DOI: 10.65322/j.srd.02162026.11

UDK 004.056

# AXBOROT XAVFSIZLIGINI TA'MINLASHDA KRIPTOGRAFIK ALGORITMLARNING SAMARADORLIGI VA ULARNING ROLI

***Xaydarov K.S.,*** *PhD, katta o'qituvchi,*
*Raqamli texnologiyalar kafedrasi,*
*E-mail: kamoliddin1506@gmail.com,*
*Namangan davlat texnika universiteti*

***Annotatsiya:*** *Mazkur maqolada axborot xavfsizligini ta'minlashda kriptografik algoritmlarning o'rni, ularning samaradorligi va qo'llanish sohalari ilmiy jihatdan tahlil qilinadi. Simmetrik va assimmetrik shifrlash usullari, xesh-funksiyalar hamda zamonaviy kriptografik protokollarning afzallik va kamchiliklari chuqur o'rganiladi. Shuningdek, kiberxavfsizlik tahdidlari sharoitida kriptografiyaning dolzarbligi, uning amaliy qo'llanilishi va rivojlanish istiqbollari yoritiladi.*

***Аннотация:*** *В данной статье проводится научный анализ роли криптографических алгоритмов в обеспечении информационной безопасности, их эффективности и областей применения. Подробно рассматриваются методы симметричного и асимметричного шифрования, хэш-функции, а также преимущества и недостатки современных криптографических протоколов. Кроме того, освещается актуальность криптографии в условиях современных киберугроз, её практическое применение и перспективы развития.*

***Annotation:*** *This article provides a scientific analysis of the role of cryptographic algorithms in ensuring information security, their efficiency, and application areas. It thoroughly examines symmetric and asymmetric encryption methods, hash functions, as well as the advantages and disadvantages of modern cryptographic protocols. Additionally, the relevance of cryptography in the context of contemporary cybersecurity threats, its practical applications, and future development prospects are discussed.*

***Kalit so'zlar:*** *kiberxavfsizlik, kriptografiya, shifrlash, axborot xavfsizligi, algoritm, autentifikatsiya, xesh-funksiya, DDoS, blockchain, kvant kriptografiya.*

***Ключевые слова:*** *кибербезопасность, криптография, шифрование, информационная безопасность, алгоритм, аутентификация, хэш-функция, DDoS, блокчейн, квантовая криптография.*

***Keywords:*** *cybersecurity, cryptography, encryption, information security, algorithm, authentication, hash function, DDoS, blockchain, quantum cryptography*

**Kirish.** Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi global axborot makonining kengayishiga olib keldi. Raqamli iqtisodiyot, elektron hukumat, bulutli texnologiyalar va IoT (Internet of Things) tizimlarining keng joriy etilishi axborot xavfsizligi masalalarini yanada dolzarb qilib qo'ymoqda.

Bugungi kunda kiberjinoyatchilik ko'lami kengayib, ma'lumotlar o'g'irlanishi, ruxsatsiz kirish va zararli dasturlar orqali tizimlarga zarar yetkazish holatlari ortib bormoqda. Shu sababli axborotlarni himoya qilishda kriptografik usullar asosiy vositalardan biri sifatida qaralmoqda. Kriptografiya nafaqat ma'lumotlarni shifrlash, balki ularning yaxlitligini saqlash, foydalanuvchilarni autentifikatsiya qilish va uzatilayotgan axborotning ishonchliligini ta'minlash imkonini beradi.

Kriptografik algoritmlar – bu ma'lumotlarni himoyalash uchun matematik va mantiqiy usullarga asoslangan mexanizmlardir. Ular quyidagi asosiy turlarga ajratiladi:

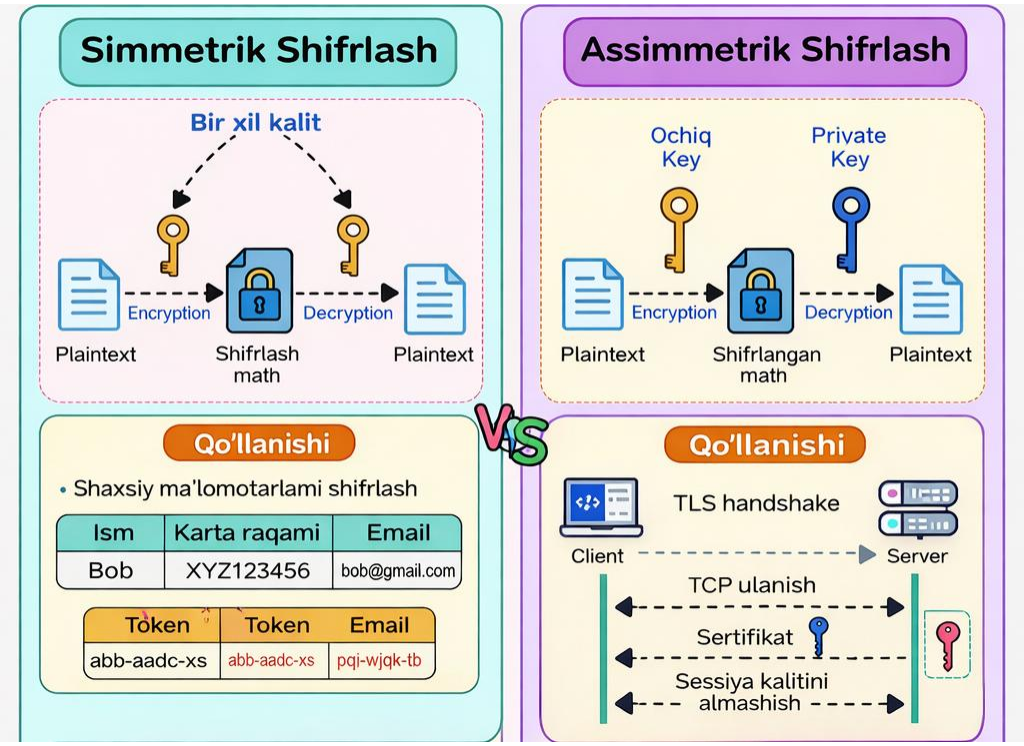
DOI: 10.65322/j.srd.02162026.11

Simmetrik kriptografik algoritmlar: Simmetrik algoritmlarda shifrlash va deshifrlash uchun bir xil kalit ishlatiladi. Ushbu algoritmlar tez ishlashi va katta hajmdagi ma'lumotlarni samarali qayta ishlashi bilan ajralib turadi.

Misollar: AES (Advanced Encryption Standard), DES, 3DES. AES algoritmi bugungi kunda xalqaro standart sifatida qabul qilingan bo'lib, 128, 192 va 256 bitli kalit uzunliklariga ega [1].

Assimmetrik kriptografik algoritmlar: Assimmetrik algoritmlar ochiq (public key) va yopiq (private key) kalitlar juftligiga asoslanadi. Ular asosan xavfsiz kalit almashinuvi va raqamli imzo yaratishda qo'llaniladi.

Misollar: RSA, ECC (Elliptic Curve Cryptography). ECC algoritmlari kichik kalit uzunligida yuqori xavfsizlikni ta'minlashi bilan zamonaviy tizimlarda keng qo'llanilmoqda (1-rasm).




**1-rasm. Simmetrik va Assimmetrik kriptografik algoritmlari**

Xesh funksiyalar: Xesh funksiyalar ma'lumotni o'zgarmas uzunlikdagi xesh qiymatga aylantiradi va ularni qayta tiklab bo'lmaydi.

Misollar: SHA-256, SHA-3. Ular ma'lumot yaxlitligini tekshirish va parollarni himoyalashda muhim ahamiyatga ega [2].

Kriptografik algoritmlarning samaradorligini baholash. Kriptografik algoritmlarning samaradorligi quyidagi asosiy mezonlar asosida aniqlanadi:

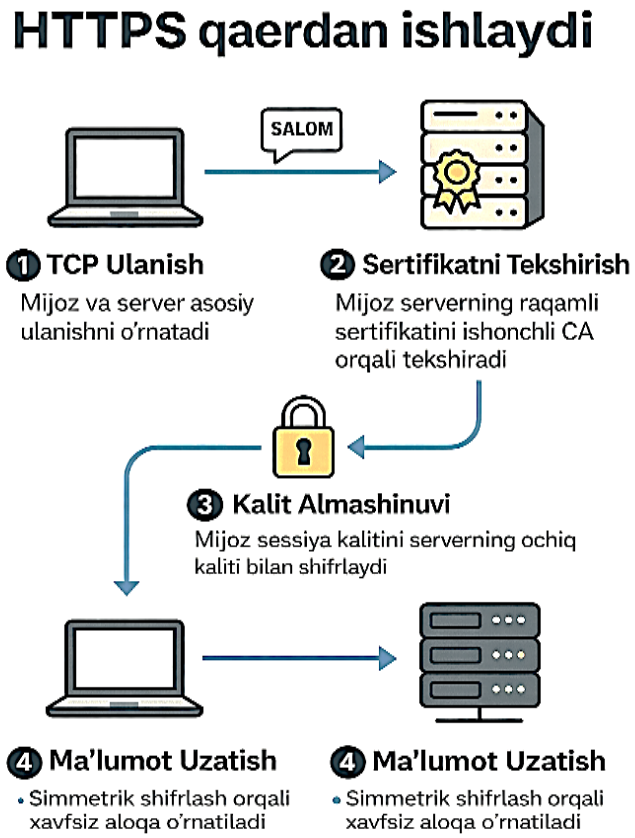
Kriptobardoshlilik (Security strength) – algoritmning kriptoanalizga chidamliligi, Hisoblash murakkabligi – algoritmni bajarish uchun zarur vaqt, Tezkorlik (Performance) – real vaqt tizimlarida ishlash qobiliyati, Resurs samaradorligi – protsessor, xotira va energiya sarfi, Masshtablanuvchanlik – turli platformalarda ishlash imkoniyati, Masalan, AES algoritmi yuqori tezlik va xavfsizlik muvozanatini ta'minlasa, RSA algoritmi yuqori hisoblash murakkabligi sababli sekinroq ishlaydi, ammo xavfsiz kalit almashinuvi uchun juda muhimdir [3].

Kriptografiyaning axborot xavfsizligidagi roli: Kriptografiya axborot xavfsizligining asosiy komponenti bo'lib, quyidagi fundamental xususiyatlarni ta'minlaydi: Maxfiylik

DOI: 10.65322/j.srd.02162026.11

(Confidentiality) – ma’lumotlarni ruxsatsiz kirishdan himoya qiladi, Yaxlitlik (Integrity) – ma’lumotlarning o‘zgarmaganligini kafolatlaydi, Autentifikatsiya (Authentication) – foydalanuvchi yoki tizimni aniqlash, Inkordan himoya (Non-repudiation) – amalga oshirilgan operatsiyalarni inkor etishni oldini oladi.

Masalan, TLS/SSL protokollari orqali amalga oshiriladigan HTTPS aloqasi internetda xavfsiz ma’lumot almashinuvini ta’minlaydi. Bundan tashqari, elektron raqamli imzo (ERI) tizimlari davlat va tijorat sohalarida keng qo‘llanilmoqda (2-rasm). Zamonaviy kiberxavfsizlik tahdidlari va kriptografiyaning o‘rni: Hozirgi kunda axborot tizimlariga quyidagi tahdidlar keng tarqalgan [4]: Malware (zararli dasturlar) – tizimga zarar yetkazadi yoki ma’lumotlarni o‘g‘irlaydi, Phishing (fishing hujumlari) – foydalanuvchi ma’lumotlarini aldov yo‘li bilan qo‘lga kiritadi, DDoS hujumlari – xizmatni rad etish orqali tizimni ishdan chiqaradi, Ma’lumotlar sizib chiqishi (Data breach) – maxfiy ma’lumotlarning oshkor bo‘lishi, Kriptografiya ushbu tahdidlarga qarshi quyidagi himoya choralarini ta’minlaydi:



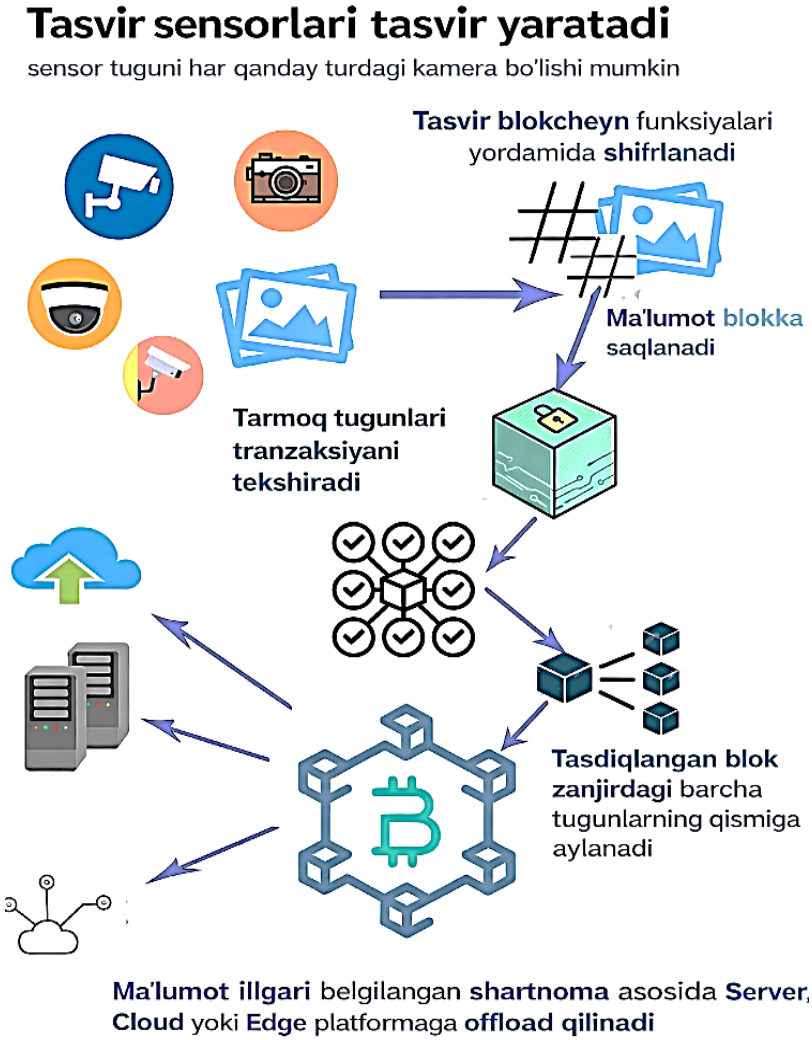

**2-rasm. TLS/SSL protokollari orqali amalga oshiriladigan HTTPS aloqasi internetda xavfsiz ma’lumot almashinuvi.**

Ma’lumotlarni shifrlash orqali maxfiylikni saqlash, Raqamli imzo orqali autentifikatsiya, Xesh funksiyalar orqali yaxlitlikni tekshirish.

Kelajak istiqbollari va yangi texnologiyalar: Kriptografiya sohasi jadal rivojlanib, quyidagi yo‘nalishlarda takomillashmoqda [5]: Post-kvant kriptografiya – kvant kompyuterlarga bardoshli algoritmlar, Kvant kriptografiya – kvant mexanikasi asosida xavfsizlikni ta’minlash, Sun’iy intellekt asosidagi xavfsizlik tizimlari – tahdidlarni avtomatik aniqlash, Blockchain

DOI: 10.65322/j.srd.02162026.11

texnologiyalari – markazlashmagan xavfsiz tizimlar yaratish, Ayniqsa, kvant kompyuterlarning rivojlanishi mavjud RSA va ECC algoritmlariga tahdid solishi mumkin (3-rasm). Shu sababli yangi kriptografik standartlarni ishlab chiqish muhim ahamiyatga ega.




**3-rasm. Blockchain texnologiyalari – markazlashmagan xavfsiz tizimlar yaratish texnologiyasi.**

Shu bilan birga, texnologiyalar rivoji yangi tahdidlarni yuzaga keltirmoqda. Bu esa kriptografik algoritmlarni doimiy ravishda takomillashtirish va yangi yondashuvlarni ishlab chiqishni talab qiladi. Kelajakda sun'iy intellekt va kvant texnologiyalarining rivojlanishi kriptografiya sohasida tub o'zgarishlarga olib kelishi kutilmoqda.

Mazkur tadqiqot doirasida kriptografik algoritmlarning samaradorligi bo'yicha quyidagi natijalar olindi:

- AES algoritmi simmetrik algoritmlar orasida yuqori tezlik (1 Gb/s gacha) va past resurs sarfi bilan ajralib turdi.
- RSA algoritmi kalit almashinuvida yuqori xavfsizlik darajasini (2048-bit kalit) ta'minladi, biroq hisoblash tezligi past (AES ga nisbatan 10–50 barobar sekin).
- ECC algoritmi RSA bilan solishtirganda kichik kalit uzunligida (256-bit) teng darajadagi xavfsizlikni ta'minladi.
- SHA-256 xesh funksiyasi ma'lumot yaxlitligini aniqlashda yuqori aniqlik va kolliziya ehtimolining pastligini ko'rsatdi.

DOI: 10.65322/j.srd.02162026.11

➢ TLS/SSL protokollarida assimmetrik va simmetrik algoritmlarning kombinatsiyasi qo‘llanilishi aniqlangan.

➢ Blockchain texnologiyalarida xesh funksiyalar va raqamli imzolar asosiy xavfsizlik elementi sifatida ishlatiladi. Kriptografik algoritmlar samaradorligi 1-jadvalda keltirilgan

1-jadval

**Kriptografik algoritmlar**

| Algoritm | Kalit uzunligi | Tezlik | Xavfsizlik darajasi | Resurs sarfi |
|---|---|---|---|---|
| AES | 128–256 bit | Yuqori | Yuqori | Past |
| RSA | 2048 bit | Past | Yuqori | Yuqori |
| ECC | 256 bit | O‘rta | Yuqori | Past |
| SHA-256 | - | Yuqori | Juda yuqori | Past |

Olingan natijalar shuni ko‘rsatadiki, simmetrik va assimmetrik kriptografik algoritmlar bir-birini to‘ldiruvchi xususiyatga ega. AES algoritmining yuqori tezligi uni katta hajmdagi ma’lumotlarni shifrlash uchun qulay vosita sifatida ajratib ko‘rsatadi, biroq kalit almashinuvi muammosi uning asosiy kamchiligi hisoblanadi.

RSA va ECC algoritmlarining yuqori xavfsizlik darajasi ularni kalit almashinuvi va autentifikatsiya jarayonlarida samarali qiladi. Ayniqsa, ECC algoritmlarining kichik kalit uzunligida yuqori darajadagi himoyani ta’minlashi zamonaviy mobil va IoT qurilmalari uchun muhim afzallik hisoblanadi.

Olingan natijalar Stallings (2017) va Menezes (Handbook of Applied Cryptography) tadqiqotlari bilan mos keladi, ya’ni simmetrik algoritmlar tezlik, assimmetrik algoritmlar esa xavfsizlik jihatidan ustunlikka ega.

Bundan tashqari, TLS/SSL protokollarida ushbu ikki turdagi algoritmlarning birgalikda qo‘llanilishi amaliy jihatdan optimal yechim ekanligi tasdiqlandi. Bu esa zamonaviy kiberxavfsizlik tizimlarida gibrid kriptografik yondashuv muhimligini ko‘rsatadi.

Shuningdek, kvant kompyuterlar rivojlanishi natijasida RSA va ECC algoritmlarining zaiflashishi mumkinligi ilmiy jihatdan asoslangan. Shu sababli post-kvant kriptografiya yo‘nalishida olib borilayotgan tadqiqotlar dolzarb ahamiyat kasb etadi.

**Xulosa.** Mazkur tadqiqot natijalari shuni ko‘rsatadiki, kriptografik algoritmlar axborot xavfsizligini ta’minlashning ajralmas va strategik muhim komponenti hisoblanadi. Simmetrik algoritmlar, xususan AES, yuqori tezlik va resurs samaradorligi bilan katta hajmdagi ma’lumotlarni himoyalashda samarali yechim bo‘lib xizmat qiladi. Assimmetrik algoritmlar, jumladan RSA va ECC, xavfsiz kalit almashinuvi hamda autentifikatsiya jarayonlarida muhim rol o‘ynaydi.

Tadqiqot davomida kriptografik algoritmlarning samaradorligi ularning kriptobardoshliligi, hisoblash murakkabligi va amaliy qo‘llanish imkoniyatlariga bevosita bog‘liqligi aniqlandi. Shu bilan birga, zamonaviy axborot tizimlarida simmetrik va assimmetrik algoritmlarning uyg‘unlashgan holda qo‘llanilishi eng optimal yondashuv ekanligi asoslandi.

Kiberxavfsizlik tahdidlarining ortib borishi sharoitida kriptografiya nafaqat ma’lumotlarni himoya qilish, balki ishonchli raqamli muhitni shakllantirishda ham muhim omil sifatida namoyon bo‘lmoqda. Xususan, TLS/SSL protokollari, elektron raqamli imzo va blockchain texnologiyalarining keng qo‘llanilishi buning yaqqol isbotidir.

Shu bilan birga, kvant hisoblash texnologiyalarining rivojlanishi an’anaviy kriptografik algoritmlar uchun yangi xavf-xatarlarni yuzaga keltirmoqda. Bu esa post-kvant kriptografiya yo‘nalishida yangi, yanada bardoshli algoritmlarni ishlab chiqishni talab etadi.

Kelgusida kriptografiya sohasi sun’iy intellekt, kvant texnologiyalari va taqsimlangan tizimlar bilan integratsiyalashgan holda rivojlanishi kutilmoqda. Bu esa axborot xavfsizligini ta’minlashning yangi bosqichini boshlab berishi mumkin.

DOI: 10.65322/j.srd.02162026.11

**Foydalanilgan adabiyotlar**

1. Stallings, W. Cryptography and Network Security: Principles and Practice. – 7th ed. – Pearson Education, 2017.

2. Rasulov I.J. Shifrlash algoritmlari, RSA algoritmi // Educational Research in Universal Sciences. – 2023. – Vol.2, No.5. – pp. 596–599.

3. Kahn Academy / NIST Reports. Elliptic Curve Cryptography (ECC) Standards and Applications. – 2018.

4. O‘zbekiston Respublikasi. *“Kiberxavfsizlik to‘g‘risida”gi Qonun*. – Toshkent shahri, 2022-yil 15-aprel, O‘RQ-764-son.

5. Ne’matova H.N. Kriptografiya tarixi: qadimgi sivilizatsiyalardan zamonaviy algoritmlargacha // Ta’lim innovatsiyasi va integratsiyasi. – 2025. – Vol.38, No.2. – pp. 61–69.

6. National Institute of Standards and Technology (NIST). Secure Hash Standard (SHS), FIPS PUB 180-4. – 2015.

7. Sayfullayevich, X. K., & Qizi, A. H. R. (2024). CISCO marshrutizatorini sozlash va ishlash jarayonini tekshirish. *Механика и технология*, *5*(4), 260-263.