\_keypair(p, q):  n = p \* q  Ф = (p-1) \* (q-1)  e = random.randrange(1, Ф)  g = gcd(e, Ф)  while g != 1:  e = random.randrange(1, Ф)  g = gcd(e, Ф)  d = xgcd(e, Ф)[1]  if d < 0:  d += Ф  return (e, n), (d, n)  def encrypt(pk, plaintext):  key, n = pk  cipher = [pow(ord(char), key, n) for char in plaintext]  return cipher  def decrypt(pk, ciphertext):  key, n = pk  plain = [chr(pow(char, key, n)) for char in ciphertext]  return ''.join(plain)  # Kalitlarni generatsiya qilish  p = 61  q = 53  public\_key, private\_key = generate\_keypair(p, q)  # Xabarni shifrlash  message = 'RSA shifrlash algoritmi!'  encrypted\_message = encrypt(public\_key, message)  print('Encrypted Message:', ''.join([str(x) for x in encrypted\_message]))  # Xabarni qaytarish  decrypted\_message = decrypt(private\_key, encrypted\_message)  print('Decrypted Message:', decrypted\_message) |

Natija:



*1.2.2-rasm. RSA shifrlash dasturi natijasi*

**2.2. Openssl kutubxonasi shifrlash algoritmlari tahlili**

OpenSSL kutubxonasi, shifrlash va kriptografiya uchun turli algoritmlarni o'z ichiga oladi. Barcha algoritmlar kriptografiya amaliyotlarida ishlatilishi mumkin. OpenSSL kutubxonasi kriptografiya tahlil qilinadigan qator asosiy shifrlash algoritmlarini o'z ichiga oladi:

1. Asimmetrik (kichik-katta kalitli) algoritmlar:
   * RSA (Rivest-Shamir-Adleman): Bu algoritm ochiq va maxfiy kalitlarni generatsiya qilish, ma'lumotni shifrlash va de-shifrlash uchun ishlatiladi. RSA kalitlarining o'lchami va kriptografiya amaliyotlarining tezligi konfiguratsiya qilinadi.
   * DSA (Digital Signature Algorithm): DSA, elektron imzo uchun ishlatiladi va xavfsizlik darajasi yuqori bo'lgan bir asimmetrik algoritm hisoblanadi.
   * Elliptic Curve Cryptography (ECC): ECC kalitlarining generatsiya qilish, ma'lumotni shifrlash va imzolash uchun ishlatiladi. U samarali va xavfsizlik darajasining yuqori bo'lishi bilan ajralib turadi.
2. Simmetrik (o'zaro kalitli) algoritmlar:
   * AES (Advanced Encryption Standard): AES, xavfsiz va samarali blok shifrlash uchun ishlatiladi. U 128, 192 yoki 256 bitlik kalitlarni qabul qiladi va ma'lumotni shifrlash va de-shifrlash amaliyotlarini bajaradi.
   * DES (Data Encryption Standard): DES kalitlarini qabul qiladi va 64 bitlik bloklar bo'yicha ma'lumotni shifrlaydi. Qo'shimcha tarzda Triple DES (3DES) ham ishlatilishi mumkin.
   * Blowfish: Bu algoritm, bloklar bo'yicha shifrlash uchun ishlatiladi va kalitning uzunligi 32 dan 448 bitgacha bo'lishi mumkin.
   * RC4: RC4 algoritmi, asosan stream shifrlash uchun ishlatiladi va shifrlangan ma'lumotni xorlash asosida amalga oshiriladi.

Bundan tashqari, OpenSSL kutubxonasi shifrlash uchun boshqa algoritmlarni ham o'z ichiga oladi. Batafsil ma'lumot va tahlillar uchun, OpenSSL dokumentatsiyasiga murojaat qilish tavsiya etiladi.

**2.3. Openssl kutubxonasi imkoniyatlari asosida ishlab chiqilgan kriptografik vositalar**

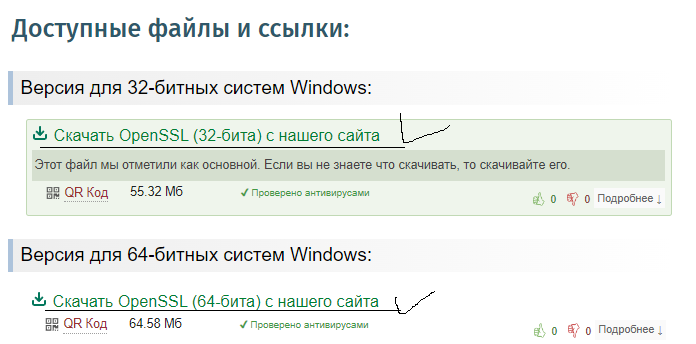
OpenSSL kutubxonasining imkoniyatlari asosida kriptografik vositalar yaratish mumkin. OpenSSL, kriptografiya bilan bog'liq turli amaliyotlar uchun o'zlashtirilgan funksiyalarni o'z ichiga oladi. Bundan foydalanib, quyidagilarni kiritish mumkin:

1. SSL/TLS protokollari: OpenSSL kutubxonasida xavfsiz kommunikatsiya o'rnatish uchun Transport Layer Security (TLS) protokollari va undan avvalgi Secure Sockets Layer (SSL) protokollari kuzatiladi. Bu protokollarni ishlatib, server va mijozlar o'rtasidagi ma'lumot almashinuvini shifrlash va xavfsizlikni ta'minlash mumkin.
2. Xavfsizlik sertifikatlarini ishlab chiqish: OpenSSL kutubxonasida X.509 standarti asosida xavfsizlik sertifikatlari generatsiya qilish va ularga mos kriptografik operatsiyalarni bajarish imkoniyati mavjud. Bu, veb saytlarda TLS/SSL sertifikatlari ishlab chiqish uchun foydalaniladi.
3. Asimmetrik shifrlash: OpenSSL kutubxonasida RSA, DSA va ECC algoritmlari orqali asimmetrik shifrlash amaliyotlari o'tkaziladi. Kalitlarni generatsiya qilish, ma'lumotni shifrlash, de-shifrlash va imzolash uchun ushbu algoritmlardan foydalanish mumkin.
4. Simmetrik shifrlash: OpenSSL kutubxonasida AES, DES, Blowfish va boshqa simmetrik shifrlash algoritmlari mavjud. Ular orqali ma'lumotni shifrlash va de-shifrlash amaliyotlarini amalga oshirish mumkin.
5. Hash funktsiyalari: OpenSSL kutubxonasida turli hash funktsiyalari, masalan, MD5, SHA-1, SHA-256, SHA-512 va boshqalar mavjud. Bu funktsiyalarni ishlatib, ma'lumotni intizomli yoki intizomsiz tartibda tekislik belgilash uchun foydalanish mumkin.
6. Digitallashtrish (Digital Signature): OpenSSL kutubxonasi digitallashtrish algoritmlarini ham o'z ichiga oladi. Bu, ma'lumotlar va hujjatlar uchun elektron imzo yaratish imkoniyatini beradi. Algoritmlar, asimmetrik shifrlash protokollari bilan birga ishlatiladi va ma'lumotning autentifikatsiyasini ta'minlash uchun foydalaniladi.
7. Randomlik generatsiyasi: OpenSSL, xavfsiz tasodifiy sonlar (random sonlar) generatsiyasi uchun ham imkoniyatlar beradi. Tasodifiy sonlar, kriptografik protokollarda kalitlarni generatsiya qilish, nonce (biror ishoraga tegishli bitta mazkur son) yaratish va tasodifiylikni ta'minlash uchun kritik ahamiyatga ega.
8. Kriptografik algoritmlarning performansini o'rganish: OpenSSL kutubxonasi imkoniyatlari orqali, kriptografik algoritmlarning samaradorligi va ishlab chiqarish yuqoriligi bilan bog'liq ma'lumotlarni o'rganish imkoniyatiga ega. Bu, kriptografiya protokollarini va algoritmlarini ta'minlash, boshqarish va optimallashtirishda yordam beradi.
9. P2P (Peer-to-Peer) kriptografiya: OpenSSL kutubxonasi, P2P kriptografiya bo'yicha ham imkoniyatlar beradi. Bu protokollar, bir-biriga bog'liq tarmoqlarda ma'lumot almashishda xavfsizlikni ta'minlash, autentifikatsiya qilish va asimmetrik kalitlardan foydalanishni o'z ichiga oladi.

**III BOB. OPENSSL KUTUBXONASIDAN FOYDALANGAN HOLDA XAVFSIZ MA’LUMOT ALMASHISHNI JORIY QILISH**

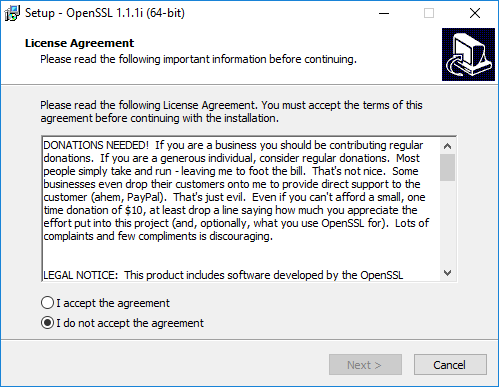
**3.1. Openssl kutubxonasi imkoniyatlari asosida xavfsiz ma`lumot almashish jarayonini tashkil etish bosqichlari**

OpenSSL kutubxonasi ochiq dastur hisoblanadi. Buning uchun GOOGLE, YANDEX yoki o’zingiz shaxsiy kompyuteringiz brouzeridan quyidagi havola orqali <https://soft.mydiv.net/win/download-OpenSSL.html> ko’chirib olish mumkin.

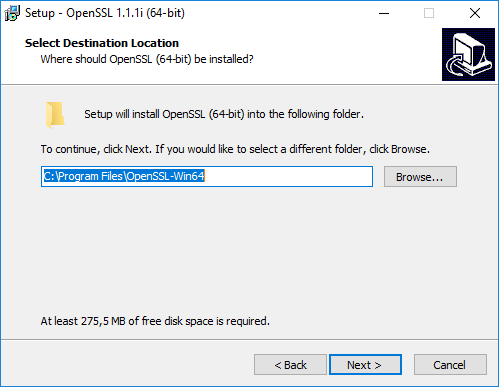


*3.1.1-rasm. OpenSSL dasturini ko’chirib olish jarayoni*

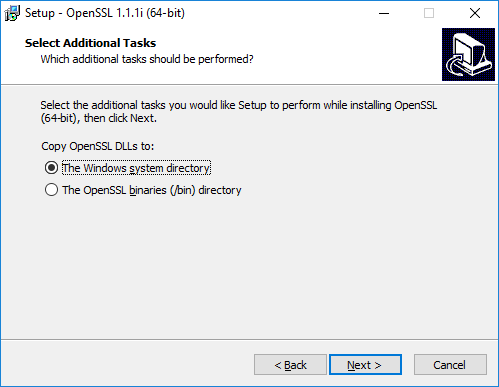
Openssl dasturini ko’chirib olgandan so’ng uni kompyuterimizga o’rnatib olamiz. Buning uchun quyidagi amallarni bajaramiz.



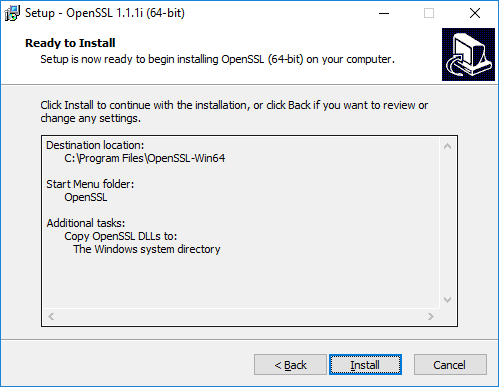
*3.1.2-rasm. OpenSSL dasturi o’rnatilish jarayoni*



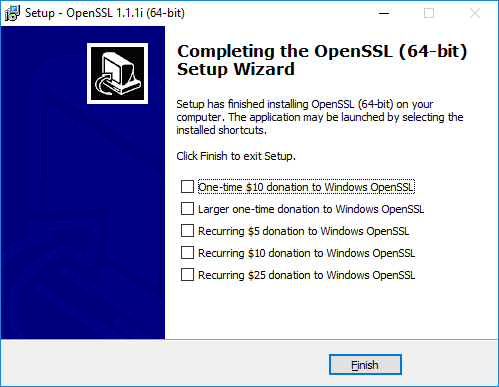
*3.2.3-rasm. OpenSSL dasturi o’rnatilish jarayoni*



*3.1.4-rasm. OpenSSL dasturi o’rnatilish jarayoni*

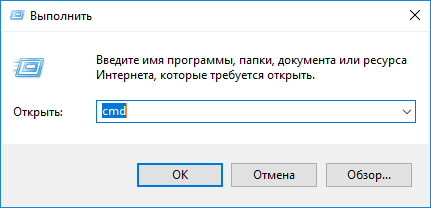


*3.1.5-rasm. OpenSSL dasturi o’rnatilish jarayoni*

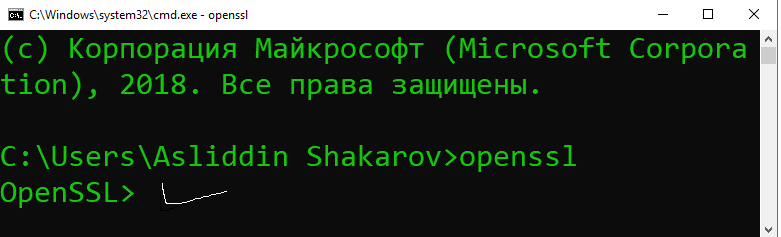


*3.1.6-rasm. OpenSSL dasturi o’rnatilish jarayoni*

OpenSSL dasturini o’rnatib bo’ldik.Keyingi bosqichda Openssl dasturini shaxsiy kompyuter CMD buyruqlar qatori bilan bog’lab olishimi kerak, ya’ni biz shifrlash buyruqlarini CMD buyruqlar qatorida bajaramiz. Ya’ni cmd buyruqlar qatoriga openssl commandasini bajarganimizda openssl buyruqlar qatori ishga tushishi lozim. 5-rasm.



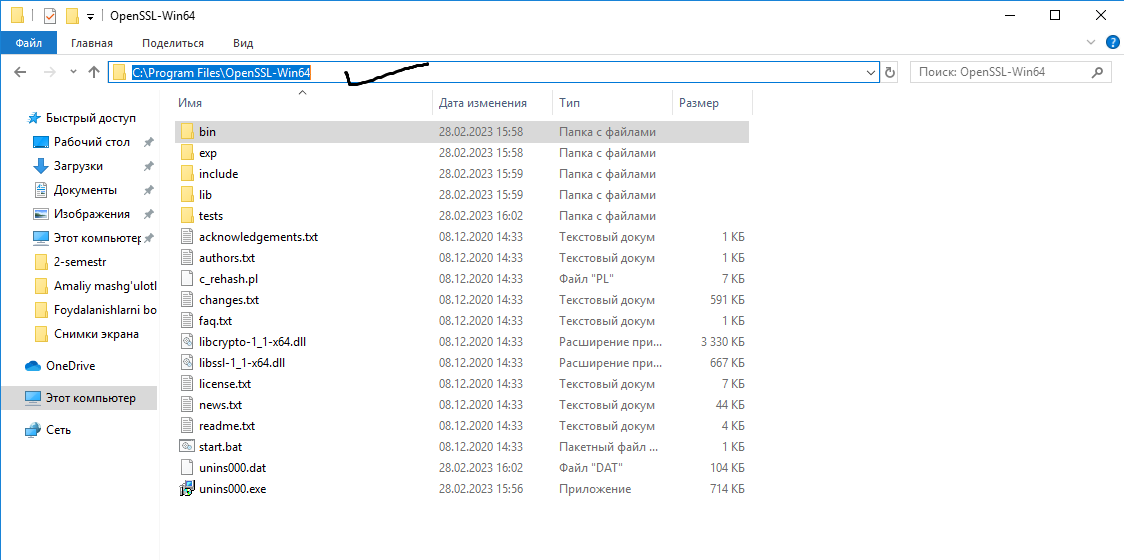
*3.1.7-rasm. “Cmd” buyruqlar satriga o’tish*



*3.1.8-rasm. “Cmd” buyruqlar satriga openssl kutubxonasini aktiv holati*

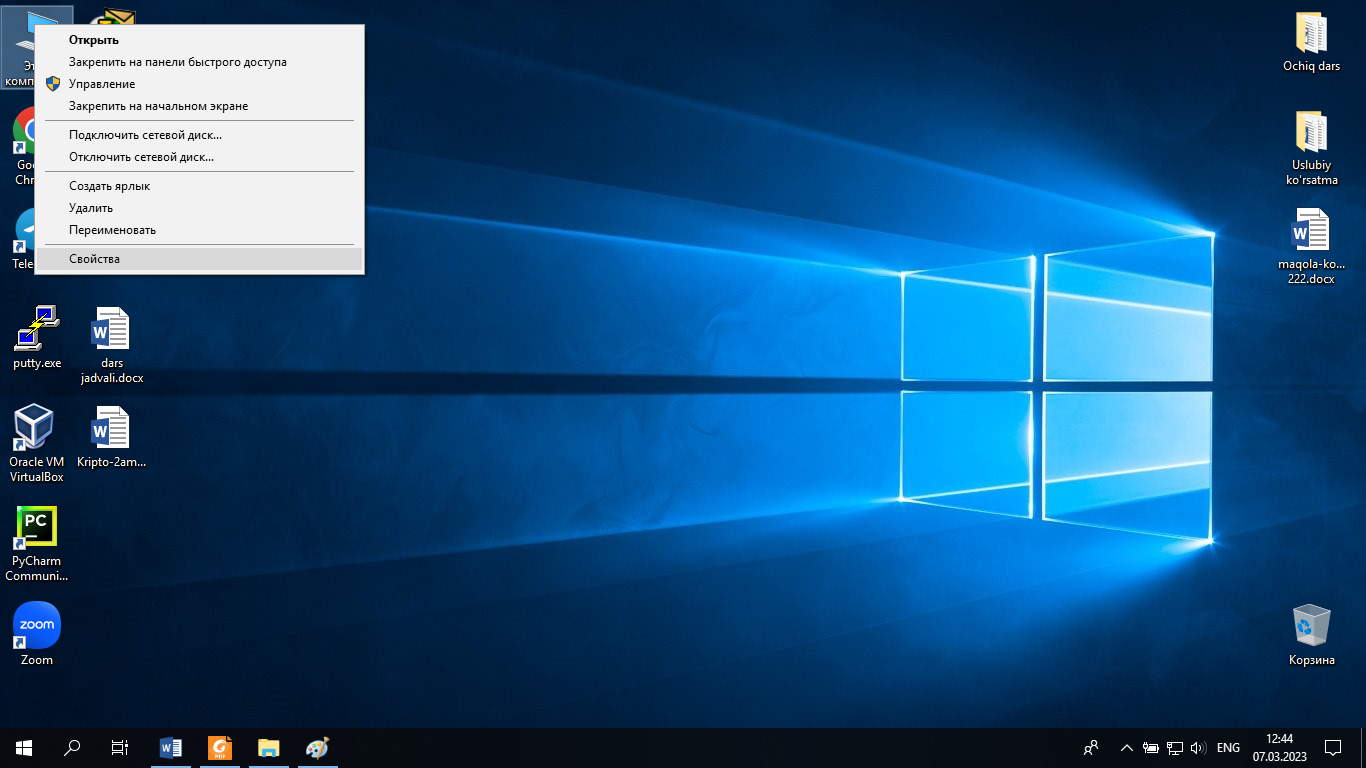
Buning uchun shaxsiy kompyuterimizning OpenSSL dasturi o’rnatilgan “bin.exe” fayli turgan manzildan nusxa olib komyuterimizga «переменные среды» bo’limining “path” qismiga o’tkazib olamiz. Buning uchun quyidagi amallarni bajaramiz.

1. Birinchi navbatda bin.exe fayli turgan yo’lidan nusxa olamiz. **C:\Program Files\OpenSSL-Win64/**

****

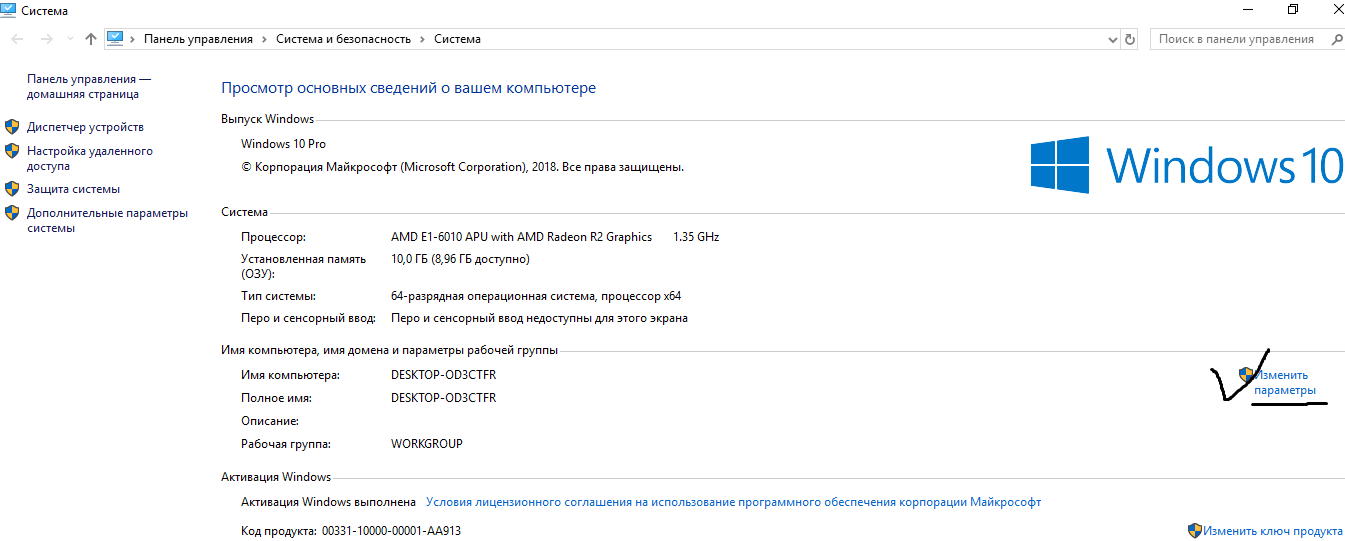
*3.1.9-rasm. Kompyuterga o’rnatilgan OpenSSL dasturini“bin.exe” faylining joylashgan joyi manzili*

1. Kompyuterimiz sichqonchasi “Этот компьютер” ustiga olib borib o’ng tomonini bosib “Свойтсва” bo'limiga o’tishimiz lozim.



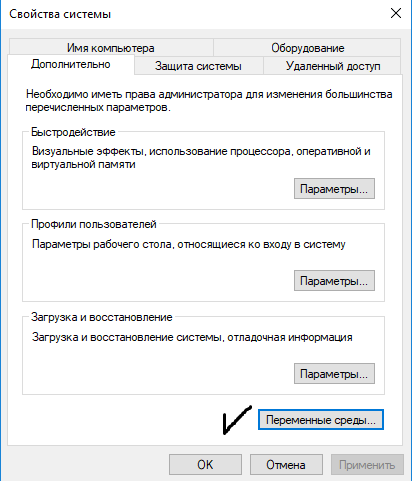
*3.1.10-rasm. Cmd buyruqlar satrida Openssl kutubxonasini aktiv holatga keltirishda bajarilgan ishlar ketma-ketligi*

1. “Изменить параметры” bo’limi tanlanadi.



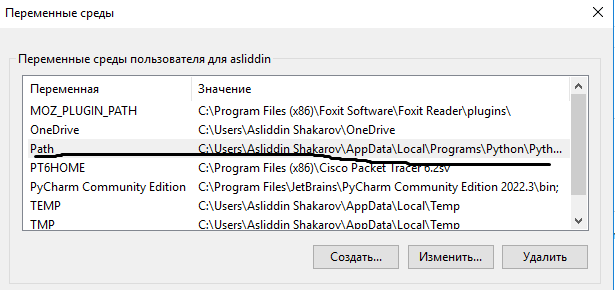
*3.1.11-rasm. Cmd buyruqlar satrida Openssl kutubxonasini aktiv holatga keltirishda bajarilgan ishlar ketma-ketligi*

1. “Дополнительно” bo’limi undan keyin “Переменные среды” bo’limiga o’tiladi.



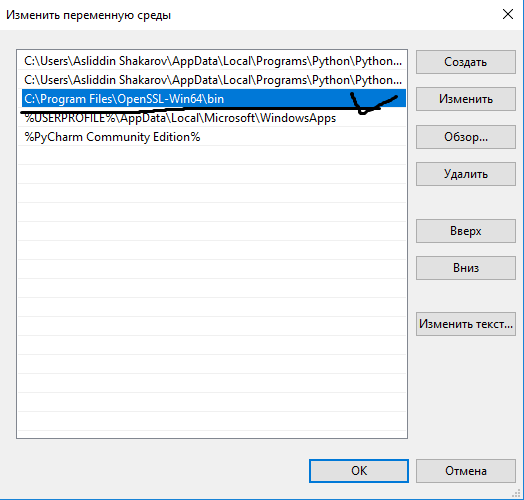
*3.1.12-rasm. Cmd buyruqlar satrida Openssl kutubxonasini aktiv holatga keltirishda bajarilgan ishlar ketma-ketligi*

1. “Path” bo’limi tanlanadi.



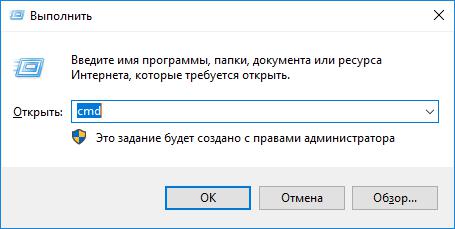
*3.1.13-rasm. Cmd buyruqlar satrida Openssl kutubxonasini aktiv holatga keltirishda bajarilgan ishlar ketma-ketligi*

1. Ko’chirib olingan bin.exe fayli yo’li ko’chirilib o’tkaziladi.



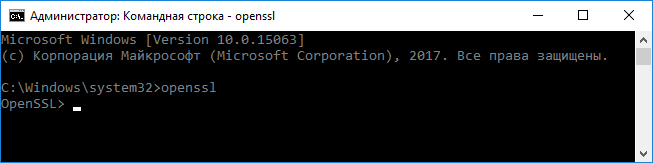
*3.1.14-rasm. Cmd buyruqlar satrida Openssl kutubxonasini aktiv holatga keltirishda bajarilgan ishlar ketma-ketligi*

Demak OpenSSL kutubxonasidan cmd buyrug‘idan foydalanishni tekshirish uchun (Windows va R birgalikda bosiladi):



*3.1.15-rasm. Cmd buyrug’ini ishga tushirish*

cmd buyruqlar satriga OpenSSL buyrug‘i kiritiladi. Bunda OpenSSL buyruqlar satriga o‘tiladi. “OpenSSL version” buyrug‘ini kiritish orqali OpenSSL versiyasini bilish mumkin. OpenSSL buyruqlarini ko‘rish uchun esa “help” buyrug‘ini kiritish mumkin.



*3.1.16-rasm. OpenSSL buyrug‘ini ishga tushirish*

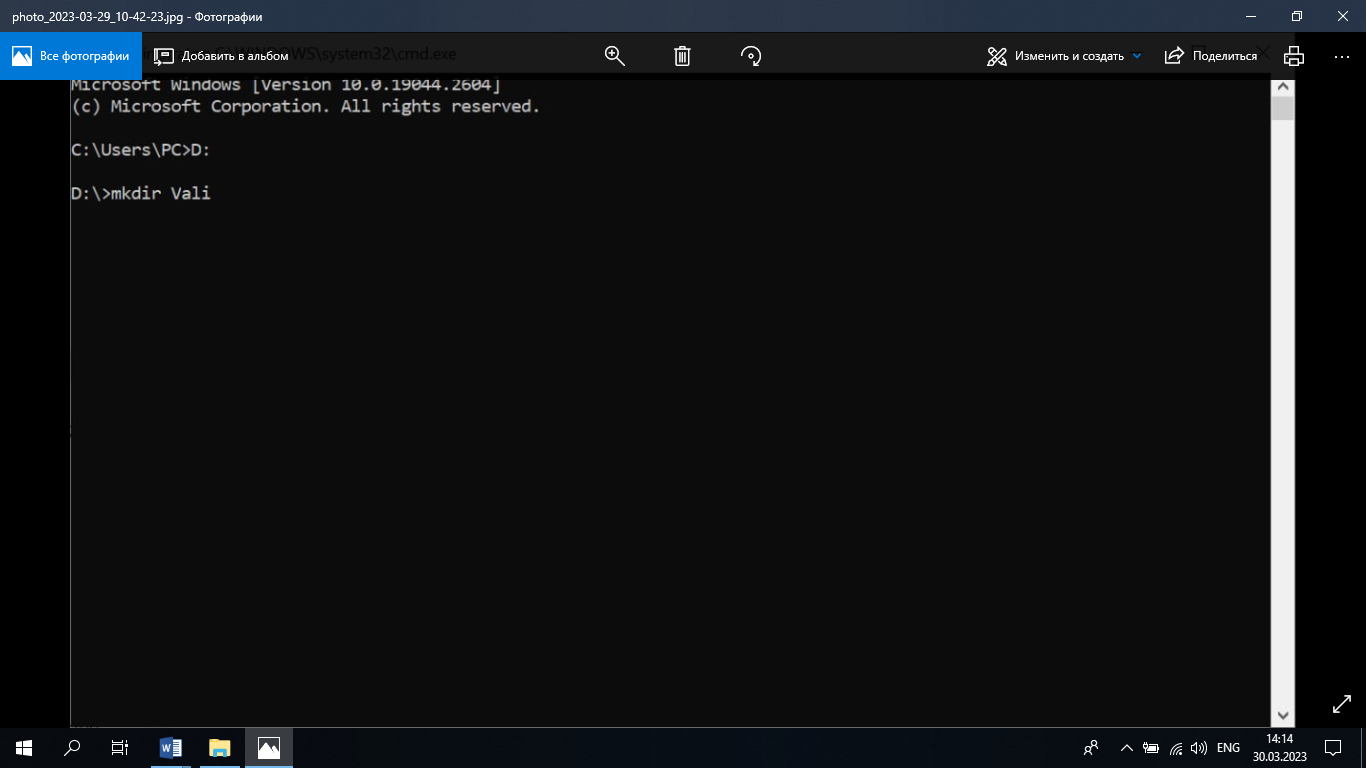
“Cmd” buyruqlar satrida openssl kutubxonamiz buyruqlar satri ishladi. Endi mana shu joyda shifrlash kommandalari bilan ma’lumotlarimiz shifrlasak bo’ladi.

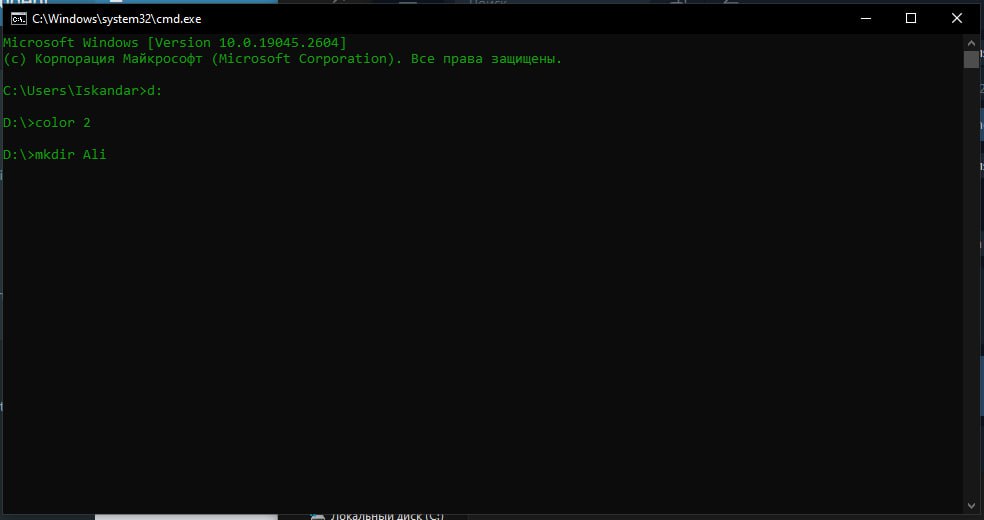
**3.2. Openssl kutubxonasidan foydalangan holda xavfsiz ma’lumot almashishni joriy qilish**

Faraz qilaylik Ali va Vali ma’lumotlarini xavfsiz almashmoqchi bo’lishmoqda. Buning uchun ular xavfsiz shifrlash algoritmidan foydalanishmoqchi. Bu RSA shifrlash algoritmidir. RSA shifrlash algoritmini OpenSSL kutubxonasidan foydalangan holda shifrlashni amalga oshiradi. O’zlarining shaxsiy kompyuterlariga yuqorida ko’rsatilganidek OpenSSL kutubxonasini o’rnatib olishgan. Keyingi qadamda quyida keltirilgan ketma ketliklarni amalga oshirishadi.

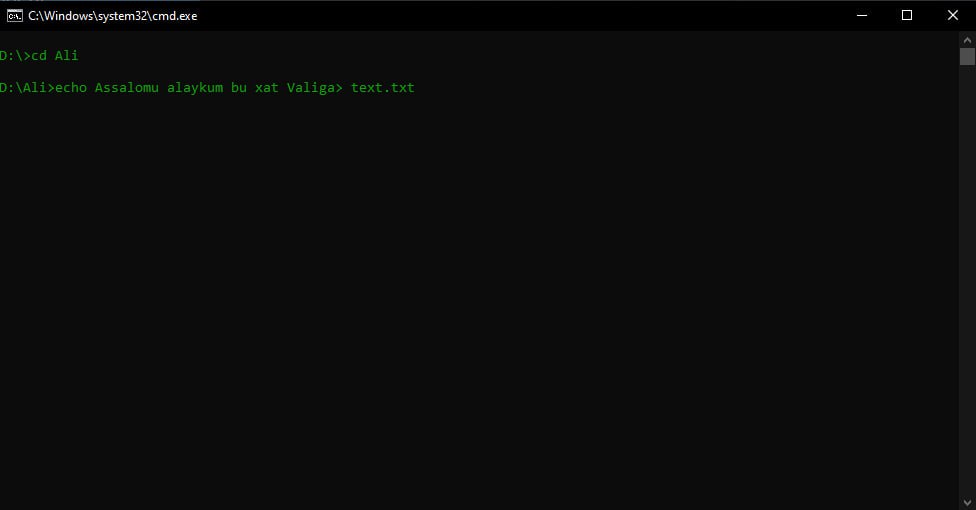
**1-qadam: kalit juftlarini yaratish**

Dastlab Ali va Vali ma’lumotlarini xavfsiz almashtirmoqchi bo’lishidan oldin Ali Vali o’zining shaxsiy kompyuterlariga Papka yaratib oladi. Papka ichiga o’zining Vali Aliga yubormoqchi bo’lgan faylini yaratadi.

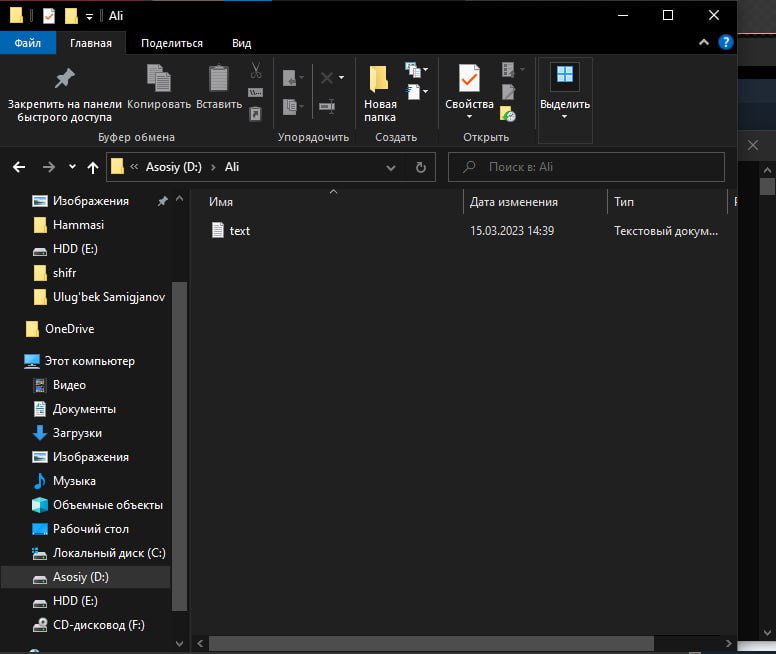


*3.2.1-rasm. Yubormoqchi faylni yaratish jarayoni*

*3.2.2-rasm. Yubormoqchi faylni yaratish jarayoni*



*3.2.3-rasm. Yubormoqchi faylni yaratish jarayoni*

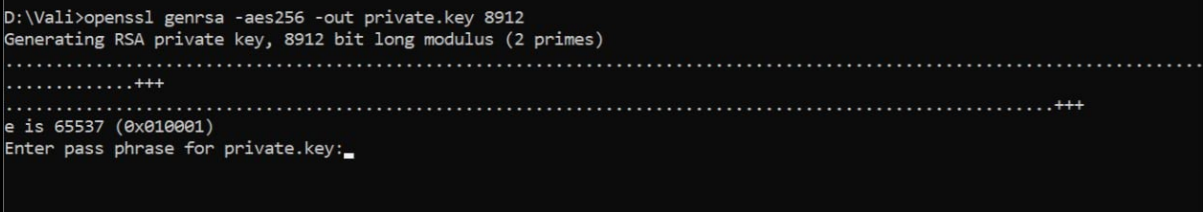
*3.2.4-rasm. Yubormoqchi faylni yaratish jarayoni*

Fayllarni shifrlashdan oldin bir juft kalit yaratish kerak. Bundan tashqari kalit Openssl kutubxonasidan foydalangan holda kalit yaratiladigan paytda parol ham qo’yilishi kerak. Qo’yilgan ushbu parolingizni eslab qoling.

Birinchi navbatda Ali va Vali ochiq kalit va yopiq kalit juftliklarini quyidagi komanda bilan yaratadi:

*openssl genrsa -aes256 -out private.key 8912*

*openssl rsa -in private.key -pubout -out public.key*

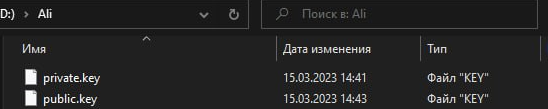
 Ushbu buyruq 4096-bit umumiy/maxfiy kalit juftligini yaratish uchun OpenSSL-ning [genrsa buyrug'idan foydalanadi.](https://www.openssl.org/docs/man1.0.2/man1/genrsa.html)Bu RSA algoritmi assimetrik bo'lgani uchun mumkin. Shuningdek, u Ali genrsa yordamida yaratadigan shaxsiy kalitni shifrlash uchun simmetrik kalit algoritmi aes128 dan foydalanadi. Buyruqni kiritgandan so'ng, OpenSSL Elisdan har safar kalitlardan foydalanmoqchi bo'lganida kiritishi kerak bo'lgan parol iborasini so'raydi:

*3.2.5-rasm. Shaxsiy kalit yaratish jarayoni*



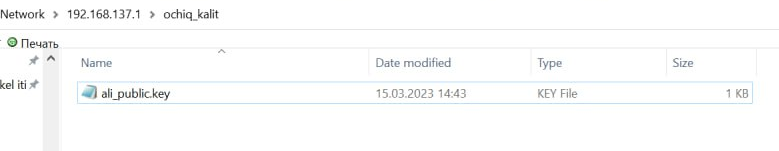
*3.2.6-rasm. Ochiq kalit yaratish jarayoni*

Ali va Vali ham o’zining shaxsiy kalitlar juftligini yaratib oldi



*3.2.7-rasm. Ochiq va Yopiq kalitlar*

E’tibor qiling Vali ma’lumotini Aliga yubormoqchi bunda Ali o’zining ochiq kalitini Valiga yuboradi.



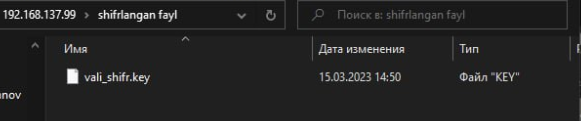
*3.2.8-rasm. Ali o’zining ochiq kalitini Valiga yuborish jarayoni*

Vali Alining ochiq kaliti yordamida o’z ma’lumotini shifrlab Aliga yuboradi.



*3.2.9-rasm. Vali ma’lumotini shifrlash jarayoni*

Vali o’zining shifrlangan faylini Aliga yuboradi.



*3.2.10-rasm. Vali shifrlangan ma’lumotni Aliga yuborish jarayoni*

Ali o’zining shaxsiy kaliti yordamida ma’lumotni deshifrlab oladi.



*17-rasm. Shifrlangan ma’lumotni Ali o’zining shaxsiy kaliti bilan deshifrlash jarayoni*

Ali Vali yuborgan shifrlangan matnni deshifrlab ochib o’qib oladi.



*3.2.11-rasm. Natija*

**3.3. Dasturiy ta’minotni yaratishda mehnat muhofazasi va texnika xavfsizligi**

Mehnat muhofaza qilishni boshqarish. Mehnat muhofaza qilishni boshqarish mazmuni va mohiyati. Davlat asosiy vazifalaridan biri-korxonalardan tartib vazirliklargacha barcha qatlamlarda mehnatni muhofaza qilish va boshqarish usullarini takomillashtirish orqali butunlay havfsiz va sog‘lom ish sharoitini yaratishdan iborat.

Xo‘jalik mexanizmining asosiy bo‘g‘ini bo‘lgan korxonada mehnatni muhofaza qilish korxonani boshqarishni biri bo‘ladi yoki podsistemasi xisoblanib, mehnatni muhofaza qilish yuqori darajada yo‘lga qo‘yilgan taqdirdagina korxona o‘z oldiga qo‘ygan vazifani muvaffaqiyatli bajara oladi.[5]

Har qanday boshqarish sistemasida avvalo obyektni mavjud va shu bilan birgalikda uni boshqaruvchi organ ham. Boshqarish jarayonida bu organ boshqarilayotgan obyektning holati va shu obyekt joylashgan muhitning holati to‘g‘risida yetarli ma’lumotga ega bo‘ladi. Shu ma’lumot asosida boshqaruvchi organ tegishli qaror qabul qiladi. Qabul qilingan qarorga asosan bir qancha ijro etuvchi organ boshqarilayotgan obyektga ta’sir ko‘rsatadi. Ba’zan boshqarish va ijro etuvchi organlar birgalikda boqarish subyektni tashkil qiladi, u holda boshqarish sistemasi ikkita podsistemadan: Boshqaruvchi va boshqariluvchi podsistemalardan iborat bo‘ladi.

Barcha hollarda boshqarish aniq maqsadga erishish uchun amalga oshiriladi. Mehnatni muhofaza qilishning maqsadi insonni mehnat jarayonida sog‘lig‘ini va ishlash qobiliyatini, uning havfsizligini ta’minlashdan iborat. Mehnat muhofazasini boshqarish obyekti bo‘lib korxonada, ishlab chiqarish uchastkalarida, g‘yexlarda, ish joylarida sog‘lom va havfsiz ish sharoitini ta’minlovchi korxona struktura bo‘linmalari va fuksional xizmatini faoliyati hisoblanadi.[5]

Korxonada mehnat muhofazasini boshqarishni korxona rahbari amalga oshiradi. Funkg‘ional xizmat va struktura bo‘linmalarida boshqaruvchi ularni rahbarlari olib boradi.

Mehnat muhofazasi boshqaruvchi sistemasini normativ va metodik asoslari /tashqi informasiya/ bo‘lib quyidagilar xizmat qiladi: mehnat qonunchiligi aktlari, hukumat qaror va topshiriqlari, normativ va normativ - texnik hujjatlar.

Mehnat muhofazasi boshqaruvchi sistemasi /MMBS/ni takomillashtirish faqat boshqarilayotgan obyektni holati to‘g‘risidagi ma’lumotga ega bo‘lingandagina mumkin. Ma’lumotlar alohida ishlab chiqarish va ish joylarida mehnat havfsizligini xarakterlovchi miqdor va sifat ko‘rsatkichlari holida qabul qilinadi.

Korxonada mehnat muhofazasi boshqaruvchi funksiyalari quyidagilar:

* mehnat muhofazasi ishlarini rejalashtirish;
* mehnat muhofazasi sohasidagi ishlarni tashkil qilish;
* mehnat muhofazasi boshqaruv sistemasini ro‘yxat va analiz qilish;
* mehnat muhofazasini va mehnat muhofazasi boshqaruvchi sistemasini holatini nazorat qilish;
* mehnat muhofazasi ishlarini takomilashtirish;

Korxonada mehnat muhofazasi boshqaruviga quyidagi asosiy vazifalar hal qilinganda erishish mumkin.

* mehnat muhofazasi savollarini tarqatish va ishchilarni mehnat havfsizligi qoidalarini o‘rganish;
* ish jihozlari havfsizligini ta’minlash;
* ishlab chiqarish jarayonlarini havfsizligini ta’minlash;
* imoratlar havfsizligini ta’minlash;
* mehnat sharoitini sanitariya gigiyena jihatidan normallashtirish;
* ishlarni shaxsiy himoya vositalari bilan ta’minlash;
* ishchilarni mehnat va dam olishni optimal rejimlari bilan ta’minlash;
* ishlarga davomat profilaktik xizmatni yo‘lga qo‘yish;
* sanitar moishiy xizmatni yo‘lga qo‘yish;
* ishlovchilarni alohida kasblar bo‘yicha saralash;

Mehnat muhofazasi ishlarini rejalashtirish. Mehnat muhofazasi boshqaruvini yetakli funkg‘iyasi bo‘lib, mehnat muhofazasi tadbirlarini rejalashtirish hisoblanadi. Rejalashtirish ishlariga qadar ishlab chiqarish travmatizmi, professional kasalliklar va boshka kursatkichlar bo‘yicha prognozlashtirish ishlari olib borilish zarur.

Ishlab chiqarish travmatizmini prognoz qilish travmatizmining bir necha yillik ko‘rsatkichlari analizi asosida olib boriladi:

Mehnat muhofazasi planlashtirish perspektiv /besh yilik/, joriy /yillik/, va operativ kvartal,oylik planlashtirishga bo‘linadi. Hozirgi paytda perspektiv planlashtirishni asosiy formasi mehnat muhofazasi va sanitar sog‘lomlashtirish ishlarini yo‘lga qo‘yishga qaratilgan. Bu planlarini joriy qilish mehnat kollektivi shartnomasini bir qismi bo‘lgan mehnat muhofazasi bo‘yicha nomenklatura tadbirlari orqali amalga oshiriladi.[5]

Jamoa shartnomada mehnatni tashkil qilishidan tartib ish sharoitini yaxshilash, ishchilarni tarbiyalash, maishiy hizmat, madaniyat ishlari o‘z aksini topadi.

Perspektiv va joriy planlar ishlab chiqarish uchastkalarida mehnat sharoitini sanitar texnik holatini analizi natijalarini hisobga olgan holda tuziladi. Shuningdek, ishlab chiqarish travmatizmini sabablari analizi, professional kasalliklar, korxona xodimlarini fikrlarini, profoyuz komiteti xodimlarini fikrlarini hisobga olinadi. Bunda sexning sanitar texnik pasporti muhim ahamiyatga ega. Sanitar – texnik pasport mehnat muhofazasi qoida va normalariga javob bermaydigan ishlab chiqarish uchastkalarini tekshirish ishlarini hujjatlashtirish uchun mo‘ljallangan.

Mehnat muhofazasi kasallari shuningdek, mehnatni va ishlab chiqarishni, boshqarishni ilmiy tashkil qilish, og‘ir qo‘l mehnati talab qiladigan ishlarni mexanizasiyalash, ayollar mehnatini muhofaza qilish, korxonalarda ishni kuzgi-qishgi mavsumga tayyorlash.[5]

Mehnat muhofazasi boshqarish sistemasini zaruriy shartlaridan bo‘lib, ma’lumotlarni qayta ishlash, saqlash, uzatish, yig‘ish, ro‘yxatga olish kabilar hisoblanadi. Bunda telefon, televizor, teletayp, mexanizasiya-ashgan avtomatlashtirilgan ma’lumotlarni qayta ishlash sistemalaridan foydalaniladi.

Ish joylarida statik elektrning razryadli toki ko‘proq kompyuterning biror bir elementiga tegib ketish natijasida xosil bo‘ladi. Bunday razryadlar insonga xavf tug‘dirmaydi, yoqimsiz ta’sirdan tashqari kompyuterni ishdan chiqishiga olib keladi. Simlar izolyatsiyasi shikastlanganda tok ta’sirini kamaytirish uchun ish xonalarining pollari bir qavatli polivinil xloridli antistatik linolium bilan qoplanishi lozim. Himoyalashni boshqa usuli ionlashtirilgan gaz bilan zaryadlarni neytrallash.

Kompyuter xonalarining kattaligi u yerda ishlovchi xodimlar va kompyuterlar soniga mos kelishi zarur. Ish joylarini tashkillashtirishga, yana xarorat, yorug‘lik, havo tozaligi, shovqindan himoyalanganlik parametrlari hisobga olinadi.

Sanitar me’yorlariga ko‘ra bir ishchi uchun ish joyining xajmi 15 m3 , ish maydoni esa 4,5 m2 dan kam bulmasligi kerak. Xonaning balandligi poldan shiftgacha 3-3,5 m bo‘lishi kerak.

Kompyuter xonalarida odatda yon tomonlama tabiiy yoritilganlik qo‘llaniladi. Tabiiy yoritilganlikda shimol yoki shimoliy-sharqqa qaratilgan yorug‘lik darchalaridan foydalanish kerak, bunda tabiiy yoritilganlik koiffitsenti 1,2-1,5 % kam bo‘lmasligi shart. Kompyuterlarni podvallarda joylashtirishga ruxsat etilmaydi.

Kompyuter xonalari va ish joylarida tabiiy yoritilganlik qo‘llanishi zarur. Boshqa xollarda esa sun’iy yoritilganlikni qo‘llash mumkin. Ish xujjatlari joylashgan stol usti yoritilganligi 300-500 lk bo‘lishi kerak.Yorug‘lik manbaini shunday joylashtirish kerakki, bunda yorug‘lik ko‘zni qamashtirmasligi kerak, ko‘rish maydonidagi yorug‘lik manbaining yorqinligi 200 kd /m2 oshmasligi kerak.

Kompyuter joyini shunday joylashtirish kerakki, bunda tabiiy yorug‘lik iloji boricha yondan tushishi lozim. Kompyuter stolining balandligi iloji boricha 680-800 mm bo‘lishi kerak. Ish stoli oyoqlar uchun balandligi 600 mm, eni 500 mm dan kam bo‘lmagan, chuqurligi tizza darajasida 450 mm dan kam bo‘lmasligi, uzatilgan oyoq darajasida 650 mm dan kam bo‘lmasligi kerak.

Ekran monitori ko‘zdan eng uzog‘i bilan 600-700 mm bo‘lishi kerak, lekin xarf va shriftlarning o‘lchamiga qarab 500 mm dan yaqin bo‘lmasligi kerak.

Xonalarni rangli jihozlanishi ishni sanitar-gigiena sharoitlarini yaxshilashga qaratiladi, ish unumini oshishiga hizmat qiladi.

Kompyuter xonalarini rangini texnik jihozlar rangi bilan bir xil rangda bo‘yash maqsadga muvofik. Xonalar va jihozlar ranglari yumshoq bo‘lishi va yaltiroq bo‘lmasligi lozim.

**Yong‘in xavfsizligi**

Elektr qurilmalari, kompyuterlardan foydalanishda turli xildagi yonishlar xavfi doim mavjuddir. Zamonaviy kompyuterlarda elektron sxemalarning elementlarini joylashish zichligi juda yuqoridir, ulash simlari, kommunakatsion kabellar bir-biriga juda yaqin joylashgan. Ulardan tok oqqanda, kata miqdorda issiqlik ajraladi, ba’zi bo‘limlarda harorat 80-100o C gacha ko‘tarilishi mumkin. Bu ularning izolyatsiya qobig‘ining erishiga, o‘tkazgich qismlarining ochilib qolishiga, oqibatda qisqa tutashuv bo‘lib, uchqun chiqishi va yonib ketishiga olib kelishi mumkin.

Ortiqcha issiqlikni yo‘qotish uchun havoni kondensionerlash va ventilyasiya tizimi xizmat qiladi. Lekin bu tizmlar mashina zallari va boshqa xonalar uchun qo‘shimcha yong‘in xavfini yuzaga keltiradi, chunki bir tarafdan, yong‘in sodir

bo‘lganda, ularni xonalarga tezda tarqalishiga yordam beradi.

Elektr qurilmalariga tok alohida yong‘in xavfi bo‘lgan kabel simlari orqali uzatiladi, yonuvchi izolyatsiya materialining mavjudligi, elektr uchquni va yaqinlashish qiyinligi kabel liniyalaridan yong‘in chiqishi va rivojlanishi ehtimoli yanada kattaligidan dalolat beradi. Shuning uchun kabel simlari yonmaydigan materiallardan tayyorlangan, olib-qo‘yiluvchi texnalogik pol ostidan o‘tishi kerak. Hisoblash markazlaridagi xonalarda yong‘in jo‘mraklari yo‘lkalarga zina maydonchalariga, kirish joylariga o‘rnatiladi. Olov o‘chirgichlari 40-50 sm2 ga bitttadan o‘rnatiladi. Yong‘in signalizatorlari va avtomatik yong‘in o‘chirish qurilmalari o‘rnatiladi.

Yng‘inlar sanoat korxonalari, xalq xo‘jaligining hamma tarmoqlari, qishloq xo‘jaligi va turar joylarda yuz berishi mumkin bo‘lgan ,etkazadigan zarari jixatidan tabiiy ofatlarga tenglashishi mumkin bo‘lgan xodisa hisoblanadi. Yong‘inlar katta moddiy zarar keltirishi bilan birga, og‘ir baxtsiz xodisalar, zaxarlanish, kuyish natijasida kishilar xayotini olib ketgan xollar ko‘plab uchraydi.

Shuning uchun ham yong‘inga qarshi kurash barcha fuqarolarning umumiy burchi hisoblanadi va bu ishlar davlat miqyosida amalga oshiriladi.

Umuman yong‘in chiqmasligini ta’minlash, yong‘in chiqqan taqdirda ham uning rivojlanib, tarqalib ketishining oldini olish, moddiy boyliklarni, inson salomatligi va uning xayotini saqlab qolishga qaratilgan chora tadbirlar bo‘lib, bu masalalar mehnatni muhofaza qilishning tarkibiy qismi hisoblanadi.

Bizning vazifamiz yongin haqida asosiy tushunchalar berish bilan birga, unga qarshi samarali kurash olib borish, yong‘inni o‘chirishda qo‘llaniladigan birlamchi vositalar, xar-xil tadbirlar bilan o‘quvchilarni tanishtirishga qaratilgan.

Yong‘inning sabablari: isitish pechlarini qurish yoki ishlatish qoidalarini buzish, ishlab chiqarish yoki uyda olovni ehtiyotsizlik bilan ishlatish, kerosin bilan ishlayotganda yoritish yoki qizdirish asboblaridan noto‘g‘ri foydalanish yoki noto‘g‘ri o‘rnatish, yashin yoki statik elektr razryadlarini ishlatish. Mashinalar va ishlab chiqarish jixozlarining nosozligi xamda ularni ishlatish qoidalariga rioya qilmaslik sabab bo‘ladi.

Yong‘inni oldini olish uchun tadbirlar: tashkiliy, texnikaviy tadbirlar qo‘llash kerak bo‘ladi.

**XULOSA**

Xulosa qilib aytganda ushbu bitiruv malakaviy ishda kriptografiya haqida umumiy tushunchalarga ega bo’ldim. Shifrlash algoritmlari haqida bilim va ko’nikmalariga ega bo’ldim. Xavfsiz ma’lumot almashishda kriptobardoshli shifrlash algoritmlaridan foydalanish uchun shifrlash algoritmlarni tahlil qilib chiqdim. Tahlillar natijasida RSA assimmetrik shifrlash algoritmini tanladim. Xavfsiz ma’lumot almashish uchun Openssl kutubxonasidan foydalandim va kutilgan natijaga erishdim.

Bitiruv malakaviy ishida yaratilgan dasturiy mahsulot elektron hujjat almashish tizimlarining elektron raqamli imzo algoritmlari uchun assimmetrik shifrlash algoritmlari ishlatilishi orqali unga ma’lum miqdorda foydalidir.

Yaratilgan dasturiy mahsulot hozirgi zamonaviy kompyuterlarda to’liq ishlash imkoniyatiga ega.

**ADABIYOTLAR RO‘YXATI**

1. O’zbekiston Respublikasi Prezidentining farmoni “O’zbekiston Respublikasini yanada rivojlantirish bo‘yicha harakatlar strategiyasi to‘g‘risida”. Toshkent sh., 2017 yil 7 fevral’, PF-4947-son. Manba: <https://www.lex.uz/acts/3107036>
2. O’zbekiston Respublikasi Prezidentining Qarori. Axborot texnologiyalari sohasida ta’lim tizimini yanada takomillashtirish, ilmiy tadqiqotlarni rivojlantirish va ularni IT-industriya bilan integratsiya qilish chora-tadbirlari to‘g‘risidaToshkent sh., 2020 yil 6 oktyabr’, PQ-4851-son. Manba: <https://lex.uz/docs/5032128>
3. O‘zbekiston Respublikasi Prezidenti Shavkat Mirziyoyevning Oliy Majlisga Murojaatnomasi. 06.01.2021. Manba: <https://uzlidep.uz/uz/news-of-uzbekistan/7998>
4. Axborot va axborotlashtirishga oid normativ-huquqiy hujjatlar to‘plami. //To‘plovchilar: A.I.O’ralov, M.I.Ishbekov, D.S.Sa’dullaev. –Toshkent, “Adolat” nashriyoti, 2008. -464 b.
5. Ulyanov S.V., Litvintseva L.V., Ulyanov S.S. Quantum information and quantum computational intelli- gence: Quantum optimal control and quantum filtering – Stability, robustness, and self-organization models in nanotechnologies. – Milan: Note del Polo (Ricerca), Universita degli Studia di Milano. – 2005. – Vol. 82.
6. Ulyanov S.V., Litvintseva L.V., Ulyanov S.S. Quantum information and quantum computational intelligence: Applied quantum soft computing in AI, quantum language and programming in computer science, quantum knowledge self-organization and intelligent wise robust control (4rd edit.). – Milan: Note del Polo (Ricerca), Universita degli Studia di Milano. – 2010. – Vol. 86.
7. Ulyanov S.V., Litvintseva L.V., Takahashi K. Fast algorithm for efficient simulation of quantum algo- rithm gates on classical computer // Systemics, Cybernetics and Informatics. – 2004. – Vol. 2. – №3. – Pp. 63-68.
8. Ulyanov S.V., Litvintseva L.V., Ulyanov S.S. Quantum information and quantum computational intelligence: Quantum probability, physics of quantum information and information geometry, quantum computational logic and quantum complexity. – Milan: Note del Polo (Ricerca), Universita degli Studia di Milano. – 2003. – Vol. 80.
9. C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (Institute of Electrical and Electronics Engineers, New York, 1984), pp. 175-179.
10. Ekert, "Quantum cryptography based on Bell's theorem", Phys. Rev. Lett. 67, 661­663 (1991).
11. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography", J. Cryptology 5, 3-28 (1992).
12. Muller, J. Breguet, and N. Gisin, "Experimental demonstration of quantum cryptography using polarized photons in optical fiber over more than 1 km", Europhysics Lett. 23, 383-388 (1993).
13. J. Breguet, A. Muller, and N. Gisin, "Quantum cryptography with polarized photons in optical fibers: experimental and practical limits", J. Mod. Opt. 41, 2405-2412 (1994).
14. Muller, H. Zbinden, and N. Gisin, "Underwater quantum coding", Nature 378, 449­449 (1995).
15. Muller, H. Zbinden, and N. Gisin, "Quantum cryptography over 23 km in installed under-lake telecom fiber", Europhysics Lett. 33, 335-339 (1996).
16. Marand and P. Townsend, "Quantum key distribution over distances as long as 30 km", Opt. Lett., 20, 1695-1697 (1995).
17. P.D. Townsend, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fiber using wavelength-division multiplexing", Electronics Lett. 33, 188-190 (1997).
18. P.D. Townsend, "Quantum cryptography on multiuser optical fibre networks", Nature 385, 47-49 (1997).
19. R. Hughes, G. Morgan, and C. Peterson, "Practical quantum key distribution over a 48-km optical fiber network", J. Mod. Opt. 47, 533-547 (2000).
20. P.A. Hiskett, G. Bonfrate, G.S. Buller, and P.D. Townsend, "Eighty kilometer transmission experiment using an InGaAs/InP SPAD-based quantum cryptography receiver operating at 1.55 Am," J. Mod. Opt. 48, 1957-1966 (2001).
21. T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka, and K. Nakamura, "Single-photon interference over 150km transmission using silica-based integrated optic interferometers for quantum cryptography", Jpn. J. Appl. Phys. 43, L1217-L1219 (2004).
22. Gobby, Z. Yuan, and A. Shields, "Quantum key distribution over 122 km of standard telecom fiber", Appl. Phys. Lett. 84, 3762-3764 (2004).
23. H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M.M. Fejer, K. Inoue, and Y. Yamamoto, "Differential phase shift quantum key distribution experiment over 105km fiber", New J. Phys. 7, 232 (2005).
24. P.A. Hiskett, D. Rosenberg, C.G. Peterson, R.J. Hughes, S. Nam, A.E. Lita, A.J. Miller, and J.E. Nordholt, "Long-distance quantum key distribution in optical fiber", New J. Phys. 8, 193 (2006).
25. Stucki, N. Gisin, O. Guinnard, G. Ribordy and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system", New Journal of Physics 4 (2002) 41.1-41.8
26. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster and J. G. Rarity "Quantum cryptography: A step towards global key distribution" , Nature. 2002. V.419. P.450.

ILOVA

*openssl genpkey -algorithm RSA -pkeyopt rsa\_keygen\_bits:2048 -pkeyopt rsa\_keygen\_pubexp:3 -out privkey-A.pem*

*openssl pkey -in privkey-A.pem -text*

*openssl pkey -in privkey-A.pem -out pubkey-A.pem -pubout*

*openssl dgst -sha1 message-A.txt*

*openssl dgst -sha1 -sign privkey-A.pem -out sign-A.bin message-A.txt*

*openssl genpkey -algorithm RSA -pkeyopt rsa\_keygen\_bits:2048 -pkeyopt rsa\_keygen\_pubexp:3 -out privkey-V.pem*

*openssl pkey -in privkey-V.pem -out pubkey-V.pem -pubout*

*openssl pkeyutl -encrypt -in message-A.txt -pubin -inkey pubkey-V.pem -out ciphertext-A.bin*

*openssl pkeyutl -decrypt -in ciphertext-A.bin -inkey privkey-V.pem -out received-V.txt*

*openssl dgst -sha1 -verify pubkey-A.pem -signature sign-A.bin received-V.txt*

*sudo yum install bind bind-utils -y*

*sudo nano /etc/named.conf*

*zone "mysite.uz" IN {*

*type master;*

*file "thegun.forward";*

*allow-update {none;};*

*};*

*zone "23.20.172.in-addr.arpa" IN {*

*type master;*

*file "thegun.reverse";*

*allow-update {none;};*

*};*

*sudo named-checkconf*

*sudo nano /var/named/asliddin.forward*

*$TTL 86400*

*@ In SOA thegun.vn. root.thegun.vn. (*

*2020110900;*

*3600;*

*1800;*

*604800;*

*86400;*

*)*

*@ IN NS thegun.vn.*

*@ IN A 172.20.23.206*

*@ IN MX 10 mail.thegun.vn.*

*mail IN A 172.20.23.205*

*www IN CNAME thegun.vn.*

*sudo named-checkzone asliddin.uz /var/named/asliddin.forward*

*sudo cp /var/named/asliddin.forward /var/named/asliddin.reverse*

*sudo nano /var/named/asliddin.reverse*

*$TTL 86400*

*@ In SOA thegun.vn. root.thegun.vn. (*

*2020110900;*

*3600;*

*1800;*

*604800;*

*86400;*

*)*

*@ IN NS thegun.vn.*

*254 IN PTR www.thegun.vn.*

*253 IN PTR mail.thegun.vn.*

*sudo named-checkzone 192.168.43.251 /var/named/asliddin.reverse*

*sudo firewall-cmd --add-service=dns --permanent --zone=public*

*sudo firewall-cmd --reload*

*sudo systemctl start named*

*sudo systemctl status named*

*sudo named-checkzone joker.vn /var/named/joker.forward*

*sudo systemctl restart named*

*sudo systemctl status named*

*sudo yum install httpd -y*

*sudo systemctl start httpd*

*sudo systemctl status httpd*

*sudo systemctl enable httpd*

*sudo firewall-cmd --add-service=http --permanent --zone=public*

*sudo dnf install php-opcache php-gd php-curl php-mysqlnd -y*

*php -v*

*sudo ls -l /etc/httpd/conf/*

*sudo nano /etc/httpd/conf/httpd.conf Oxiriga IncludeOptional sites-enabled/\*.conf*

*sudo ls -l /etc/httpd/conf/*

*sudo mkdir -p /etc/httpd/sites-available/*

*sudo mkdir -p /etc/httpd/sites-enabled/*

*sudo ls -l /etc/httpd/*

*sudo nano /etc/httpd/sites-available/asliddin.uz.conf*

*<VirtualHost \*:80>*

*ServerName www.thegun.vn*

*ServerAlias thegun.vn*

*DocumentRoot /var/www/asliddin.uz/index.php*

*</VirtualHost>*

*sudo cp /etc/httpd/sites-available/asliddin.uz.conf /etc/httpd/sites-enabled/asliddin.uz.conf*

*sudo mkdir -p /var/www/asliddin.uz/*

*sudo nano /var/www/asliddin.uz/index.php*

*<!DOCTYPE html>*

*<html lang="en">*

*<head>*

*<title>The gun</title>*

*</head>*

*<body>*

*TATU SAMARQAND FILIALI*

*</body>*