# ELEKTRON RAQAMLI IMZO VA MUHRNING ISHLASH PRINSIPI

**Davlatova Sayyora Toshpulatovna**
TDMAU Katta o`qituvchisi PhD.
*davlatovqsayyora@gmail.com.*
ORSID: 0009-0001-9605-2192

*https://doi.org/10.5281/zenodo.19224753*

***Annotatsiya.*** *Ushbu maqola elektron raqamli imzo va muhrning ishlash prinsipi, qo`llanilish sohalari, kelajakdagi o`rni haqida yozilgan. Elektron raqamli imzoning qo`llanilish oshalari haqida keng ma'lumot berilgan.*

***Kalit so`z:*** *electron, raqamli, prinsip, ochiq kalit, kriptografik, imzo.*

Elektron raqamli imzo (ERI) — bu elektron hujjatning haqiqiyligini, yaxlitligini va muallifini tasdiqlovchi kriptografik vositadir. U an'anaviy qo'l imzosining raqamli shakli hisoblanadi. Elektron raqamli imzo (ERI) — elektron hujjatdagi ma'lumotlarni kriptografik o'zgartirish orqali hosil qilinadigan, hujjat muallifini identifikatsiya qilish va uning butunligini tasdiqlovchi belgilar ketma-ketligidir. Qog'oz hujjatdagi shaxsiy imzo bilan bir xil yuridik kuchga ega bo'lib, u yopiq kalit (imzolash) va ochiq kalit (tekshirish) orqali ishlaydi.

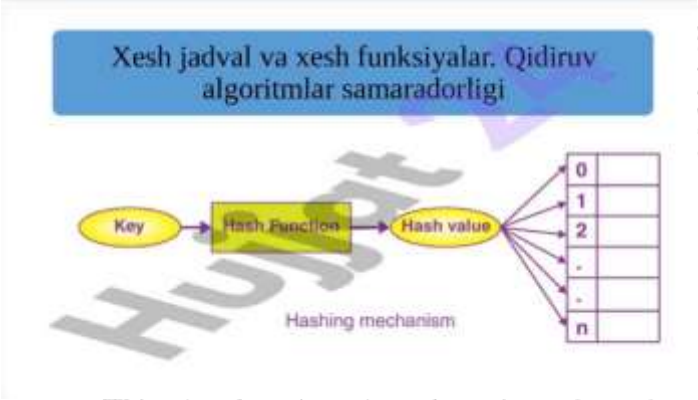
ERI yordamida: hujjat o'zgartirilmaganligi aniqlanadi, kim tomonidan yuborilganligi tasdiqlanadi. Hujjat rad etilmaydi (inkor etib bo'lmaydi)

**ERI ning ishlash prinsipi**

ERI kriptografiya asosida ishlaydi, ayniqsa assimetrik shifrlash usuliga tayangan holda. \

ERI jarayoni quyidagicha amalga oshiriladi:

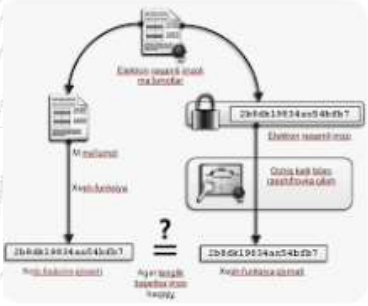
1-bosqich: Hujjatni xeshlash




Hujjat maxsus algoritm yordamida qisqa kodga aylantiriladi (hash).

Masalan: SHA-256 algoritmi.

2-bosqich: Imzo yaratish



sudex.uz
Elektron imzo tushunchasi va ...

Gazeta.uz
Elektron raqamli imzo olish. Qo'llanma – O'zbekisto...

Hosil bo‘lgan hash qiymat foydalanuvchining yopiq kaliti yordamida shifrlanadi — bu elektron imzo hisoblanadi.

3-bosqich: Tekshirish

Qabul qiluvchi tomon:

hujjatdan yana hash hosil qiladi

imzoni ochiq kalit bilan deshifrlaydi

ikkala hashni solishtiradi

Agar mos kelsa — hujjat haqiqiy.

**Ochiq va yopiq kalitlar tushunchasi**

Assimetrik kriptografiyada ikki xil kalit ishlatiladi:

Yopiq kalit (Private key) — faqat egasida bo‘ladi va imzo qo‘yishda ishlatiladi

Ochiq kalit (Public key) — hammaga ochiq bo‘ladi va imzoni tekshirish uchun ishlatiladi

Mashhur algoritmlardan biri — RSA algoritmi.

**Elektron muhr (raqamli muhr) tushunchasi**

Elektron muhr — bu tashkilot yoki yuridik shaxs tomonidan qo‘llaniladigan raqamli tasdiqlash vositasi.


adliya.uz
Muhr va shtamplardan xavf...


КиберЛенинка
ELEKTRON HUKUMAT VA INTERAKTIV ...

Farqli jihati:

ERI — shaxsga tegishli

Elektron muhr — tashkilotga tegishli

Elektron muhr hujjatning tashkilot tomonidan tasdiqlanganligini bildiradi.

**ERI va elektron muhr o‘rtasidagi farq**

Belgilar ERI

Elektron muhr, Kimga tegishli, Jismoniy shaxs, Yuridik shaxs

Maqsadi, Shaxsni tasdiqlash, Tashkilotni tasdiqlash, Qo‘llanishi

Shaxsiy hujjatlar, Rasmiy hujjatlar, Javobgarlik, Shaxsiy, Tashkilot.

6. Afzalliklari va qo‘llanilishi

Afzalliklari:

Xavfsizlik yuqori

Hujjatni qalbakilashtirish qiyin

Tezkor va qulay

Masofadan ishlash imkoniyati

Qo‘llanilish sohalari:

Elektron hukumat tizimlari

Bank va moliya tizimlari

Onlayn shartnomalar

Soliq va hisobot tizimlari

Elektron raqamli imzo va muhr zamonaviy axborot xavfsizligining ajralmas qismi bo‘lib, ular orqali elektron hujjatlar ishonchliligi ta’minlanadi. Ular kriptografik usullarga asoslanib, axborotni himoyalashda muhim rol o‘ynaydi.

**Foydalanilgan adabiyotlar**

1. Stallings W. Cryptography and Network Security
2. NIST kriptografiya standartlari
3. Menezes A. Handbook of Applied Cryptography
4. O‘zbekiston Respublikasi “Elektron raqamli imzo to‘g‘risida”gi qonuni
5. Schneier B. Applied Cryptography
6. Axborot xavfsizligi bo‘yicha o‘quv qo‘llanmalar