PERSONAL ILOVALARI ALGORITMLARI VA ULARNI HIMOYALASH USULLARI

Shaxbos Davronov Erkin o'g'li

Buxoro davlat tibboiyot institute assistenti

Annotatsiya: *Bugungi kunda zamonaviy texnologiyalar jamiyatning istiqbolini belgilovchi muhim unsurlardan biriga aylangan va sohaga bo'lgan talab kun sayin ortib bormoqda. Aksariyat muassasalarda foydalanish bloklangan ko'pchilikga ma'lum ijtimoiy tarmoqlardan farqli o'laroq, tashkilotning personal ilovalari ishchini vaqtini behudaga olmaydi va uni mehnat faoliyatidan chalg'itmaydi. Aksincha aksincha, turli vazifalarni bajarishda yordam beradi. Aynan shundan korporativ ilovalar, ularning funksiyalari hamda xususiyatlari haqida ushbu maqolada so'z yuritiladi.*

Kalit so'zlar: *Simmetrik shifrlash, algoritmlar, internet, ilova, korporativ ilovalar, personal ilovalar, kriptografiya, axborot texnologiyalari.*

Axborotni himoyalashda kriptografiyaning o'rni elektron ko'rinishdagi ma'lumotlarni hajmini ortishi, uni saqlash bilan bog'liq bo'lgan muammolar hajmini ham ortishiga olib keladi. Ushbu muammolarni hal qilishda mavjud bo'lgan usullar esa, kundan-kunga yangilanaveradi. Shunga qarmasdan axborot xavfsizligini ta'minlashda qadimda ham foydalanilagan va hozirda ham foydalanilaètgan usullardan biri bu – kriptografik himoya usullaridir. Kriptografik himoya usullari o'zining ishonchliligi, samaradorligi va foydalanish darajasi qamrovi kengligi bilan boshqa usullardan farq qiladi.[1]

Hozirda axborot xavfsizligini ta'minlashning har bir jabhasida kriptografik usullardan foydalanilmoqda. Bu esa uning muhimligidan darak beradi. Umumiy holda axborot xavfsizligi konsepsiyasi uchta tashkil etuvchidan

[1] A.To'ramaxmudov. "Axborotlarni himoyalash usullari".T: - 2021 y.

iboratligini e’tiborga olsak, axborot xavfsizligini ta’minlash deganda ma’lumotning uchta xususiyatini ta’minlash tushunish mumkin.

Autentifikatsiya jaraèni foydalanuvchini tizimdan foydalanish uchun uni haqiqiyligini tekshirish sanalib, autentifikatsiyalash jaraèni kriptografik usullardin foydalanilgan holatda amalgi oshirilib, bunda kriptografik kalit uzutish protokollari, autentifikatsiyalash protokollari, ma’lumotni autentifikatsiyalash kodlari va hak foydalaniladi. Ushbu jarayonda ham kriptografik himoya usullari o‘zining bardoshligi, ishonchliligi bilan ajralib turadi.

Kriptografiya - axborotlarni aslidan o‘zgartirilgan holatga akslantirish uslublarini topish va takomillashtirish bilan shug‘illanadi. Dastlabki sistemalashgan kriptografik uslublar eramiz boshida, Yuliy Sezarning ish yuritish yozishmalarida uchraydi. U, biror ma’lumotni mahfiy holda, biror kishiga yetkazmoqchi bo‘lsa, alfavitning birinchi harfini alfavitning to‘rtinchi harfi bilan, ikkinchisini beshinchisi bilan va hokazo shu tartibda almashtirib matnning asli holatidan shifrlangan matn holatiga o‘tkazgan.

Axborotlarning muxofazasi masalalari bilan kriptologiya (kryptos-mahfiy, logos - ilm) fani shug‘illanadi. Kriptologiya maqsadlari o‘zaro qarama-qarshi bo‘lgan ikki yo‘nalishga ega: – kriptografiya va kriptoanaliz.

Kriptografiyaning ochiq ma’lumotlarni shifrlash masalalarini matematik uslublari bilan shug‘illanishi to‘g‘risida yuqorida aytib o‘tildi. Kriptoanaliz esa shifirlash uslubini (kalitini yoki algoritmini) bilmagan holda shifrlangan ma’lumotni asli holatini (mos keluvchi ochiq ma’lumotni) topish masalalarini yechish bilan shug‘illanadi.

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

1) Simmetrik kriptotizimlar.

2) Ochiq kalit algoritmiga asoslangan kriptotizimlar.

3) Elektron raqamli imzo kriptotizimlari.

4) Kriptotizimlar uchun kriptobardoshli kalitlarni ishlab chiqish va ulardan foydalanishni boshqarish.

Shifrlash tizimlari foydalaniladigan kalitlar soniga koʻra ikki qismga boʻlinadi: simmetrik va asimmetrik - ochiq kalitli. Simmetrik kriptotizimlarda shifrlash uchun ham va deshifrlash uchun ham bir hil kalitdan foydalaniladi.

Ochiq kalitli kriptotizimlarda ikkita kalitdan foydalaniladi -– oʻzaro matematik bogʻliq boʻlgan ochiq va yopiq kalitlardan. Bunda ma'lumotlar hammaga ma'lum boʻlgan ma'lumot yuborilayotgan shaxsning ochiq kaliti bilan shifrlanadi va faqat ma'lumot yuborilayotgan shaxsning oʻzigagina ma'lum boʻlgan yopiq kalit bilan deshifrlanadi.[2]

Kalitlarni taqsimlash va boshqarish – kriptobardoshli kalitlarni ishlab chiqish (yoki yaratish), ularni muhofazali saqlash, hamda kalitlarni foydalanuvchilar orasida muhofazalangan holda taqsimlash jarayonlarini oʻz ichiga oladi.

Elektron raqamli imzo - elektron matnga ilova qilinadigan kriptografik almashtirishdan iborat boʻlib, shu elektron matn joʻnatilgan shaxsga qabul qilingan elektron matnning va matinni raqamli imzolovchining haqiqiy yoki nohaqiqiy ekanligini aniqlash imkonini beradi.

Shifrlash algoritmlari asoslarini ochiq ma'lumotni ifodalovchi alfavit belgilarini yoki belgilar birikmalarini shifrma'lumotni ifodalovchi alfavit belgilariga yoki belgilar birikmalariga akslantiruvchi matematik modellar tashkil etiladi. Shuning uchun ham shifrlash algoritmlarini sinflarga ajratishning boshlangʻich bosqichi, ular negizidagi akslantirish turlari asosida amalga oshiriladi. Agar shifrlash jarayonida ochiq ma'lumot alfaviti belgilari shifr ma'lumot alfaviti belgilariga almashtirilsa, bunday akslantirishga asoslangan shifrlash algoritmi oʻrniga qoʻyish shifrlash sinfiga kiradi. Agar shifrlash jarayonida ochiq ma'lumot alfaviti belgilarining oʻrinlari almashtirilsa, bunday shifrlash algoritmi oʻrin almashtirish shifrlash sinfiga kiradi.

Koʻrinib turibdiki, oʻrin almashtirish shifrlash algoritmlarida ochiq ma'lumotni tashkil etuvchi alfavit belgilarining ma'nosi shifr ma'lumotda ham oʻzgarmasdan qoladi. Aksincha, oʻrniga qoʻyish shifrlash algoritmlarida

[2] hozir.org

shifrma’lumotni tashkil etuvchi alfavit belgilari ma’nosi ochiq ma’lumotni tashkil etuvchi alfavit belgilarining ma’nosi bilan bir hil bo‘lmaydi. Shifrlash jarayonida o‘rniga qo‘yish va o‘rin almashtirish akslantirishlarining kombinatsiyalaridan birgalikda foydalanilsa, bunday shifrlash algoritmi kompozitsion shifrlash turkumiga kiradi. Demak, shifrlash algoritmlari akslantirish turlariga qarab o‘rniga qo‘yish, o‘rin almashtirish va kompozitsion shifrlash sinfiga bo‘linadi.

Shifrlash algoritmlariga qo‘yiladigan asosiy talablar quyidagilardir:

– shifrlangan axborotni o‘zgartirib qo‘yish yoki shifrni buzib ochishga yo‘l qoldirmaslik;

– axborot himoyasi faqat kalitning ma’lumligiga bog‘liq bo‘lib, algoritmning ma’lum yoki noma’lumligiga bog‘liq bo‘lmaslik (O. Kerkgoff qoidasi);

– dastlabki (shifrlanadigan) axborotni yoki kalitni biroz o‘zgartirish shifrlangan matnni butunlay o‘zgartirib yubo¬rishi lozim (K. Shennon tamoyili, — o‘pirilish hodisasi);

– kalit qiymatlari sohasi shunday katta bo‘lishi kerakki, unda kalit qiymatlarini bir boshdan ko‘rib chiqish asosida shifrni buzib ochish imkoni bo‘lmasligi lozim;

– algoritm iqtisodiy jihatdan tejamli va yetarli tez¬korlikka ega bo‘lishi lozim;

– shifrmatnni buzib ochishga ketadigan sarf-harajatlar axborot bahosidan yuqori bo‘lishi lozim.

Shifrlash algoritmlari, kalitlardan foydalanish turlariga ko‘ra, simmetrik va asimmetrik sinflarga bo‘linadi. Agar shifrlash va deshifrlash jarayonlari bir xil kalit bilan amalga oshirilsa, bunday shifrlash algoritmi simmetrik shifrlash algoritmi sinfiga kiradi. Agar shifrlash jarayoni biror kalit bilan amalga oshirilib, deshifrlash jarayoni bo‘lgan kalit bilan amalga oshirilib, kalitni bilgan holda kalitni topish yechilishi murakkab bo‘lgan masala bilan bog‘liq bo‘lsa, bunday shifrlash algoritmi asimmetrik shifrlash algoritmi sinfiga taaluqli bo‘ladi.

Simmetrik shifrlash algoritmlari ma’lumotni shifrlashda va deshifrlashda aynan bir xil kalitdan foydalanadi. Bunday kriptotizimda kalit aloqaning faqat ikkala tomoni uchun ma’lum, lekin ikkovlaridan boshqa hech kimga oshkora bo‘lmasligi, ya’ni o‘zgalardan mutlaqo maxfiy bo‘lishi shart. Bunday tizimning xavfsizligi asosan yagona maxfiy kalitning himoya xossalariga bog‘liq.

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

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

Hujjatlardagi qo‘yilgan shaxsiy imzolarni sohtalashtirish nisbatan murakkab bo‘lib, shaxsiy imzolarning mualliflarini hozirgi zamonaviy ilg‘or kriminalistika uslublaridan foydalanish orqali aniqlash mumkin. Ammo Elektron raqamli imzo xususiyatlari bundan farqli bo‘lib, ikkilik sanoq sistemasi xususiyatlari bilan belgilanadigan xotira registrlari bitlariga bog‘liq. Xotira bitlarining ma’lum bir ketmaketligidan 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 siivilizatsiyasida hujjatlar, jumladan mahfiy hujjatlarning ham, Elektron ko‘rinishda ishlatilishi va aloqa tizimlarida uzatilishi keng qo‘llanilib borilayotganligi Elektron hujjatlar va

Elektron imzolarning haqiqiyligini aniqlash masalalarining muhimligini keltirib chiqarmoqda.

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

Foydalanilgan adabiyorlar

1. A.To‘ramaxmudov. “Axborotlarni himoyalash usullari”.T: - 2021 y.
2. А. В. Росляков, С. В. Ваняшин, А. Ю. Гребешков. «ИНТЕРНЕТ ВЕЩЕЙ» Учебное пособие. Самара – 2015.
3. Макаров С.Л. «ARDUINO UNO И RASPBERRY PI 3: от схемотехники к интернету вещей». ДМК Пресс – 2019.
4. Перри Ли. «Архитектура интернета». ДМК Пресс – 2019.
5. Mamarajabov M.E. Raqamlashtirilgan ta’lim sharoitida bo‘lajak o‘qituvchilarning kasbiy pedagogik tayyorgarligini takomillashtirish, p.f.d.(DSc) ilmiy darajasini olishga ezilgan dissert.–T.:-2023.- 184 b.
6. Maxmudov A.X., Anarbaeva F.U. Raqamli ta’limda pedagogik texnologiyalarni qo‘llash imkoniyatlari. Development issues of innovative economy in the agricultural sector. 2021.-476 b.
7. Maxmudov A. X., Abduraxmonov Z. B. Ta’limda zamonaviy raqamli texnologiyalaridan foydalanishning yutuqlari va muammolari //Academic research in educational sciences. – 2021. – Т. 2. – №. CSPI conference 3. – S. 97-99.
8. Davronov Sh.E Tibbiyotda axborot texnalogiyalarini o’qitish metodikasi //Educational Research in Universal Sciences. – 2023. – Т. 2. – №. 9. – С. 159-164.
9. Бродовская Е.В., Домбровская А.Ю., Петрова Т.Е., Пырма Р.В., Азаров А.А. Цифровая среда ведущих университетов мира и РФ: результаты сравнителного анализа данных сайтов // Высшее образование в России. 2019. – Т. 28. – № 12. – С. 9–22.

10. Эркин Ш. и др. Технология получения тонкослойных гетероструктур n-cds/p-cef3 и исследование их электрических свойств //Results of National Scientific Research International Journal. – 2022. – Т. 1. – №. 7. – С. 326-338.

11. Khakim Rustamov, Siddiq Qahhorov, талабаларнинг таянч компетенцияларини ривожлантиришда дастурий воситалардан фойдаланишнинг аҳамияти , центр научных публикаций (buxdu.uz): том 34 № 34 (2023): статьи и тезисы (buxdu.uz)

12. Khakim Rustamov, Suhrob Qurbonov, zamonaviy axborot-kommunikatsiya texnologiyalaridan foydalanish ta’lim samaradorligining asosiy omili , центр научных публикаций (buxdu.uz): том 34 № 34 (2023): статьи и тезисы (buxdu.uz)

13. Сиддик Қаҳҳоров, Акмал Жўраев, теоретические основы использования программированных образовательных инструментов в профессиональной подготовке преподавателей технологии будущего , центр научных публикаций (buxdu.uz): том 2 № 2 (2020): педагогические мастерство (buxdu.uz)

14. http://uz.infocom.uz/

15. https://en.wikipedia.org/