O’zbekiston Respublikasi Oliy va O’rta maxsus ta’lim vazirligi

O’zbekiston Davlat jahon tillari universiteti huzuridagi Marg’ilon ko’p tarmoqli tehnikumi

Himoyaga ruhsat berildi.

Tehnikum direktori:

T.M.Karimov.

Marg’ilon ko’p tarmoqli texnikumi

Kompyuter injineringi yo’nalishi Ⅱ-bosqich 5-20 guruh o’quvchisi Xakimova Sevaraxon A’zamovnaning

**KALIT YARATISHDA VA SAQLASHDA XAVFSIZ QURILMALARDAN FOYDALANISH**

mavzusida tayyorlagan

**Bitiruv malaka ishi**

Bitiruv malaka ish rahbari: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

**MAVZU: KALIT YARATISHDA VA SAQLASHDA XAVFSIZ QURILMALARDAN FOYDALANISH**

|  |  |
| --- | --- |
| ***REJA:***  **KIRISH………………..……………………………………….3**  **Texliliy qism.**   1. **BOB. MA'LUMOTLARNI KODLASH HAQIDA UMUMIY MA’LUMOT**    1. **Ma'lumotlarni**[**kodlash va shifrlash**](https://hozir.org/2--laboratoriya-ishi-axborotlarni-kodlashtirishga-doir-misolla.html)**…………………………6**    2. **Tasodifiy va psevdotasodifiy sonlar asosida**   **kalitlarni yaratish ………….………………...………………..12**   * 1. **Kalitlarni xavfsiz saqlash va yaratish tizimi  …………..….17**   **ASOSIY QISM**   1. **BOB. OCHIQ VA YOPIQ KALITLAR BILAN ISHLASH**    1. **Ochiq kalitlar [bilan shifrlash tizimi](https://hozir.org/reja-shifrlash-haqida-malumot-simmetrik-shifrlash-tizimi-haqid.html)……………….………...22**   **2.2. Yopiq kalitlar [bilan shifrlash tizimi](https://hozir.org/reja-shifrlash-haqida-malumot-simmetrik-shifrlash-tizimi-haqid.html)…………….…………....30**  **Xulosa ………………………………………………………….37**  **Foydalaninlgan adabiyotlar ro’yxati…………………………40** |  |

**I.KIRISH**

Davlat aktivlarini boshqarishni yanada maqbullashtirish, aloqa va axborotlashtirish sohasi tashkilotlariga yuklangan vazifalar samarali bajarilishi uchun qlulay [shart-sharoitlar yaratish](https://hozir.org/hozirgi-vaqtda-deyarli-barcha-davlatlar-axborot-sohasi-tadriji.html), ularning moddiy-texnika bazasini mustaxkamlash maqsadida ―O‘zbekiston Respublikasi Vazirlar Maxkamasi‖ tomonidan bir qancha qarorlar ishlab chiqilgan bo‘lib ushbu qarorlarning maqsadi O‘zbekisyon Respublikasi hududida axborotlashtirish sohasini rivojlantirishga xizmat qiladi. Bundan tashqari sohani rivojlantirishga qaratilgan ―O‘zbekiston Respublikаsining Аxborotlаshtirish to‘g‘risidа‖ vа ―Dаvlаt sirlаrini sаqlаsh to‘g‘risidа‖gi qonunlаrigа muvofiq, shuningdek аxborotni muhofаzа qilishning kriptogrаfik vositаlаri hаmdа kriptogrаfiya tizimlаridаn foydаlаngаn holdа mаxfiy yoki dаvlаt sirlаridаn iborаt bo‘lgаn mа‘lumotlаr bаyon etilgаn аxborotni muhofаzа qilish fаoliyatini tаrtibgа solish mаqsаdidа amalga oshiriladi..  
Huquqni muhofaza qilish faoliyatining axborot ta‘minotini jadallashuvi, tezkor vaziyatni tavfsiflovchi, ishonchli ma‘lumotlarni muntazam yig‘ib borilishi, uning o‘z vaqtida va sifatli tahlil qilinishi hozirgi sharoitda jinoyatchilikka qarshi kurashni tashkil etishning muhim shartlaridan biri hisoblanadi. Axborot jarayonlarini avtomatlashtirish kompyuter texnikasini joriy etishga, ma‘lumotlarni yig‘ish, saqlash, qayta ishlash va uning asosida ma‘lumotlarni berish avtomatlashtirilgan tizimlarini yaratishga bevosita bog‘liqdir.  
O‘zbekiston Respublikasi prezidentining 2015 yildagi ―O‘zbeksiton Respublikasi Axborot Texnologiyalari va Kommunikatsiyalarini Rivojlantirish Vazirligini yaratish haqida‖gi qarorida ―Axborot xavfsizligini ta‘minlash, mahfiy va sifatli aloqani tashkil etish ...‖ muammolari ham alohida ko‘rib chiqilishi berilgan

**«**Kriptografiya**»**atamasi dastlab «yashirish, yozuvni berkitib qo‗ymoq» ma‘nosini bildiradi. Birinchi, marta u yozuv paydo bo‗lgan davrlardayoq aytib o‗tilgan. Hozirgi vaqtda kriptografiya deganda har qanday shakldagi, ya‘ni diskda saqlanadigan sonlar ko‗rinishida yoki hisoblash tarmoqlarida uzatiladigan xabarlar ko‗rinishidagi axborotni yashirish tushuniladi. Kriptografiyani raqamlar bilan kodlanishi mumkin bo‗lgan har qanday axborotga nisbatan qo‗llash mumkin. Maxfiylikni ta‘minlashga qaratilgan kriptografiya kengroq qo‗llanilish doirasiga ega. Aniqroq aytganda, kriptografiyada qo‗llaniladigan usullaning o‗zi axborotni himoyalash bilan bog‗liq bo‗lgan ko‗p jarayonlarda ishlatilishi mumkin.

Kriptografiya axborotni [ruxsatsiz kirishdan himoyalab](https://hozir.org/kriptografiya-axborotni-ruxsatsiz-kirishdan-himoyalab-uning-ma.html), uning maxfiyligini ta‘minlaydi. Masalan, to‗lov varaqlarini elektron pochta orqali uzatishda uning o‗zgartirilishi yoki soxta yozuvlarning qo‗shilishi mumkin. Bunday hollarda axborotning ta‘minlash zaruriyati paydo bo‗ladi. Umuman olganda kompьyuter tarmog‗iga ruxsatsiz kirishning mutlaqo oldini olish mumkin emas, lekin ularni aniqlash mumkin. Axborotning yaxlitligini tekshirishning bunday jarayoni, ko‗p hollarda, axborotning haqiqiyligini ta‘minlash deyiladi. Kriptografiyada qo‗llaniladigan usullar ko‗p bo‗lmagan o‗zgartirishlar bilan axborotlarning haqiqiyligini ta‘minlashi mumkin[4].  
Nafaqat axborotning kompyuter tarmog‗idan ma‘nosi buzilmasdan kelganligini bilish, balki uning muallifdan keganligiga ishonch hosil qilish juda muhim. Axborotni uzatuvchi shaxslarning haqiqiyligini tasdiqlovchi turli usullar ma‘lum. Eng universal protsedura parollar bilan almashuvdir, lekin bu juda samarali bo‗lmagan protsedura. Chunki parolni qo‗liga kiritgan har qanday shaxs axborotdan foydalanishi mumkin bo‗ladi. Agar ehtiyotkorlik choralariga rioya qilinsa, u holda parollarning samaradorligini oshirish va ularni kriptografik usullar bilan himoyalash mumkin, lekin kriptografiya bundan kuchliroq parolni uzluksiz  
o‗zgartirish imkonini beradigan protseduralarni ham ta‘minlaydi. Kriptografiya sohasidagi oxirgi yutuqlardan biri – raqamli signatura – maxsus xossa bilan axborotni to‗ldirish yordamida yaxlitlikni ta‘minlovchi usul, bunda axborot uning muallifi bergan ochiq kalit ma‘lum bo‗lgandagina [tekshirilishi](https://hozir.org/referat-tarkibidagi-klishelangan-jumlalar-referat-matnidagi-kl.html) mumkin. Ushbu usul maxfiy kalit yordamida yaxlitlik tekshiriladigan ma‘lum usullardan ko‗proq afzalliklarga ega.

Ma‘lumotlarni shifrlash va uni mahfiy kanal orqali uzatishda bir martalik parollarning o‘rni kata hisoblanadi. Ularni generatsiya qilish va saqlashda maxsus kalit qurilmalarini saqlovchi e-tokenlar, Java simcardlar va boshqalaridan foydalaniladi.  
*Ishning maqsadi:*Kalitlarni xavfsiz saqlash va yaratish tizimini ishlabchiqish.  
Ushbu bakalavr bitiruv ishi kirish, 3 ta qism, xulosa va foydalanilgan adabiyotlar to‘plamidan iborat.  
1-qism nazariy qism bo‘lib, kalitlarni yaratishda va saqlashda kriptogafiyaning o‘rni, simmetrik va asimmetrik shifrlash algoritmlariga bag‘ishlangan.  
2-qism amaliy qism, unda kalitlarni yaratuvchi va saqlovchin tizimlar: e-Tokenlar, Java cardlar, USB kalitlar va boshqalari tahlil qilinib, kriptografik algoritmlardan foydalanib kalit yaratish dasturini ishlab chiqilgan.  
3-qismda hayot faoliyati xavfsizligiga oid ma‘lumotlar keltirilgan.  
Xulosada ish bo‘yicha asosiy natijalar berilgan.

* 1. **Ma'lumotlarni [kodlash va shifrlash](https://hozir.org/2--laboratoriya-ishi-axborotlarni-kodlashtirishga-doir-misolla.html)**.

Ma’lumotlarni shifrlash – bu axborot himoyaning dasturlar vositasining turlari va amaliyotda alohida o‘rniga ega axborotni birdan bir ishonchli himoyasi.

“Shifrlash” tushunchasi “Kriptografiya” tushinchaga qaraganda ko‘proq ishlatadi. Kriptografiyani ichiga shifrlash kiradi va sonli ma’lumotlarni imkoni boricha almashtirishga bog‘liq muammolarni hal etish usullarini qo‘shimcha ko‘rib chiqadi: o‘zining qаrаmоg‘ida bo‘lgan faqat nоl va birlarning ketma-ketligiga ega bo‘lib sonli ma’lumotlarni qanday qilib tekshirish va qog‘ozda qo‘l qo‘yib yozilganga o‘xshatib qanday qilib elektron hujjatlarga viza qo‘yish kerak. Bu muammolar va ularni hal etish usullari keyin ko‘rib chiqiladi. Shifrlaydigan dasturlar soni cheklangan, ularning bir qismi de-fakto yoki de-yure standartlari.

Biroq, agar, shifrlash аlgоritmi maxfiy bo‘lmаsаdа, yopilgan kalitni bilmasdan deshifrlash (yoki shifrni yechish) juda qiyin. Zamonaviy shifrlash dasturlari bu хususiyatini kalitdan foydalanib (yoki ikkita kalit–shifrlash va shifrni yechish uchun bittadan) berilgan ochiq axborotni (“plain text” ingliz tili adabiyotlarida) ko‘p pog‘onali qayta ishlash jarayonida ta’minlaydi. Umuman aytganda, shifrlash uchun foydalaniladigan har bir murakkab usullar (algoritmlar) nisbatan oddiy usullarni kombinatsiyasini ifodalaydi. Shifrlash klassik algoritmlari bir birovidan quyidagicha farq qiladi:

• algoritmlash (oddiy [bir alfavitli](https://hozir.org/nazariy-qism-polialfavitli-almashtirish-usullari.html), bir tuzоqli ko‘p alfavitli, ko‘p аlfаvitli ko‘p tuzоqli);

• o‘rin almashtirish (oddiy, mураkkаblаshgаn);

• gammalshtirish (kalta bilan birlashtirish, uzun yoki chеklаnmаgаn maskali).

Klyuch kodini bilmasdan shifrni yechishga yuqorida sanab o‘tilgan usullarning har birini mustaxkamligi ko‘rsatkich [S yordamida sonli ifodalanadi](https://hozir.org/moq-qoshimchasi-yordamida-ifodalanadi.html), bu esa eng kam shifrlangan matn xajmiga teng bo‘lib, сtаtiсtik taxlil asosida shifrni yechish mumkin bo‘ladi.

Almashtirish ishlatadigan alfavit o‘rniga alternativ alfavitdan (yoki bir nechta alfavitlardan) foydalanishni nazarda tutadi.

Oddiy almashtirish bo‘lsa, masalan, ingliz alfavit simvollari uchun quyidagi almashuvini taklif qilish mumkin: “cache” degan so‘z shifrlangan ko‘rinishda “usuxk” bo‘ladi. Biroq xolis olingan uzun matnda simvollarni ma’lum stаtistik chastotasini qaytarilishi yordamida xabarni shifrini yechish imkoniyati mavjud. Masalan YE simvoli eng ko‘p uchraydi – har bir 1000 simvоllargа o‘rtacha 123 martta yoki 12,3% da, qolgan simvollar quyidagicha: T-9,6%, A-8,1%, 0-7,9% ,N-1,2%, J-7,2%, S-6,6%, R-6,0%, H-5,1%, L-4,0% va h.k. Ma’lumotlar manbaiga qarab ko‘rsatilgan sonlar, albatta o‘zgarishi mumkin.

Shuning uchun shifrni yechish ko‘rsаtkichini SKB mustaxkamligi bunda 20....30 dan oshmaydi. 2-jadvalda simvollarni almashtirilishi misol qilib ko‘rsatilgan.

|  |  |
| --- | --- |
| Ma’lum bo‘lgan [alfavit](https://hozir.org/ozbekiston-respublikasi-oliy-va-orta-maxsus-talim-vazirligi-is-v69.html) | A B C D E F G ] –I i J K L X Y Z |
| Alternativ alfavit | S O i H K T L : X N W m Y A P J |

Ko‘p аlfаvitli almashtirishda shunday qilish mumkinki, shifrlangan mаtndа xamma simvollar bir [xil chасtоtаdа uchrashi mumkin](https://hozir.org/1-laboratoriya-boyicha-topshiriq-azimov-nizomiddin.html), bu esa shifiрlаngаndаgi al’ternativ alfavit va tарtibni bilmasdan turib shifrni yechish ancha qiyinchiliklargа olib keladi. o‘rin almashtirish to‘g‘ri аlmаshtirishgа qaraganda shifrni yechishda yuqori mustaxkamligini ta’minlaydi va sonli kalitni ishlatib bajariladi yoki Misol tariqasida pасtdа ko‘rsаtilаdigаn ekvivalentli kalitli so‘z.

Sonli kalit qaytarilmaydigan sonlardan unga tegishli kalit so‘zi esa – qаytаrilmаydigаn simvollardan iborat. Kelib chiqadigan matn (plain text) kalit tagiga qatorma-qator yoziladi. Shifrlangan xabar (cipher text) ustunlargа kalit sonlariga qarab o‘sha tartibda yozib chiqishadi (yoki аlfаvitdаgi kalit so‘zining ayrim simvollari ularda joylashgan tartibda)

Ko‘rilayotgan misol uchun shifrlarngаn xabar TRANSPOSITION IS THE ENCIPHER METHOD quyidagi ko‘rinishda bo‘ladi:

AIHHORTTPHPaEaaSNaRaTIaITOINMccNOEEDSSCEct.

3-jadvalda oddiy o‘rin almashuvini ishlatish misoli keltirilgan.

*3-jadval*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Kalitli so‘z | S | E | C | n | R | 1T | V |
| Sonli kalit | 5 | 2 | 1 | 7 | 4 | 36 | 8 |
| Qatorma-qator yozilgan berilgan matn (plain text), | T | R | A | N | S | PO | S |
|  | I | T | I | O | N | al | S" |
|  | a | T | H | E | a | EN | C |
|  | I | P | H | E | R | aM | E |
|  | T | H | o | D | a | aa | a |

Oldindan tanlangan ikki хоnаli ketma-kеtligidа (maskali) berilgan xabarni 2 modul 2 (yoki o‘shаni o‘zi bo‘lgan yoki mantiq bo‘yicha uni inkor etuvchi) bitlarni qo‘shimcha asoslangan gammalashtirish

Maskani yaxlit (kompakt) ko‘rinishida o‘nlik tizimidagi hisob-lash [sonlari xizmat qilishi mumkin](https://hozir.org/aholi-daromadining-oshishi.html), yoki ba’zi mаtn (bu holatda simvollarning Ichki kodi ko‘rib chiqilаdi-ingliz matni uchun ASC// jadvali).

2-modul bo‘yicha qo‘shish operatsiyasi (isklyuchаyushее yoki) teskari bo‘ladi, shifrlаnggаn xabarni o‘sha maska (kalit) bilan qo‘shilса biz yana berilgan matnni olamiz (shifrni yechish bo‘ladi).

Maska (kalit) sifatida konstantalar n yoki e turdagilarni ishlatish mumkin va bunda mасkа oxirgi uzunlikka ega bo‘ladi.

Shifrni yechishda eng yuqori mustaxkamlikni cheksiz uzunlik maskalarni qo‘llaganda ta’minlanadi, bu esa ketma-ketliklar tasodifiy generatori bilan hosil bo‘lgan (aniqrog‘i psevdo-tasodifiy).

Bunday gеnеrаtоr apparatli yoki dasturli vositalari yordamida oson hal qilinadi masalan, bu esa teskari bog‘lаmаli siljish registr yordamida halaqit qilishga chidamli ikkilik kodni hisoblashda qo‘llaniladi.

Liniyaning qabul qilish oxirida generatorda aniq qayta tiklash psеvdо-tasodifiy ketma-kеtligini ta’minot shunday birlamchi holatni o‘rnatilganda (siljish реgiсtорdаgi borliqni) gеnераtорdаgi uzatadigan охiridаgi o‘sha teskari bog‘lаmаli strukturalar.

Sanab o‘tilgan Shifrlashning klassik usullari ([almashtirish](https://hozir.org/variant-3-daromat-samarasi-va-almashtirish-samarasi.html), o‘rnini almashtirish va gаmmаlаshtirish) - to‘g‘ri chiziqli dеyish mumkin shu ma’nodaki, shifrlangan xabarning uzuligi berilgan matnning uzunligiga teng. Chiziqli bo‘lmаgаni qayta tuzish mumkin, Masalan, oldindan tanlangan boshqa уzуnlikdаgi simvollar kombinatsiyasini Berilgan simvollarning (yoki butun so‘zlar, jumla, gaplar) o‘rniga almashtirish.

Shifrlashning standart usullari (Milliy yoki xalqaro) shifrlarni yechishga mustaxkamlik darajasini oshirish uchun shifrlashni bir nechta etаplar (qadamlar) [amalga oshiradi](https://hozir.org/5a110901-pedagogika-nazariyasi-va-tarixi-faoliyat-turi-boyicha.html), bularning har birida tanlangan kalitga (yoki kаlitlargа) qarab shifrlashni turli klаssik usullari ishlatiladi. Shifrlashning prinsipial har xil ikkita standart usullari mavjud:

• shifrlash va shifrlarni yechishda (simmetrik shifrlash yoki ochiq kаlitli tizimlar – Private – key sistems) bir xil kalitlarni ishlatib shifrlash.

• Shifrlash uchun ochiq kalitlarni va yopiq kalitlarni shifrlarni yechish uchun (simmetrik bo‘lmagan shifrlash) foydalanib shifrlash.

Shifrlashni standart usullarini qo‘llashda algoritmlarning aniq mаtеmаtik ifodalash juda qiyin. Foydalanuvchilar uchun birinchi navbatda har xil usullarning ishlatish xususiyatlari muhim (shifrni yechishda mustaxkamlik darajasi, shifrlash va shifrni yechish tezligi, kаlitlari tartibi va tarqatish qulayligi).

Ma’lumotlarni shifrlash standarti AQSH da DES (Data Encryptijn Standard) simmetrik shifrlash usullarining guruhiga tegishli bo‘lib 20 yildan ko‘proq ishlab kelmoqda (1976 y qabul qilingan). Qo‘llаnаlidigаn operatsiyalari – o‘rnini almashtirish, gammalantirish va chiziqli bo‘lmagan almashuv.

Qadamlar soni - 16. Kalitning uzunligi 56 bit, ulardan 8 bit – bu juft/toqlik tekshiradigan razryadlari.

Uzoq vaqt davomida bu usulni shifrni yechishga mustaxkamlik darajasi yetarli deb hisоblаnаrdi, lekin 1998 y maxsuslashtirilgan kompyuter (DES cracker) ixtiro qilingani to‘g‘risida xabar paydo bo‘ladi, bu kompyuter uzog‘i bilan 9 kun ichida (HTTP:/www. eff. orq /des racker ). Shifrlangan matnni yechishga qodir ekan. Bunday xabarlarni raqоbаtli kurashning bir nаmunаsi deb hisоblаsа bo‘ladi.

Bizning 28147-89 GOSTi DES ga analog (o‘xshash) bo‘ladi, lekin kаlitning uzunligi 256 bit, shuning uchun shifrni yechishga mustaxkamlik darajasi ancha yuqori. Ya’ni muhim tоmоni shundaki, Bunda butun himoyalash tizimi ko‘zda tutilgan bo‘lib, shifrlashni simmetrik usullarini “avlodli” kamchiliklarini yengib o‘tadi – ya’ni xabarlarni almashtirish imkoniyati. Imitоvstаvkаlar, xesh – funksiyalar va elektron sonli (yozilishlari)? – bunday tаkоmillаsh-tiрilgаnliklari uzatadigan xabarlarni “avtorizovat” qilishga imkon yaratadi. Shifrlаshni simmetrik usullarini avzalligi – shtfrlash va shifrni [yechishni katta tezligi](https://hozir.org/a-3-b-3-c-2-d-tjy.html), kamchiligi esa – agar kalti uchinchi shaxsga tegadigan bo‘lsa, bunda himoyalash darajasi kam bo‘ladi.

**1.2. Tasodifiy va psevdotasodifiy sonlar asosida kalitlarni yaratish**

Jamiyat taraqqiyoti insoniyat tafakkurining mahsuli bo‘lgan rivojlangan ilm-fan yutuqlariga asoslangan texnika va texnologiyalar [bilan bir qatorda](https://hozir.org/sinkveyn-texnologiyasi-haqida-tushuncha.html), keng ma‘noda, axborotlarning muhim ahamiyatga egaligi orqali ham belgilanadi. Inson tafakkuri rivojining manbai esa ma‘lumotlar (axborotlar) majmuidan iboratdir. Shak-shubhasiz o‘z vaqtida olingan to‘la va ishonchli ma‘lumot, shu ma‘lumot bilan bog‘liq bo‘lgan holatdan kelib chiqadigan amaliy faoliyatlarning maqsadli kechishlarini muvofiqlashtirishda muhim ahamiyat kasb etadi. Faoliyat maqsadlarining turlicha bo‘lishi tabiiy ravishda axborotlardan turli maqsadlarda foydalanish asoslariga sabab bo‘ladi. Shuning uchun bugungi, axborotlarni saqlash va uzatish tizimlari bir tomondan takomillashib murakkablashgan va ikkinchi tomondan axborotlardan foydalanuvchilar uchun keng qulayliklar vujudga kelgan davrda, axborotlarni maqsadli boshqarishning qator muhim masalalari kelib chiqadi. Bunday masalalar qatoriga katta hajmdagi axborotlarning tez va sifatli uzatish hamda qabul qilish, axborotlarni ishonchliligini ta‘minlash, axborotlar tizimida axborotlarni begona shaxslardan (keng ma‘noda) muhofaza qilish kabi ko‘plab boshqa masalalar kiradi. Axborot va axborot tizimidan foydalanish insoniyat faoliyatining barcha sohalariga kirib borib, muhim ahamiyat kasb etib, rivojlanib borayotgan bugungi jamiyatda axborotlarni maqsadli boshqarish faollashmoqda. Kompyuterlar va kompyuter tizimlari axborot tizimining muhim bo‘g‘imidir. Internet tarmoqlari jamiyat faoliyatining barcha sohalarini qamrab olib, axborotni tez va sifatli almashinuvini ta‘minlash texnologiyalarining rivojlanishiga ijobiy manba bo‘lib kelmokda. Yuqoridagi keltirilgan asosli mulohazalardan kelib chiqib, axborotlarni asli holidan o‘zgartirilgan holda, ya‘ni shifrlangan holda, saqlash va uzatish masalalarining muhim ekanligiga shubxa yo‘qdir. Axborotlarning muhofazasini ta‘minlash masalalari insoniyat jamiyatida qadimdan muxim bo‘lib kelgan. [Aytish mumkinki](https://hozir.org/til-millatning-asosiy-belgilaridan-davlat-mustaqilligining-aso.html), axborotni muhofaza qilish uslublari jamiyatda dastlabki paydo bo‘lgan muomila tili va yozuvi bilan uzviy bog‘liq hamda tengdoshdir. Haqiqatdan ham, qadimda yozuv muomila vositasidan faqat ayrim yuqori tabaqadagi jamiyat a‘zolarigina foydalanganlar. Qadimiy Misr va Hindistonning ilohiy kitoblari bunga misol bo‘la oladi. Eramizdan avvalgi beshinchi asrda yashab o‘tgan grek olimi Gerodotning habar berishicha, qadimiy Misrda shifrlangan axborotlar rolini, jreslar, ya‘ni yuqori tabaqadagi yetuk fikrli kishilar tomonidan yaratilgan muomila tili bajargan. Bunda uchta alfbo asoslanilgan: yozuv, ilohiy va mahfiy. Yozuv alfbosi oddiy o‘zaro muomilada qo‘llanilgan, ilohiy alfavit diniy muomila vositasi sifatida qo‘llanilgan, mahfiy alfbo esa ma‘lumotlarning asl ma‘nosini begonalardan muhofaza qilishda va astriologlar tomonidan qo‘llanilgan. Turli yozuv alfbolarining vujudga kelishi va rivojlanishi natijasida *kriptografiya* mustaqil yo‘nalishda rivojlana bordi.  
 Fan sifatida *kriptografiya -* axborotni aslidan o‘zgartirilgan holatga akslantirish uslublarini topish va takomillashtirish bilan shug‘ullanadi. Dastlabki sistemalashgan kriptografik uslublar eramiz boshida, Yuliy Sezarning ish yuritish yozishmalarida uchraydi. U, biror ma‘lumotni mahfiy holda biror kishiga yetkazmoqchi bo‘lsa, alfboning birinchi harfini to‘rtinchi harfi bilan, ikkinchi harfini beshinchisi bilan va hokazo tartibda almashtirib matnni asl holatidan shifrlangan matn holatiga o‘tkazgan.  
 Kriptografiya tizimlari yo‘nalishidagi izlanishlar ayniqsa birinchi va ikkinchi jahon urushi yillari davrida muhim ahamiyat kasb etdi va jadal rivojlandi. [Urushdan keyingi yillarda](https://hozir.org/urushdan-keyingi-yillarda-ozbekistonning-iqtisodiy-va-madaniy.html), hisoblash texnikalarining yaratilishi, ularning takomillashib, insoniyat faoliyatining barcha sohalariga chuqur va keng ma‘noda kirib borishi, kriptografik uslublarni tabiiy ravishda rivojlanib va takomillashib borishini ta‘qozo etmoqda.  
Kriptografiyaning axborot tizimi muhofazasi masalalarida qo‘llanilishi, ayniqsa, hozirgi kunda faollashib bormoqda. Haqiqatan ham, bir tomondan kompter tizimlarida internet tarmoqlaridan foydalangan holda katta hajmdagi davlat va harbiy ahamiyatga ega bo‘lgan, hamda, iqtisodiy, shahsiy va boshqa turdagi axborotni tez va sifatli uzatish, qabul qilish kengayib bormoqda. Ikkinchi tomondan esa bunday axborotlarning muhofaza qilinishi ta‘minlash masalalari muhimlashib bormoqda. Axborotni muxofaza qilish masalalari bilan *kriptologiya* (kryptos- mahfiy, logos- ilm) fani shug‘ullanadi. Kriptologiya maqsadlari o‘zaro qarama-qarshi ikkita yo‘nalishiga ega bo‘lgan – *kriptografiya* va *kriptoanaliz.*  
Kriptografiyaning ochiq ma‘lumotlarni shifrlash masalalarining matematik uslublari bilan shug‘ullanishi to‘g‘risida yuqorida aytib o‘tildi.  
Kriptoanaliz esa shifrlash uslubi (kaliti yoki algoritmi)ni bilmagan holda shifrlangan ma‘lumotni asl holatini (mos keluvchi ochiq ma‘lumotni) topish masalalarini yechish bilan shug‘ullanadi.  
Kriptografiya quyidagi to‘rtta bo‘limni o‘z ichiga oladi:

* Simmetrik kriptotizimlar.
* Ochiq uslubga yoki yana boshqacha aytganda ochiq kalitlar algoritmiga asoslangan kriptotizimlar.
* Elektron raqamli imzo kriptografik tizimlari.
* Kriptotizimlar uchun kriptobardoshli kalitlarni ishlab chiqish va ulardan foydalanishni boshqarish.

Uzuliksiz (oqimli) shifrlash algoritmlarini yaratilishi ham tabiiy zaruriyat asosida vujudga kelgan. Nisbatan kichik uzunlikka ega bo‘lgan, ya‘ni

kafolatlangan kriptobardoshlilikni ta‘minlovchi uzunlikga ega bo‘lgan - bugungi kunda 128 bitdan kam bo‘lmagan kalit bilan bir tomonli kriptografik akslantirishlar asosida, yetarli darajada katta uzunlikdagi psevdotasodifiy sonlar ketma-ketlik (PTSKK) gammasi ishlab chiqaruvchi generatorlar negizida uzuliksiz shifrlash algoritmlari yaratiladi. Uzunligi 128 bitdan kam bo‘lmagan [kalitlarning mumkin](https://hozir.org/bt-dagi-elektron-kalitlarning-ishlash-prinsipi-asosiy-xususiya-v2.html) bo‘lgan barcha variantlari soni tadan kam bo‘lmay, ularni hammasini tanlab chiqish jarayonini amalga oshirish, bugungi kun hisoblash texnika va texnologiyalarining mavjud ilg‘or imkoniyatlaridan foydalanilganda har doim ham samarali natijalar beravermaydi. Ana shunday generatorlar ishlab chiqargan gamma ketma-ketlikni tashkil etuvchi alfavit belgilarini ochiq ma‘lumot mos alfaviti belgilari bilan biror amal bajarish orqali shifr ma‘lumot alfaviti belgilariga almashtirish – gammalashtirish amalga oshiriladi. Bunday shifrlash jarayoni ko‘p alfavitli o‘rniga qo‘yish shifrlashni amalga oshirishni samarali usuluni ifodalaydi –kafolatli kriptobardoshlilikni ta‘minlovchi kichik uzunlikdagi kalit bilan, ochiq ma‘lumotning chastotaviy xususiyatlarini shifrma‘lumotga ko‘chirmaydigan yetarli kriptobardoshlilikni ta‘minlovchi shifrlashni amalga oshiradi

Oqimli shifrlash algoritmlari asosini PTSKK ishlab chiqaruvchi generatorlar tashkil etadi. Bunday generatorlarning asosiy kriptobardoshlilik xarakteristikasi ushbu generatorlar hosil qilgan ketma-ketlikning tasodifiyligidadir. Hosil qilingan ketma-ketliklar bloklarining tasodifiylik darajasi ma‘lum bir kriteriylar orqali baholanadi. Tasodifiylik darajasi yuqori bo‘lgan psevdotasodifiy ketma-ketlikni ishlab chiqaruvchi generatorlar zamonaviy kriptotizimlarning ajralmas qismi hisoblanadi. Tasodifiy ketma-ketliklar kriptografiyada quyidagi maqsadlarda qo‘laniladi:

* simmetrik kriptotizimlar uchun tasodifiylik darajasi yuqori bo‘lgan seans

kalitlari va boshqa kalitlarni generasiya qilishda;

* asimmetrik kriptotizimlarda qo‘llaniladigan katta qiymatlar qabul qiluvchi parametrlarning tasodifiy boshlang‘ich qiymatlari generasiyasida;
* blokli shifrlash algoritmlarining boshlang‘ich tasodifiy qiymat talab qiluvchi SVS, OFB va boshqa qo‘llanish tartib-qoidalari uchun tasodifiylik darajasi yuqori bo‘lgan boshlang‘ich vektorlar hosil qilishda;
* elektron raqamli imzo tizimlarida katta qiymatga ega parametrlar uchun dastlabki tasodifiy [qiymatlarni generasiyasida](https://hozir.org/davolash-ishi-fakulteti.html);
* bitta protokol orqali bir xil ma‘lumotlarni har-xil kalitlar qo‘llash bilan

shifrlab har-xil ko‘rinishda uzatish uchun talab qilinadigan holatlarda kalit uchun yetarli uzunlikdagi tasodifiy ketma-ketlik hosil qilishda, masalan SSL va SET protokollarida.   
Biror ketma-ketlikni tashkil etuvchi elementlar, shu ketma-ketlikda deyarli teng miqdorda qatnashgan bo‘lsa, bu ketma-ketlik tekis taqsimotga ega deyiladi:  
agar *A* -ketma-ketlikni tashkil etuvchi *xt* ∈*A* -elementlari soni *N* ta bo‘lsa, u holda ihtiyoriy *t*∈*N* uchun, *A* -ketma-ketlikni tashkil etuvchi *xt* ∈*A* -elementning, shu ketma-ketlikdagi chastotasi, boshqa elementlarning chastotasi bilan deyarli bir xil bo‘ladi, ya‘ni [har bir](https://hozir.org/informatika-fanidan-viii-sinflar-uchun-bilimlar-bellashuvida-m.html)*xt* ∈*A* –element shu ketmaketlikda deyarli bir xil ehtimollik bilan qatnashadi. Tasodifiy ketma-ketliklar xaqiqiy tasodifiy ketma-ketliklarga va psevdotasodifiy ketma-ketliklarga bo‘linadi.

Tasodifiy ketma-ketlikni: fizik generatorlar va dasturiy generatorlardan foydalanib hosil qilish mumkin.

**1.3.Kalitlarni xavfsiz saqlash va yaratish tizimi**

USB kalitlarni bir ko‘rinishi sifatida E-Tokenni keltirsak bo‘ladi. U apparatura va dasturlar orqali amalda oshirilib autentifikatsiyalovchi tizimimda ya‘ni, USB qurilmada electron raqamli imzo saqlanadi. Uning ko‘rinishi quyidagicha bo‘lishi mumkin: eToken PRO - USB-kalit.

Ular bir martalik va ko‘p martalik kalit generatsiya qilinishi bilan farqlanadi. Masalan: Aladdin firmasi tomonidan tayyorlangan 32k va 64k versiyali USB qurilmalari bir martalik kalit asosida ishlaydi ya‘ni har bir foydalanishda yangi kalit hosil qilib turadi.  
Uni amalga oshirish uchun dastur yoki apparatura va eToken NG-OTP - gibrid USB-kalit kerak bo‘ladi.

Xozirda Alladin firmasi tomonidan ishlab chiqilgan smart kartalar xuddi eTokenlar bajargan ishlarni xam amalga oshiryapti.  
Lekin muammoni bir tarafi hal bo‘lgani bilan ikkinchi tarafi shundaki, smart kartalarni ishlatish uchun kompyuterda yana boshqa qurilma zarur lekin eToken uchun shart emas. Bundan tashqari eTokenlar faqat kalitlarni emas ixtiyoriy maxfiy ma‘lumotlar, sertifikatlar va boshqa ma‘lumotlarni xavfsiz saqlashi mumkin.  
Agar eTokenda tizimga kiruvchi PIN(Personal Identification Number) saqalngan bo‘lsa, u %systemroot%\system32\etcpass.ini. faylidagi ma‘lumotni o‘zgartirib qo‘yadi. Va tizimga kirishda faqat shu eToken ichidagi parol orqali kiriladi.

**Parol**– foydalanuvchi hamda uning axborot almashinuvidagi sherigi biladigan narsa. O`zaro autentifikatsiya uchun foydalanuvchi va uning sherigi o`rtasida parol almashinishi mumkin. Plastik karta va smart-karta egasini  
autentifikatsiyasida shaxsiy identifikatsiya nomeri PIN sinalgan usul hisoblanadi.  
PIN – kodning mahfiy qiymati faqat karta egasiga ma`lum bo`lishi shart. Dinamik – (bir martalik) parol - bir marta ishlatilganidan so`ng boshqa  
umuman ishlatilmaydigan parol. Amalda odatda [doimiy parolga yoki tayanch](http://hozir.org/1-int-parol111a-agar-a-soni-parolga-teng-bolsa-xush-kelibsiz.html)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| iboroga asoslanuvchi muntazam o`zgarib turuvchi qiymat ishlatiladi. | | | | | | | | | | | |  |  |
|  | “**So`rov-javob” tizimi**- taraflarning biri noyob va oldindan bilib | | | | | | | | | | | | |
| bo`lmaydigan | | | ―so`rov‖ | | qiymatini | | ikkinchi | | tarafga | | jo`natish | |  |
| orqali autentifikatsiyani | | | | boshlab | | beradi, | | ikkinchi | | taraf esa | | so`rov | |
| va | sir yordamida hisoblangan | | | | | javobni | jo`natadi. | | Ikkala | | tarafga | bitta | sir |
| ma`lum | | bo`lgani | | sababli, | | birinchi taraf | |  | ikkinchi | | taraf |  |  |
| javobini to`g`riligini tekshirishi mumkin. | | | | | | |  |  |  |  |  |  |  |
|  | ―So`rov-javob‖ | | | mexanizmi | |  | quyidagicha.Agarb | | | | foydalanuvchi | | A |
| foydalanuvchi V dan oladigan xabari yolg`on [emasligiga ishonch](http://hozir.org/abdulloh-ulkan-ishonch-abdulloh-ulkan-ishonch-masuliyat-chekla.html) | | | | | | | | | | | xosil | qilishni | |

istasa, u foydalanuvchi V uchun yuboradigan xabarga oldindan bilib bo`lmaydigan element – X so`rovini (masalan, qandaydir tasodifiy sonni) qo`shadi. Foydalanuvchi V javob berishda bu amal ustida ma`lum amalni (masalan, qandaydir f(X) funktsiyani hisoblash) bajarishi lozim. Buni oldindan bajarib bo`lmaydi, chunki so`rovda qanday tasodifiy son X kelishi foydalanuvchi Vga ma`lum emas. Foydalanuvchi V harakati natijasini olgan foydalanuvchi A foydalanuvchi V ning xaqiqiy ekanligiga ishonch xosil qilishi mumkin. Ushbu usulning kamchiligi - so`rov va javob o`rtasidagi qonuniyatni aniqlash mumkinligi.

**Sertifikatlar [va raqamli imzolar](http://hozir.org/mysql-enterprise-encryption-faqat-tanlangan-tijorat-nashrlarid.html)** - agar autentifikatsiya uchun  
sertifikatlar [ishlatilsa](http://hozir.org/agar-funksiya-ichida-loop-lar-ishlatilsa.html), bu sertifikatlarda raqamli imzoning ishlatilishi  
talab etiladi. Sertifikatlar foydalanuvchi tashkilotining mas`ul shaxsi, sertifikatlar serveri yoki tashqi ishonchli tashkilot tomonidan beriladi.

Internet doirasida ochiq kalit sertifikatlarini tarqatish uchun ochiq kalitlarni boshqaruvchi qator tijorat infrastrukturalari PKI (Public Key  
Infrastrusture) paydo bo`ldi. Foydalanuvchilar turli daraja sertifikatlarini olishlari mumkin.  
Autentifikatsiya jaryonlarini ta`minlanuvchi xavfsizlik darajasi bo`yicha ham turkumlash mumkin. Ushbu yondashishga binoan autentifikatsiya jarayonlari quyidagi turlarga bo`linadi:

* parollar va raqamli sertifikatlardan [foydalanuvchi autentifikatsiya](http://hozir.org/environmental-pollution.html);
* kriptografik usullar va vositalar asosidagi qatiy autentifikatsiya;
* nullik bilim bilan isbotlash xususiyatiga ega bo`lgan autentifikatsiya jarayonlari (protokollari);
* foydalanuvchilarni biometrik autentifikatsiyasi.

Xavfsizlik nuqtai nazaridan yuqorida keltirilganlarning har biri o`ziga xos masalalarni echishga imkon beradi. SHu sababli autentifikatsiya [jarayonlari va](http://hozir.org/11-mavzu-qaror-qabul-qilishning-markov-jarayonlari-maruzaqa-qo.html)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| protokollari | amalda faol | | | ishlatiladi. SHu bilan bir qatorda ta`kidlash lozimki, | | | |
| nullik bilim bilan isbotlash xususiyatiga ega bo`lgan | | | | | | autentifikatsiyaga qiziqish | |
| amaliy | xarakterga | | nisbatan | | ko`proq [nazariy](http://hozir.org/nazariy-mexanika-v2.html) | xarakterga ega. | |
| Balkim,yaqin kelajakda ulardan axborot almashinuvini himoyalashda faol | | | | | | | |
| foydalanishlari mumkin. | | |  |  |  |  |  |
| *Foydalanuvchilarni* | | | | biometrik parametrlari. [Oxirgi](http://hozir.org/mavzu-fayllardan-oqish-va-fayllarga-yozish.html) | | | vaqtda |
| insonning | fiziologik | | parametrlari va xarakteristikalarini, [xulqining](http://hozir.org/mavzu-bola-xulqining-buzilish-omillari-mundarija-kirish-asosiy.html) | | | | |
| xususiyatlarini | | o`lchash | | orqali | foydalanuvchini | | ishonchli |

autentifikatsiyalashga imkon beruvchi biometrik autentifikatsiyalash keng tarqalmoqda.

Biometrik autentifikatsiyalash usullari an`anaviy usullarga nisbatan quyidagi afzalliklarga ega:  
⎯ biometrik alomatlarning [noyobligi tufayli](http://hozir.org/mavzu-biologik-xilma-xillikning-moslashuv-muammolari-dars-maqs.html) autentifikatsiyalashning ishonchlilik darajasi yuqori;

* biometrik alomatlarning sog`lom shaxsdan ajratib bo`lmasligi;
* biometrik alomatlarni soxtalashtirishning qiyinligi.

Foydalanuvchini autentifikatsiyalashda faol ishlatiladigan biometrik algoritmlar quyidagilar:

* barmoq izlari;
* qo`l [panjasining geometrik shakli](http://hozir.org/reja-bolalarning-buyumlar-shakli-va-geometrik-shakllarni-idrok.html);
* yuzning shakli va o`lchamlari;
* ovoz xususiyatlari;
* ko`z yoyi va to`r pardasining naqshi.

**2.1. Ochiq kalitlar [bilan shifrlash tizimi](https://hozir.org/reja-shifrlash-haqida-malumot-simmetrik-shifrlash-tizimi-haqid.html)**

Ochiq kalitli kriptografiya, yoki assimetrik kriptografiya, juftlarini ishlatadigan kriptografik tizimdir kalitlar: ochiq kalitlar, bu keng tarqalishi mumkin va shaxsiy kalitlarfaqat egasiga ma'lum bo'lgan narsalar. Bunday kalitlarning yaratilishi bog'liq kriptografik algoritmlar asoslangan matematik ishlab chiqarish uchun muammolar bir tomonlama funktsiyalar. Xavfsizlikni ta'minlash uchun faqat shaxsiy kalitni maxfiy saqlash kerak; ochiq kalit xavfsizlikka zarar etkazmasdan ochiq taqsimlanishi mumkin.

Bunday tizimda har qanday odam mumkin shifrlash qabul qiluvchidan foydalanadigan xabar ochiq kalit, lekin bu shifrlangan xabarni faqat qabul qiluvchining shifrini ochish mumkin shaxsiy kalit. Bu, masalan, server uchun mo'ljallangan kriptografik kalitni yaratishga imkon beradi nosimmetrik kalitli kriptografiya, keyin mijozning ochiq-oydin bo'lishidan foydalaning ochiq kalit yangi yaratilgan kodni shifrlash uchun nosimmetrik kalit. Endi, server ushbu shifrlangan nosimmetrik kalitni xavfli kanallarda mijozga yuborishi mumkin va faqat mijoz uni mijozning shaxsiy kalitlari juftligi yordamida ushbu xabarni shifrlash uchun server foydalanadigan ochiq kalitga parolini ochishi mumkin. Mijoz va server ikkalasi bir xil nosimmetrik kalitga ega bo'lgan holda, ular xavfsiz bo'lmagan kanallarda oldinga va orqaga ishonchli aloqa qilish uchun nosimmetrik kalitlarni shifrlashga xavfsiz tarzda o'tishlari mumkin. Bu nosimmetrik kalitlarni qo'lda oldindan ulashishning hojati yo'qligi va shu bilan birga ma'lumotlar uzatishning yuqori afzalliklariga ega bo'lishining afzalligi nosimmetrik kalitli kriptografiya assimetrik kalit kriptografiyasi orqali.

Ochiq kalitli kriptografiya bilan, mustahkam autentifikatsiya ham mumkin. Yuboruvchi xabarni shaxsiy kalit bilan birlashtirib, qisqa yaratish mumkin elektron raqamli imzo xabarda. Yuboruvchining tegishli ochiq kalitiga ega bo'lgan har bir kishi imzo haqiqiyligini, ya'ni tegishli shaxsiy kalit egasi tomonidan qilinganligini tekshirish uchun bir xil xabarni va u bilan bog'liq taxminiy raqamli imzoni birlashtirishi mumkin.

Ochiq kalit algoritmlari zamonaviy xavfsizlikning asosiy tarkibiy qismidir kriptotizimlar, maxfiyligini, haqiqiyligini va rad etmaslik elektron aloqa va ma'lumotlarni saqlash. Ular kabi turli xil Internet standartlarini qo'llab-quvvatlaydi Transport qatlamining xavfsizligi (TLS), S / MIME, PGPva GPG. Ba'zi ochiq kalit algoritmlari taqdim etadi kalitlarni taqsimlash va maxfiylik (masalan, Diffie-Hellman kalit almashinuvi), ba'zilari beradi elektron raqamli imzolar (masalan, Raqamli imzo algoritmi), ba'zilari esa ikkalasini ham beradi (masalan, RSA). Ga solishtirganda nosimmetrik shifrlash, assimetrik shifrlash ko'p maqsadlar uchun sekin. Bugungi kriptosistemalar (masalan TLS, Xavfsiz Shell) nosimmetrik shifrlashdan ham, assimetrik shifrlashdan ham foydalaning.

1970-yillarning o'rtalaridan oldin barcha shifrlash tizimlari ishlatilgan nosimmetrik kalit algoritmlari, unda bir xil kriptografik kalit asosiy algoritm bilan ham jo'natuvchi, ham oluvchi tomonidan ishlatiladi, ular ikkalasi ham buni sir tutishlari kerak. Zero, har qanday tizimdagi kalit tizimni ishlatishdan oldin aloqa qilayotgan tomonlar o'rtasida xavfsiz tarzda almashinishi kerak edi - a xavfsiz kanal. Ushbu talab hech qachon ahamiyatsiz emas va ishtirokchilar sonining ko'payishi bilan, yoki kalitlarni almashtirish uchun xavfsiz kanallar mavjud bo'lmaganda yoki (masalan, oqilona kriptografik amaliyotda) kalitlar tez-tez o'zgartirilganda juda tez boshqarib bo'lmaydigan bo'ladi. Xususan, agar xabarlar boshqa foydalanuvchilar tomonidan xavfsiz bo'lishi kerak bo'lsa, har bir mumkin bo'lgan foydalanuvchilar juftligi uchun alohida kalit talab qilinadi.

Aksincha, ochiq kalit tizimida ochiq kalitlar keng va ochiq tarzda tarqatilishi mumkin va faqat shaxsiy kalit egasi tomonidan xavfsiz saqlanishi kerak.

Ochiq kalit kriptografiyasining eng taniqli ikkita usuli:

Ochiq kalitlarni shifrlash, unda xabar qabul qiluvchining ochiq kaliti bilan shifrlanadi. Tegishli shaxsiy kalitga ega bo'lmagan, shu kalit egasi va ochiq kalit bilan bog'langan shaxs deb hisoblanadigan har bir kishi xabarni parolini hal qila olmaydi. Bu ta'minlash uchun ishlatiladi maxfiylik.

Elektron raqamli imzolar, unda xabar jo'natuvchining shaxsiy kaliti bilan imzolanadi va uni jo'natuvchining ochiq kalitiga kirish huquqiga ega bo'lgan har bir kishi tasdiqlashi mumkin. Ushbu tekshirish jo'natuvchining shaxsiy kalitga kirish huquqiga ega ekanligini va shuning uchun ochiq kalit bilan bog'langan shaxs bo'lishi mumkinligini tasdiqlaydi. Bu, shuningdek, xabar buzilmasligini kafolatlaydi, chunki imzo matematik ravishda u dastlab qilingan xabar bilan bog'langan va tekshirish har qanday boshqa xabar uchun, asl xabarga qanchalik o'xshash bo'lishidan qat'iy nazar, muvaffaqiyatsiz bo'ladi.

Muhim masalalardan biri - ma'lum bir ochiq kalitning haqiqiyligi, ya'ni uning to'g'ri ekanligi va da'vo qilingan shaxsga yoki tashkilotga tegishli ekanligi va zararli uchinchi shaxs tomonidan buzilmaganligi yoki almashtirilmaganligi to'g'risida ishonch / dalil. Bir nechta yondashuvlar mavjud, jumladan:

A ochiq kalitli infratuzilma (PKI), unda bir yoki bir nechta uchinchi shaxslar sifatida tanilgan sertifikat idoralari - kalit juftlarga egalik huquqini tasdiqlash. TLS bunga tayanadi.

A "ishonchli veb"foydalanuvchi va ochiq kalit o'rtasidagi bog'lanishning individual tavsiyalaridan foydalangan holda autentifikatsiyani markazlashtirmaydi. PGP ushbu yondashuvdan foydalanadi, shuningdek domen nomlari tizimi (DNS). The DKIM elektron pochta xabarlarini raqamli imzolash tizimi ham ushbu usuldan foydalanadi.

Ochiq kalitlarni shifrlash tizimining eng aniq qo'llanilishi - bu aloqani ta'minlash uchun shifrlash maxfiylik - jo'natuvchi qabul qiluvchining ochiq kalitidan foydalangan holda shifrlashi haqidagi xabar faqat oluvchining juftlashgan shaxsiy kaliti yordamida shifrlangan bo'lishi mumkin.

kalit kriptografiyasidagi yana bir dastur bu elektron raqamli imzo. Yuboruvchi uchun elektron raqamli imzo sxemalaridan foydalanish mumkin autentifikatsiya.

Rad etmaslik tizimlar raqamli imzolardan foydalanib, bir tomon hujjat yoki kommunikatsiya muallifligi to'g'risida muvaffaqiyatli bahslasha olmasligini ta'minlaydi.

Ushbu poydevor asosida qurilgan qo'shimcha dasturlarga quyidagilar kiradi: raqamli naqd pul, parol bilan tasdiqlangan kalit shartnomasi, vaqtni belgilash bo'yicha xizmatlarrad etmaslik protokollari va boshqalar.

Gibrid kriptotizimlar Asimmetrik kalit algoritmlari deyarli har doim nosimmetrikga qaraganda ancha zichroq bo'lganligi sababli, ko'p hollarda public / private dan foydalanish odatiy holdir assimetrik kalitlarni almashtirish algoritmi shifrlash va almashtirish nosimmetrik kalit, keyin o'tish nosimmetrik kalitli kriptografiya hozirda birgalikda foydalaniladigan ma'lumotlar yordamida ma'lumotlarni uzatish nosimmetrik kalit va nosimmetrik kalitlarni shifrlash algoritmi. PGP, SSH, va SSL/ TLS sxemalar oilasi ushbu protseduradan foydalanadi va shunday chaqiriladi gibrid kriptotizimlar. Boshlang'ich assimetrik server tomonidan yaratilgan almashish uchun kriptografiyaga asoslangan kalit almashinuv nosimmetrik serverdan mijozga kalit, simmetrik kalitni qo'lda oldindan almashishni talab qilmaslikning afzalligi, masalan, bosilgan qog'ozda yoki kuryer orqali olib boriladigan disklarda, simmetrik kalit kriptografiyasining yuqori assotsiatsiyasi uchun simmetrik kalit kriptografiyasini taqdim etadi. umumiy ulanishning qolgan qismi.

Zaif tomonlari

Xavfsizlik bilan bog'liq barcha tizimlarda bo'lgani kabi, yuzaga kelishi mumkin bo'lgan zaif tomonlarni aniqlash ham muhimdir.

Algoritmlar Barcha ochiq kalit sxemalar nazariya nuqtai nazaridan "qo'pollik bilan kalitlarni qidirish hujumi".[4] Ammo, agar muvaffaqiyatli hisoblash uchun zarur bo'lgan hisoblash miqdori "ish omili" deb nomlangan bo'lsa, bunday hujumlar amaliy emas Klod Shannon - barcha potentsial hujumchilarning imkoniyatidan mahrum. Ko'pgina hollarda, ish omilini shunchaki uzunroq kalitni tanlash orqali oshirish mumkin. Ammo boshqa algoritmlarda ish omillari ancha past bo'lishi mumkin, bu esa qo'pol kuch hujumiga qarshilikni ahamiyatsiz qiladi. Shifrlashning ba'zi bir ochiq algoritmlariga hujum qilishda yordam beradigan ba'zi maxsus va o'ziga xos algoritmlar ishlab chiqilgan RSA va ElGamal shifrlash qo'pol kuch ishlatish usulidan ancha tezroq bo'lgan hujumlarni bilishadi.[5]

Ilgari umidvor bo'lgan bir nechta assimetrik kalit algoritmlari uchun asosiy zaifliklar topildi. The "yukxalta bilan qadoqlash" algoritmi yangi hujum rivojlangandan so'ng o'ziga ishonchsiz deb topildi.[6] Barcha kriptografik funktsiyalarda bo'lgani kabi, ochiq kalitli dasturlar ham zaif bo'lishi mumkin yon kanal hujumlari maxfiy kalitni qidirishni soddalashtirish uchun ma'lumot tarqalishidan foydalanadigan. Yangi hujumlarni kashf etish va ularni himoya qilish bo'yicha tadqiqotlar olib borilmoqda.

Ochiq kalitlarni o'zgartirish

Asimmetrik kalitlarni ishlatishda xavfsizlikning yana bir potentsial zaifligi - bu "o'rtada odam" hujumi, unda ochiq kalitlarning aloqasi uchinchi tomon tomonidan ushlab turiladi ("o'rtada odam") va keyin o'zgartirilib, uning o'rniga turli xil ochiq kalitlarni taqdim etadi. Shifrlangan xabarlar va javoblar, shubhalanmaslik uchun, barcha holatlarda, turli xil aloqa segmentlari uchun to'g'ri ochiq kalitlardan foydalangan holda tajovuzkor tomonidan tutilishi, parolini ochishi va qayta shifrlanishi kerak.

Ma'lumotlar tutib olishga imkon beradigan tarzda uzatiladigan aloqa xavfsiz emas deyiladi (shuningdek, "hidlash"). Ushbu atamalar jo'natuvchining shaxsiy ma'lumotlarini to'liq o'qishni nazarda tutadi. Qabul qilishning oldini olish yoki jo'natuvchi tomonidan kuzatib bo'lmaydigan aloqa, ayniqsa xavfli hisoblanadi.[7]

O'rtada odam hujumi zamonaviy xavfsizlik protokollarining murakkabligi sababli amalga oshirilishi qiyin bo'lishi mumkin. Biroq, jo'natuvchi jamoat tarmoqlari, kabi xavfsiz bo'lmagan vositalardan foydalanganda, vazifa osonroq bo'ladi Internetyoki simsiz aloqa. Bunday hollarda tajovuzkor ma'lumotlarning o'zi emas, balki aloqa infratuzilmasini buzishi mumkin. Gipotetik zararli xodim Internet-provayder (ISP) o'rtada odam hujumini nisbatan sodda deb topishi mumkin. Ochiq kalitni qo'lga olish uchun faqat Internet-provayderning aloqa vositalari orqali yuborilganda kalitni qidirish kerak bo'ladi.

"O'rtada odam" ning ba'zi bir rivojlangan hujumlarida aloqaning bir tomoni asl ma'lumotni ko'radi, ikkinchisi zararli variantni oladi. Odamlar o'rtasida assimetrik hujumlar foydalanuvchilarning aloqasi buzilganligini anglashiga to'sqinlik qilishi mumkin. Bir foydalanuvchining ma'lumotlari buzilganligi ma'lum bo'lgan taqdirda ham, bu haqiqat bo'lib qoladi, chunki ma'lumotlar boshqa foydalanuvchiga yaxshi ko'rinadi. Bu foydalanuvchilar o'rtasida chalkash kelishmovchiliklarni keltirib chiqarishi mumkin, masalan, "bu sizning oxirida bo'lishi kerak!" hech bir foydalanuvchi aybdor bo'lmaganida. Demak, o'rtada odam hujumlarini faqat aloqa infratuzilmasi bir yoki ikkala tomon tomonidan jismoniy nazorat ostida bo'lgan taqdirda to'liq oldini olish mumkin; masalan, jo'natuvchining o'z binosi ichidagi simli yo'nalish orqali. Xulosa qilib aytganda, jo'natuvchi tomonidan ishlatiladigan aloqa apparati tajovuzkor tomonidan boshqarilganda ochiq kalitlarni o'zgartirish osonroq bo'ladi.

Ochiq kalitlarning infratuzilmasi

Bunday hujumlarning oldini olish uchun bitta yondashuv a dan foydalanishni o'z ichiga oladi ochiq kalitli infratuzilma (PKI); raqamli sertifikatlarni yaratish, boshqarish, tarqatish, ishlatish, saqlash va bekor qilish hamda ochiq kalitda shifrlashni boshqarish uchun zarur bo'lgan rollar, siyosat va protseduralar to'plami. Biroq, bu o'z navbatida mumkin bo'lgan zaif tomonlarga ega.

Masalan, sertifikat beruvchi sertifikat beruvchiga kalit egasining shaxsini to'g'ri tekshirganligi, sertifikat berganida ochiq kalitning to'g'riligini ta'minlashi, kompyuter qaroqchiligidan himoyalangan bo'lishi va kelishuvga erishgan bo'lishi kerak. himoyalangan aloqa boshlanishidan oldin barcha ishtirokchilar o'zlarining barcha sertifikatlarini tekshirishlari kerak. Veb-brauzerlarMasalan, PKI provayderlarining "o'z-o'zidan imzolangan shaxsiy guvohnomalari" ning uzoq ro'yxati bilan ta'minlangan - bu tekshiruv uchun ishlatiladi vijdonan sertifikat idorasining, so'ngra ikkinchi bosqichda potentsial kommunikatorlarning sertifikatlari. Sertifikat idoralaridan birortasini soxta ochiq kalit uchun sertifikat berishga qodir bo'lgan tajovuzkor "o'rtada odam" hujumini sertifikat sxemasi umuman ishlatilmagandek osonlikcha uyushtirishi mumkin. Muqobil stsenariyda kamdan-kam muhokama qilinadi[iqtibos kerak], hokimiyat serverlariga kirib, uning sertifikatlari va kalitlari do'konini olgan (ommaviy va xususiy) tajovuzkor operatsiyalarni cheksiz ravishda buzishi, maskalashi, parolini ochishi va soxtalashtirishi mumkin.

Nazariy va potentsial muammolariga qaramay, ushbu yondashuv keng qo'llaniladi. Bunga misollar kiradi TLS va uning oldingisi SSL, odatda veb-brauzer operatsiyalari xavfsizligini ta'minlash uchun ishlatiladi (masalan, onlayn-do'konga kredit karta ma'lumotlarini xavfsiz yuborish).

Muayyan kalit juftligining hujumiga qarshilik ko'rsatishdan tashqari, sertifikatlash xavfsizligi ierarxiya ochiq kalit tizimlarini joylashtirishda e'tiborga olish kerak. Ba'zi bir sertifikat idorasi - odatda server kompyuterida ishlaydigan maxsus dastur - raqamli sertifikat ishlab chiqarish orqali maxsus shaxsiy kalitlarga berilgan shaxsiyat uchun kafolat beradi. Ochiq kalit raqamli sertifikatlar odatda bir necha yil davomida amal qiladi, shuning uchun tegishli shaxsiy kalitlar shu vaqt ichida xavfsiz saqlanishi kerak. PKI server ierarxiyasida yuqori darajadagi sertifikat yaratish uchun foydalaniladigan shaxsiy kalit buzilgan yoki tasodifan oshkor qilingan bo'lsa, ""o'rtada hujum"har qanday bo'ysunuvchi guvohnomani to'liq xavfli qilib, qilish mumkin.

Misollar

Turli maqsadlar uchun yaxshi ko'rib chiqilgan assimetrik kalit texnikaning namunalariga quyidagilar kiradi:

Diffie-Hellman kalit almashinuvi protokol

O'z ichiga olgan DSS (Raqamli imzo standarti) Raqamli imzo algoritmi

ElGamal

Elliptik-egri kriptografiya

Elliptik egri raqamli imzo algoritmi (ECDSA)

Elliptik egri chiziq Diffie-Hellman (ECDH)

Turli xil parol bilan tasdiqlangan kalit shartnomasi texnikasi

Paillier kriptosistemasi

RSA shifrlash algoritmi (PKCS №1)

Cramer – Shoup kriptosistemasi

YAK tasdiqlangan kalit kelishuv protokoli

Asimmetrik kalit algoritmlarining keng qabul qilinmagan misollariga quyidagilar kiradi:

Shifrlash kriptotizim

McEliece kriptotizimi

Asimmetrik kalit algoritmlarning diqqatga sazovor, ammo xavfsiz emasligiga quyidagilar kiradi:

Merkle-Hellman tizza to'plami kriptosistemasi

Asimmetrik kalit algoritmlaridan foydalanadigan protokollarga quyidagilar kiradi:

S / MIME

GPG, amalga oshirish OpenPGP

EMV, EMV sertifikat markazi

IPsec

PGP

ZRTP, xavfsiz VoIP protokol

Transport qatlamining xavfsizligi tomonidan standartlashtirilgan IETF va uning oldingisi Xavfsiz soket qatlami

SILC

SSH

Bitcoin

Yozuvdan tashqari xabarlarEntsiklopediya site:ewikiuz.top

**2.2. Yopiq kalitlar [bilan shifrlash tizimi](https://hozir.org/reja-shifrlash-haqida-malumot-simmetrik-shifrlash-tizimi-haqid.html)**

Kalitdan foydalanib shifrlash algoritmining ikki xil ko‘rinishi mavjud:  
*simmetrik*va *asimmetrik*

Xabarlarni shifrlash uchun foydalanilgan kalit shifrni ochish kalitidan olingan va aksi o‘rinli bo‘lsa, bunday kriptografik algoritmlar simmetrik deb nomlanadi. Ko‘pgina simmetrik algoritmlarda yagona kalitdan foydalaniladi. [Bunday algoritmlar](https://hozir.org/1-modul-algoritmlar-haqida-asosiy-tushunchalar-1-mavzu-hisobla-v2.html)*bir kalitli*yoki maxfiy kalitli algoritmlar deb ataladi hamda xabarni yuboruvchi va uni qabul qiluvchi qanday kalitdan foydalanishni kelishib olishlarini talab etadi. Bir kalitli algoritmlarning ishonchliligi kalitni tanlash bilan aniqlanadi. Agar jinoyatchiga kalit ma’lum bo‘lsa, hech qanday qarshiliksiz barcha tutib olingan ma’lumotlar shifrini ochish imkoni yaratiladi. Demak tanlangan kalitni begonalardan sir saqlash zarur.

Shifrlashning simmetrik algoritmlari ikki turda bo‘ladi. Ulardan biri ochiq matnga bitlar bo‘yicha ishlov beradi. Ular *potokli algoritmlar*yoki *potokli shifrlar*deb nomlanadi. Ikkinchisida esa, ochiq matn bir necha bitdan iborat bo‘lgan bloklarga bo‘linadi. Bunday algoritmlar *blokli algoritmlar*yoki *blokli shifrlar*deb nomlanadi. Blokli shifrlashning zamonaviy kompyuter algoritmlarida, odatda, blok uzunligi 64 bitni tashkil etadi. Simmetriyali tizimlarda quyidagi ikkita muammo mavjud: 1) Axborot almashuvida ishtirok etuvchilar qanday yo‘l bilan maxfiy kalitni bir-birlariga uzatishlari mumkin? 2) Jo‘natilgan xabarning haqiqiyligini qanday aniqlasa bo‘ladi? Simmetrik kalit bilan shifrlash sxemasini quyidagi misolda ko‘rib chiqamiz. Ali (A) va Vali (V) nomli korrespondentlar bir-biri bilan xabar almashishmoqchi. Korrespondentlarning har biri o‘zining maxfiy kalitiga ega, bu kalitdan xabarni tarmoq orqali yuborishdan avval ma’lumotlarni shifrlashda foydalanishi mumkin. Shifrlash sxemasini ko‘rimliroq tasvirlash uchun, [kalitni oddiy kalit](https://hozir.org/20-maruza-togri-yurishli-kuchlanish-ozgartirgichlari.html), shifrlangan xabarni esa konvertga solingan hujjat ko‘rinishida tasvirlaymiz. Shifrlash va qayta shifrlash jarayoni quyidagi rasmda tasvirlangan.

Simmetrik kalit yordamida shifrlash tizimi foydalanuvchi A o‘zining maxfiy kaliti bilan xabarni shifrlaydi va xabarni tarmoq orqali jo‘natadi, qabul qiluvchi V (xuddi shunday maxfiy kalitdan foydalanib) xabarni qayta tiklaydi. Rasmda sxemaning simmetrik ekanligi ko‘rinib turibdi. Chap va o‘ng tomondagi foydalanuvchilar bir xil (simmetrik) kalitlardan foydalanishmoqda, shuning uchun bunday turdagi shifrlash simmetrik kalit yordamida shifrlash deb yuritiladi. Maxfiy kalit yordamida shifrlash usuli ma’lum kamchiliklardan holi emas. Birinchi navbatda, simmetrik shifrlash autentifikatsiyalash muammosini hal qilib bermaydi. Masalan, Ali (A) Soli (S)ga xat yozib yuborishi, lekin bu xatni Vali (V) yozgan deb tan olmasligi mumkin. Bundan tashqari, simmetrik kalit xabar yuborilishidan oldin xabar jo‘natuvchi va qabul qiluvchi kompyuterlarda o‘rnatilgan bo‘lishi kerak. Tabiiyki, Internetda xavfsiz [muloqot qilish uchun shifrlash](https://hozir.org/reja-i-kirish-ii-asosiy-qism-jeferson-kriptografik-shifrlash-q.html), korrespondentlarning shaxsan uchrashishlari shart bo‘lmagan holatda ma’noga ega. Muammomaxfiy kalitni uzatishda yuzaga keladi. Haqiqatda, agar jo‘natuvchi Ali qabul qiluvchi Valiga kalitni shifrlamasdan uzatsa, kalitni tutib olishlari mumkin. Agar kalit shifrlangan ko‘rinishda jo‘natilsa, unda qabul qiluvchi Vali uni ocha olmaydi. Bir nechta korrespondentlar bilan yozishmalar olib borish uchun, har bir qabul qiluvchi uchun alohida kalitlar bo‘lishi lozim, bu esa noqulaylikni tug‘diradi. Bu muammoni yechimini topish uchun asimmetrik shifrlash (ochiq (ommaviy) kalit yordamida shifrlash) sxemasi taklif etilgan. Ochiq kalitli shifrlash yoki shifrlashning asimmetrik algoritmlari deb ataluvchi algoritmlarda shifrlash uchun ishlatiladigan kalit shifrni ochish uchun ishlatiladigan kalitdan farq qiladi. Bundan tashqari, shifrlash kalitini bilgan holda, shifrni ochish uchun zarur kalitni juda katta muddat ichida hisoblab topish imkoni bo‘lmaydi. Ixtiyoriy foydalanuvchi shifrlash kaliti yordamida [xabarni shifrlashi mumkin](https://hozir.org/ozbekiston-respublikasi-axborot-texnologiyalari-va-kommunikats-v496.html), lekin bu kalitga mos shifrni ochish kalitiga ega shaxsgina bu xabarni o‘qiy oladi. Shifrlash kalitini ochiq (ommaviy) kalit, shifrni ochish kalitini esa yopiq (maxfiy, xususiy) kalit deyiladi. Xabarni yopiq yoki ochiq kalit yordamida shifrlash mumkin, qayta tiklash esa ikkinchi kalit yordamida amalga oshiriladi. Ya’ni, yopiq kalit yordamida shifrlangan matn faqat ochiq kalit yordamida qayta tiklanishi mumkin va aksincha. Yopiq kalit faqat egasiga ma’lum, va u hech kimga

berilmaydi, ochiq kalit esa ochiq tarqatiladi va u hammaga ma’lum bo‘lishi mumkin. Ikkita kalitni autentifikatsiyalash masalasining yechimini topish uchun hamda konfedensiallikni ta’minlashda qo‘llash mumkin. Agar birinchi kalit yopiq bo‘lsa, u holda u elektron imzo sifatida ishlatiladi va bu usul bilan axborotni autentifikatsiyalash, ya’ni axborotning butunligini ta’minlash imkoni paydo bo‘ladi. Axborotni autentifikatsiyalashdan tashqari quyidagi masalalarni yechish mumkin:

– foydalanuvchini autentifikatsiyalash, ya’ni kompyuter tizimi resurslariga kirmoqchi bo‘lgan [foydalanuvchini aniqlash](https://hozir.org/tarmoq-administratorligi-4-dars.html);

– tarmoq abonentlari aloqasini o‘rnatish jarayonida ularni o‘zaro autentifikatsiyalash.

Quyidagi sxemaga muvofiq, foydalanuvchi Ali (A) oldindan ochiq kalitni Vali (V) va Soli (S) nomli korrespondentlarga jo‘natadi, keyin esa yopiq kalit bilan shifrlangan matnni yuboradi.

Xabarni faqat Ali (A) jo‘natishi mumkin (yopiq kalit unga tegishli), bunda autentifikatsiya muammosi yechilgan. Lekin, masalan Vali (V)ning unga yo‘llangan xatni Soli (S) o‘qimaganligiga aniq ishonchi yo‘q. Demak, konfedensiallik ta’minlanmagan. Konfedensiallikni ta’minlash sxemasi quyidagi rasmda tasvirlangan.

Xabarni faqat Ali (A) o‘qishi mumkin, chunki u xabarni qayta tiklash imkonini beruvchi yopiq kalitga ega, xabarni konfedensialligi ta’minlangan. Lekin, Ali (A) xabarni Soli (S) ubormaganiga aniq ishonchi yo‘q, chunki u Vali (V) nomidan xabarni yuborishi ham mumkin. Demak, autentifikatsiyalash ta’minlanmagan. Ikkita shaxs orasida xabar almashishda konfedensiallikni ta’minlash uchun ikkita kalit bo‘lishi shart. Juft kalit bilan shifrlashda Ali (A) tomonidan hammaga ochiq kalit jo‘natilishi shart emas. Ochiq kalit tarmoqdagi ochiq foydalanishni imkonini beruvchi serverga joylashtirilishi mumkin. Simmetrik va asimmetrik kalit yordamida shifrlash. Shuni ta’kidlash lozimki, asimmetrik shifrlash algoritmida ma’lumotlarni shifrlash va qayta tiklash uchun simmetrik shifrlashga qaraganda ko‘p vaqt talab qilinadi, shuning uchun zamonaviy shifrlash tizimlarida asimmetrik shifrlash va an’anaviy simmetrik shifrlashning kombinatsiyalari qo‘llaniladi. Ochiq kalit yordamida shifrlash simmetrik kalitni uzatishda foydalaniladi, bu kalit yordamida uzatiladigan axborot shifrlanadi. Bu sxemani ishlash qoidasi quyidagi rasmda keltirilgan. Avval Ali (A) boshlang‘ich faylni simmetrik kalit yordamida shifrlaydi (1-punkt). Keyin (2-punkt) Ali ochiq manbalardan Vali (V)ga tegishli

bo‘lgan ochiq kalitni oladi va bu kalit yordamida o‘zining simmetrik kalitini shifrlaydi. So‘ngra (3-punkt) ikkala obyekt (shifrlangan fayl va shifrlangan simmetrik kalit) Internet orqali Vali (V)ning manziliga jo‘natiladi. Vali ikkala obyektni qabul qilib oladi (4-punkt). [Simmetrik](https://hozir.org/simmetrik-kophadlar-reja.html) kalit Valiga tegishli bo‘lgan yopiq kalit yordamida qayta tiklanadi (5- punkt) va qayta tiklangan simmetrik kalit yordamida boshlang‘ich fayl shifrdan yechiladi (6-punkt). Kimdir, sizning yopiq kalitingiz yordamida shifrlangan xabarni olsa, u sizdan xabar kelganiga ishonch hosil qiladi. Ya’ni, bu holatda, shifrlash imzo qo‘yganga ekvivalent bo‘ladi. Demak, raqamli (elektron) imzo – bu jo‘natuvchi yoki imzo muallifini autentifikatsiyalash usuli bo‘lib, hujjat mazmuni o‘zgartirilmaganligini tasdiqlaydi1. Raqamli imzo shifrlangan holda yoki ochiq shifrlanmagan holda yuborilishi mumkin. *Raqamli sertifikatlar.*Ochiq kalitli shirflash sxemasidan foydalanganda ochiq kalitni mijozlarga tarqatish yoki tarmoqdagi serverga o‘rnatmoq kerak. Lekin raqib sizning nomingiz bilan o‘zini tanitishi va ochiq kalitni sizning nomingizdan tarqatishi mumkin. Ommaviy kalitni haqiqiy egasi kimligini aniqlash uchun, hamma korrespondentlar ishonch bildiradigan uchinchi tomonga ehtiyoj paydo bo‘ladi. Bu masala sertifikatlashtirish markazlari (Certification Authority) orqali hal etiladi. Ular tomonidan sertifikatlar – egasini identifikatsiyalaydigan ochiq kalit va axborotning mosligini tasdiqlaydigan raqamli ma’lumotlar, kafolatchi imzolagan raqamli imzo beriladi. [Sertifikatda ommaviy kalit](https://hozir.org/22-mavzu-majdon-tomoshalari-tushunchasi-reja-1-ommaviy-bayram.html), kalitning egasi haqidagi ma’lumot, sertifikatlashtirish markazining nomi, sertifikatni amal qilish muddati kabi ma’lumotlar bo‘ladi. Sertifikatning har bir nusxasiga sertifikat bergan tashkilotning raqamli imzosi biriktiriladi, shuning uchun kim sertifikat olgan bo‘lsa, uning haqiqiyligiga ishonch hosil qilishi mumkin. Sertifikat shaxsni kimligini tasdiqlovchi hujjatning analogidir. Shaxsni identifikatsiya qilish muammosi (pasport, haydovchilik guvohnomasi va hokazo) uchrashuv paytida yuzaga keladi. Tarmoqda sherikni ko‘rmasdan turib muloqot qilishda, shaxsning kimligini bilish yanada muhimroqdir.

Kriptomustahkamlik shifrning tasnifi bo‘lib, u kalitni bilmasdan turib shifrni yechishga bo‘lgan mustahkamlikni bildiradi. Shifrlash orqali axborotni himoyalashning samaradorligi kalitning yashirin saqlanishiga va shifrning kriptomustahkamligiga bog‘liq. *Shifrlashga qo‘yiladigan asosiy talablar.*Zamonaviy shifrlash usullari quyidagi asosiy talablarga javob berishi kerak:

– shifrning mustahkamligi shifrlash algoritmining maxfiyligi bilan emas, kalitning sir saqlanishi bilan ta’minlanadi;

– faqat barcha mumkin bo‘lgan kalitlarni birma-bir to‘liq ko‘rib chiqish orqaligina shifrni yechish mumkinligi;

– kalitlarni birma-bir to‘liq ko‘rib chiqishdagi chekli amallar soniga zamonaviy kompyuterlarda erishib bo‘lmaslik;

– shifrlangan matn hajm jihatdan berilgan matndan juda ham katta bo‘lmasligi;

– shifrlash jarayonida ketma-ket ishlatilayotgan kalitlar oddiy va tezkor aniqlanadigan bog‘liqlikda bo‘lmasligi;

– shifrlash jarayonidagi xatolik axborotning buzilishi va yo‘qolishiga [olib kelmasligi kerak](https://hozir.org/proektorni-noutbukga-ulash.html);

– shifrlash juda ham ko‘p mehnat talab qilmasligi va uning qiymati himoyalanuvchi axborotning qiymati bilan mos kelishi kerak. Ushbu talablarga shifrlash usullaridan: o‘rinlarini almashtirish;

almashtirish; gammalashtirish; analitik o‘zgartirish kabilari javob beradi.

Simmetrik va assimetrik shifrlash

Shifrlash nima

Ba'zi ma'lumotlarni ruxsatsiz shaxslardan yashirish va ruxsat berilgan foydalanuvchilarga maxfiy ma'lumotlarni taqdim etish kerak bo'lganda shifrlash foydali bo'ladi.

Asimmetrik shifrlashning xususiyatlari

Ommaviy-xususiy kalit juftligidan foydalanish quyidagi tarzda ishlatilishi mumkin:

* axborotni himoya qilishning mustaqil vositalari;
* kalitlarni tarqatish moslamasi;
* foydalanuvchi autentifikatsiya vositalari.

Quyidagi afzalliklarga ega:

* maxfiy kalitni xavfsiz joyda saqlash, buning o'rniga ochiq kalit ochiq kanal orqali uzatiladi;
* shifrni hal qilish kaliti faqat bir tomonga ma'lum;
* katta assimetrik tizimda nosimmetrikdan farqli o'laroq kamroq kalitlardan foydalaning.

Bunday algoritmlarga biron bir o'zgartirish kiritish qiyin. Bunday tizim uzoq kalitlarga ega. Agar simmetrik kalit 128 bit bo'lsa, RSA kaliti 2304 bit bo'ladi. Shu sababli, shifrni ochish tezligi yomonlashadi - bu 2-3 baravar sekinroq. Shifrni ochish katta hisoblash resurslarini talab qiladi.

Simmetrik va assimetrik shifrlash tizimlariga ko'plab misollar mavjud.

Simmetrik shifrlash - bu nimaga o'xshaydi?

Simmetrik shifrlash va amalga oshirish sxemasiga misol quyida keltirilgan.

1. Maxfiy ma'lumot almashishni rejalashtirgan ikkita suhbatdosh bor.
2. Birinchi suhbatdosh kalitni hosil qiladi d, shifrlash algoritmlari E va shifrni hal qilish D. Keyin u bu ma'lumotni ikkinchi suhbatdoshga yuboradi.
3. Xabar d kaliti bilan shifrlangan.

Asosiy kamchilik - matnning haqiqiyligini aniqlashning iloji yo'qligi. Agar kalit ushlanib qolsa, tajovuzkor maxfiy ma'lumotni parolini ochadi.

Klassik usullar mavjud.

1. Oddiy va ikki tomonlama almashtirish.
2. Sehrli kvadrat.
3. Yagona almashtirish.

Birinchi usul eng oddiylaridan biri bo'lib, sxemada kalit ishlatilmaydi. Yuboruvchi va qabul qiluvchi jadval o'lchami shaklida taqdim etilgan ma'lum bir kalit bo'yicha kelishib oladilar. O'tkazilgan xabar jadval ustunlariga yoziladi, lekin satr satr o'qiladi. Jadvalning o'lchamini bilgan holda, qabul qiluvchi xabarning shifrini ochadi. Ko'proq maxfiylikni ta'minlash uchun ikki marta almashtirish qo'llaniladi. Shunday qilib, ilgari shifrlangan matnni shifrlash sodir bo'ladi. Buning uchun jadvallar qatorlar va ustunlar sonida farq qilishi kerak. Ular vertikal, gorizontal, ilon, spiral shaklida to'ldiriladi. Bu usul shifrlashni kuchaytirmaydi, lekin yorilish jarayoni uzoqroq davom etadi. "Sehrli kvadrat" - bu matritsa bo'lgan murakkabroq tuzilma. Natural sonlar katakchalarga shunday yozilganki, har bir ustun, qator, diagonal uchun sonlar yig’indisi bir xil bo’ladi. Har bir raqam xabardagi harfga mos keladi. Olingan matn raqamlar va belgilarni solishtirish orqali satrga yoziladi.

Asimmetrik shifrlash misollari

Bunday holda, ochiq kalit ochiq kanal orqali yuboriladi va nazariy jihatdan hujumchilar tomonidan ushlab turilishi mumkin.

Simmetrikdan farqli o'laroq, assimetrik shifrlash kalitlari boshqacha. Ochiq kalit shifrlash uchun ishlatiladi, shaxsiy kalit xabarning shifrini ochish uchun ishlatiladi. Ikkita tugmachadan foydalanish simmetrik usulda bo'lgan interceptability muammosini hal qiladi. U quyidagicha amalga oshiriladi.

1. Birinchi suhbatdosh shifrlash va parolni hal qilish algoritmlarini, bir juft kalitni tanlaydi. Ochiq kalit ikkinchi suhbatdoshga yuboriladi.
2. Ikkinchi suhbatdosh olingan kalit yordamida ma'lumotni shifrlaydi. Maxfiy kalit yordamida xabarni parolini hal qiladigan birinchi chat sherigiga ma'lumot yuboradi.

## Xulosа

XXI-аsr аxborot аsri bo’lgаnligi munosаbаti bilаn O’zbekiston Respublikаsi prezidenti Islom Аbdug’аnievich Kаrimovning “kompyuterlаshtirish vа аxborot texnаlogiyalаrini rivojlаntirish to’g’risidа ”gi 2002yilning 30 mаydаgi fаrmoni vа Vаzirlаr mаhkаmаsining bu fаrmonni аmаliyotdа kuchgа kirishi 2002 yilning 6 iyundаgi qаrori bilаn tаsdiqlаndi. SHu sаbаbli mаmlаkаtimizning turli korxonа vа tаshkilotlаrini vа oliy vа o’rtа mаhsus o’quv yurtlаrini zаmonаviy kompyuterlаr bilаn tа’minlаsh vа bu kompyuterlаrni ishlаtish uchun etuk mutаhаsislаr tаyyorlаsh vа kompyuterlаrni xonаgа joylаshdа mehnаt muxofаzаsi qonun qoidаlаrigа rioya etishni tаlаblаri ishlаb chiqildi. Ungа аmаl qilish hаr bir mutаhаsisning oldigа qo’yilgаn mаqsаd vа vаzifаsidir. Xonа keng, meoyoridа yoritilgаn vа hаvosi oson аlmаshtirilаdigаn bo’lishi kerаk. YOrqin quyosh nurlаri monitorgа sаlbiy tаosir etаdi.Qorong’i xonаdа fаqаt ish joyini yoritish hаm mаqsаdgа muvofiq emаsdir.Stolni shundаy joylаshtiring-ki, derаzа oynаsi qаrshingizdа bo’lmаsin. Аgаr buning iloji bo’lmаsа, u holdа qаlin [pаrdа yoki jаlyuzi sotib oling](https://fayllar.org/sotishni-ragbatlantirish.html), shundа derаzаdаn tushаyotgаn yorug’lik sizgа xаlаl bermаydi. Аgаr oynа yon tomondа bo’lsа, yanа pаrdа yoki jаlyuzi joningizgа oro kiritаdi. CHаng vа issiqliq sаlomаtlikkа putur etkаzibginа qolmаy, texnikаgа hаm yomon tаosir o’tkаzаdi, shuning uchun xonаgа kondisioner o’rnаtgаn mа’qul.

Men yana ushbu diplom ishimda **Shifrlash**-Kriptografik uslublardan foydalanishga asoslangan axborotni oʻzgartirish jarayoni. Axborotni shifrlash uni begonalar tomonidan oʻrganish yoki oʻzgartirish imkoniyatini yoʻqqa chiqaradi. Shuningdek, maʼlumotlarga va dasturlarga, ulardan noqonuniy foydalanish maqsadida, ruxsatsiz raqamli imzo tizimiga kirishning oldini olishni taʼminlaydi. Shifrlashning ikki usuli mavjud: simmetrik va asimmetrik. Simmetrik shifrlashda, kodlash va kodni ochish uchun birgina kalitning oʻzidan foydalaniladi. Asimmetrik shifrlashda ikkita kalitdan foydalaniladi. Ulardan biri (ochiq kalit) dastlabki matnni shifrmatnga oʻgirishni, ikkinchisi esa (yopiq kalit) dastlabki matnga oʻgirishni taʼminlaydi. Samaradorlikni yanada oshirish maqsadida simmetrik va asimmetrik shifrlash algoritmlari birgalikda ishlatiladi. Bu holatda simmetrik shifrlashdan maʼlumotlarni ochiq kanallar orqali uzatishda maʼlumotlarni shifrlashda, asimmetrik shifrlashdan esa simmetrik shifrlash algoritmlarining kalitlarini shifrlashda ishlatiladi. CryptoAPI yordamida simmetrik shifrlash sxemasini amalga oshirish Hozirgi kunda mavjud kriptografik shiyaralash algoritmlarining asosida kriptografik kalit yotadi, shirlash algoritmlarining kriptobardoshliligi aynan shu kalitlarga bogʻliqdir. Shifrlash algoritmlari uchun kalitlarni generatsiya qilishning usullaridan biri bu parollardan (kalit soʻzdan) kriptografik kalit yaratishdir. Ushbu parol oʻzgaruvchan uzunlikda boʻladi va kriptografik kalitdan uzunligi kichik boʻladi. Lekin parol kalit yaratish uchun uncha yaxshi boʻlmagan material hisoblanadi, chunki foydalanuvchilar parol sifatida esda qoluvchi lugʻatlarda mavjud soʻzlardan koʻp foydalanadi, buni esa lugʻat yordamidagi hurujlardan osonlik bilan buzish mumkin. Odatda lugʻat yordamidagi hurujlar 105-106operatsiya yordamida amalga oshiriladi, shu sababli parollardan kalit yasash uzoq vaqt davom etishi kerak, bu vaqt hisoblash mashinalari uchun uzoq sanaladi, foydalanuvchilar uchun esa bilinmaydigan vaqtdir. Agar lugʻatdagi soʻzlar soni N ta, kalitnisaqlash vaqti T boʻlsa, u holdakalitdan parol yaratish uchun ketadigan vaqt t0quyidagi formula orqali hisoblanadi[22]: t0= 2T/N Agar kalitni saqlash muddati oʻrtacha T = 7kun = 6,1 \*105 sekund, lugʻat kattaligi N = 106ta boʻlsa paroldan kalit yaratish vaqti t0 = 1,2 sekunddan kam boʻlmasligi zarur. Agar xavfsizlikning yuqoribosqichi talab etilsa bunday hollarda parol tasodifiy ketma-ketliklardan tashkil topishi zarur. Bunday ketma-ketliklarni kriptoprovayderda CryptGenRandom()funksiyasi yordamida yoki boshqa tasodifiy sonlar datchigidan olish mumkin[23]. Parollar yordamida kalit yaratishning bir qancha shartlari mavjud: - parol ixtiyoriy uzunlikda berilishi mumkin, kalit esa fiksirlangan uzunlikda boʻladi; - bir-biriga oʻxshash va yaqin parollardan, bir-biriga oʻxshamagan va uzoq kalitlar yaratilishi kerak; - turli xil parollar yordamida bir xil kalitlar yaratilmasligi kerak; Bunday shartlar asosida kalit yaratishga xeshlash funksiyalarini ishlatish juda samarali hisoblanadi.Kalitlarning kriptobardoshliligini yanada oshirish maqsadida ushbu mexanizmga „asos“ vektori (salt) va iteratsiyalar sonini qoʻshish mumkin. „Asos“ vektori — tasodifiy ketma-ketlik boʻlib, parol bilan aralashtiriladi. „Asos“ vektorining qoʻllanilishi lugʻat hurujlarini qiyinlashtiradi, ushbu vektorning bugungi kunda tavfsiya etilgan uzunligi 8 bayt Iteratsiyalar soni — bu paroldan kalit yaratish almashtirish funksiyasining qatnashishlar soni. Agar almashtirish funksiyasi sifatida xeshlash funksiyasi ishtirok etsa u holda xeshlash funksiyasi iteratsiyalar soniga teng miqdorda ishtirok etadi. Bugungi kunda iteratsiyalar soni 1000 tadan kam boʻlmasligi zarur. Bu holatda joʻnatuvchi va qabul qiluvchi parollarni oldindan kelishib olishlari zarur. Keltirilgan kalit yaratish mexanizmi orqali foydalanuvchilar quyidagi sxemada koʻrsatilgan kabi maʼlumot almashadi:

Himoyalangan kanal mavjud boʻlmagan holatda kalitlar asimmetrik shifrlash algoritmi yordamida shifrlab joʻnatiladi. Buning uchunxabar joʻnatuvchida qabul qiluvchining ochiq kaliti boʻlishi kerak, ushbu ochiq kalit yordamida shifrlash kaliti asimmetrik shifrlash usulida shifrlanadi va shifrlangan axborot bilan qoʻshib ochiq kanal orqali qabul qiluvchiga uzatiladi.Kalitlar sertifikatlarda yoki konteynerlarda saqlanadi. Shifrlash kalitini esa tasodifiy sonlar generatori orqali yaratiladi. Bu kalit ochiq holatda hech qaerda saqlanmaydi, ushbu kalit bilan bogʻliq barcha operatsiyalar kompyuter tezkor xotirasida amalga oshiriladi. Bunday kalitlar sessiya kaliti deb ham yoritiladi. Sessiya kaliti har bir yangi aloqa boshlanganda bir marta yaratiladi.

**Foydalanilgan adabiyotlar**

1. A.Sattorov “Informatika va axborot tehnologiyalari” Toshkent “O’qituvchi” 2001.
2. A.Abduqodirov va boshqalar “Informatika” Toshkent “Meros”2002.
3. S.Rahmomqulov “IBM PC shaxsiy kompyuterda ishlash” Toshkent “Sharq” 1998.
4. A.Axmedov. N.Tayloqov.”Informatika” Toshkent “O’zbekiston”2001.
5. http:// [www.microsoft.com/](http://www.microsoft.com/)
6. http:// www.ref.uz/
7. http:// www.ziyonet.uz/