RAQAMLI IMZO TEXNOLOGIYASI: KRIPTOGRAFIK ASOSLAR VA ZAMONAVIY ALGORITMLAR TAHLILI

Akbarova Gulzoda Karimovna
Andijon shaxar 4-son texnikumi
maxsus fan katta o‘qituvchisi

Annotatsiya. Mazkur maqolada raqamli imzo texnologiyasining kriptografik asoslari, ishlash mexanizmi, asosiy algoritmlari (RSA, DSA, ECDSA) hamda zamonaviy rivojlanish yo‘nalishlari tahlil qilinadi. Shuningdek, xesh-funksiyalar, ochiq kalitli kriptografiya va xavfsizlik xususiyatlari ilmiy nuqtai nazardan yoritiladi.

Kalit so‘zlar: raqamli imzo, kriptografiya, RSA, DSA, ECDSA, xesh-funksiya, autentifikatsiya, axborot xavfsizligi

Abstract. This article analyzes the cryptographic foundations of digital signature technology, its mechanism of operation, main algorithms (RSA, DSA, ECDSA), and modern development trends. It also discusses hash functions, public-key cryptography, and security features from a scientific perspective.

Keywords: digital signature, cryptography, RSA, DSA, ECDSA, hash function, authentication, information security

Kirish

Axborot texnologiyalarining rivojlanishi natijasida elektron hujjatlar almashinuvi global miqyosda keng qo‘llanilmoqda. Shu bilan birga, elektron axborotning haqiqiyligi va yaxlitligini ta’minlash muammosi dolzarb bo‘lib qolmoqda. Ushbu muammoni hal etishda raqamli imzo texnologiyasi muhim vosita sifatida qaraladi.

Raqamli imzo — bu matematik kriptografik mexanizm bo‘lib, elektron hujjatlarning haqiqiyligini, yaxlitligini va muallifini tasdiqlash imkonini beradi.

Raqamli imzoning kriptografik asoslari

Raqamli imzo ochiq kalitli kriptografiya (asymmetric cryptography) asosida ishlaydi. Ushbu modelda ikkita kalit mavjud:

- **Yopiq (private) kalit** — imzo yaratish uchun ishlatiladi
- **Ochiq (public) kalit** — imzoni tekshirish uchun ishlatiladi

Raqamli imzo quyidagi uchta asosiy xavfsizlik xususiyatini ta’minlaydi:

1. **Autentifikatsiya** – yuboruvchini aniqlash
2. **Yaxlitlik (Integrity)** – ma’lumot o‘zgarmaganligini kafolatlash
3. **Rad etib bo‘lmaslik (Non-repudiation)** – yuboruvchi imzoni inkor eta olmaydi. (techtarget.com)[1].

Zamonaviy jamiyat rivojlanib borayotgan sari, turli sohalarda raqamlashtirish jarayoni tezlashmoqda. Shu jarayon natijasida elektron hujjatlar va ularni tasdiqlash vositalari tobora ommalashib bormoqda. Elektron raqamli imzo (ERI) ana shu vositalarning muhim turlaridan biri hisoblanadi. ERI hujjatning muallifligini tasdiqlash, uning o‘zgarmasligini kafolatlash va yuridik kuchini oshirishda muhim vosita hisoblanadi.

Elektron raqamli imzo huquqiy hujjat sifatida O‘zbekiston Respublikasi qonunchiligida ham mustahkam o‘rin egallagan. Xususan, 2003-yilda qabul qilingan “Elektron raqamli imzo to‘g‘risida”gi Qonun bilan uning yuridik maqomi va qo‘llash tartibi belgilanib qo‘yilgan. Shu bilan birga, xalqaro amaliyotda ham elektron raqamli imzo ko‘plab mamlakatlarda qo‘llanilib, hujjat muomalasining ajralmas qismi sifatida tan olingan.[2]

1. Elektron raqamli imzo tushunchasi va asoslari

Elektron raqamli imzo (ERI) – elektron hujjatga qo‘yilgan, maxsus kriptografik algoritmlar asosida yaratilgan va uni yaratgan shaxsning shaxsi hamda hujjatning yaxlitligini tasdiqlovchi raqamli koddir. ERI shaxsning elektron muomaladagi ishonchli identifikatori bo‘lib xizmat qiladi. Shu orqali elektron hujjatlar ham qog‘oz shaklidagi hujjatlar kabi yuridik kuchga ega bo‘lishi ta’minlanadi.[4,5]

Qonuniy jihatdan ERI quyidagilarga asoslanadi:

- Elektron hujjatning haqiqiyligini kafolatlash – ERI orqali hujjat muallifi aniq belgilanadi.
- Elektron hujjatning yaxlitligini ta’minlash – ERI qo‘yilgan hujjat o‘zgartirilmaganligini kafolatlaydi.

- Rad etib bo‘lmaslik prinsipi – hujjat muallifi uni imzolaganligini keyinchalik rad eta olmaydi.

Shu tarzda, elektron raqamli imzo shaxsiy identifikatsiya, hujjatning o‘zgarmasligini ta’minlash va yuridik kuchini mustahkamlash kabi asosiy vazifalarni bajaradi.

2. ERIning ishlash prinsipi

Elektron raqamli imzo ikki asosiy kalitga tayangan holda ishlaydi: maxfiy kalit va ochiq kalit. Bu usul asimmetrik kriptografiya deb ataladi.

- Maxfiy kalit – faqat imzo qo‘yuvchi shaxsda bo‘ladi. Shu kalit orqali elektron hujjatning imzosi yaratiladi.
- Ochiq kalit – barcha uchun ochiq bo‘lib, imzo to‘g‘riligini tekshirish uchun ishlatiladi.

ERI yaratish jarayoni quyidagicha bo‘ladi:

1. Elektron hujjatdan xesh qiymati olinadi (maxsus xesh-funksiya orqali).
2. Olingan xesh qiymati maxfiy kalit bilan shifrlanadi.
3. Shu shifrlangan xesh qiymati elektron raqamli imzo sifatida hujjatga qo‘yiladi.

Imzo tekshirilayotganda esa ochiq kalitdan foydalaniladi: shifrlangan xesh ochiladi va hujjatdan qayta olingan xesh qiymati bilan solishtiriladi. Agar ular mos tushsa, hujjat o‘zgarmagan va haqiqiy deb topiladi.

Bugungi kunda ERI yaratishda keng tarqalgan RSA, DSA, SHA-256 kabi algoritmlar qo‘llaniladi. Ular ma’lumotlarning maxfiyligi va yaxlitligini ishonchli tarzda ta’minlaydi.

3. Elektron raqamli imzoning qo‘llanilishi

Hozirda elektron raqamli imzo turli sohalarda muvaffaqiyatli qo‘llanmoqda:

3.1. Davlat xizmatlari

Davlat xizmatlarini elektron shaklda ko‘rsatishda ERI muhim rol o‘ynaydi. Masalan, O‘zbekistonning Yagona interaktiv davlat xizmatlari portali orqali turli arizalar, shartnomalar va so‘rovnomalar elektron shaklda yuboriladi. Shu bilan birga, davlat idoralari ham o‘zaro hujjat almashishda ERI asosida ishlaydi.

3.2. Moliya va bank sohasi

Bank sohasida ERI hisob-kitoblarni amalga oshirish, shartnomalarni tasdiqlash va boshqa muhim jarayonlarda ishonchli vosita sifatida qo‘llanadi. Elektron bank xizmatlari, onlayn to‘lovlar va elektron hisobvaraq-fakturalar ERI orqali yuridik kuchga ega bo‘ladi.

3.3. Savdo va shartnomalar

Elektron savdo tizimlari va elektron shartnomalar imzolashda ham ERI hujjatning yuridik maqomini ta’minlab beradi. Bu esa biznes jarayonlarini soddalashtiradi va hujjat muomalasini tezlashtiradi.

4. ERIning afzalliklari va ahamiyati

Elektron raqamli imzo quyidagi afzalliklarga ega:

Hujjat muomalasini tezlashtiradi va qulaylik yaratadi.

Qog‘oz hujjatlar va pochta xarajatlarini kamaytiradi.

Hujjatlar xavfsizligini va maxfiyligini oshiradi.

Shaxsiy identifikatsiya va hujjat yaxlitligini kafolatlaydi.

Sud va boshqa yuridik muammolar yuzaga kelganda ishonchli dalil sifatida xizmat qiladi.[3,4]

Shu sababli, ERI zamonaviy iqtisodiyot va huquqiy muhitda yuridik hujjatlar aylanmasini soddalashtirish va ishonchli qilishning muhim vositasidir.

Elektron raqamli imzo – zamonaviy jamiyatning ajralmas qismi bo‘lib, hujjat muomalasida xavfsizlik, tezkorlik va ishonchlilikni ta’minlaydi. U shaxsiy identifikatsiya, hujjat yaxlitligi va yuridik kuchni mustahkamlashga xizmat qiladi. Bugungi kunda ERI davlat va biznes sohalarida, shuningdek, kundalik turmushda ham keng qo‘llanilmoqda.

O‘zbekiston Respublikasi qonunchiligi va xalqaro tajriba asosida elektron raqamli imzo kelajakda ham hujjat muomalasining yirik va barqaror qismi bo‘lib qoladi. Shu bois, uni to‘g‘ri qo‘llash va rivojlantirish davlat va jamiyatning asosiy vazifalaridan biri hisoblanadi.

7. Xulosa

Raqamli imzo texnologiyasi zamonaviy axborot xavfsizligining asosiy komponentlaridan biri hisoblanadi. Uning matematik asoslari va kriptografik algoritmlari

yuqori darajadagi ishonchlilikni ta’minlaydi. Kelajakda post-kvant kriptografiya va yangi algoritmlar ushbu sohani yanada rivojlantirishi kutilmoqda.

Adabiyotlar ro‘yxati

1. TechTarget. (2024). *Digital signature definition*. https://www.techtarget.com (techtarget.com)
2. ScienceDirect. (2021). *Digital signature – overview*. Elsevier. (ScienceDirect)
3. GeeksforGeeks. (2025). *Digital Signature Algorithm (DSA)*. (GeeksforGeeks)
4. ScienceDirect. (2022). *Digital signature scheme*. Elsevier. (ScienceDirect)
5. SEAL Systems. (2023). *Digital signature cryptography basics*. (SEAL Systems AG)