Yuldashev Shamsiddin Mamarajabovich,
fizika-matematika fanlari bo‘yicha falsafa doktori

Abdullayev Baxtiyor Panji o‘g‘li

Eng kuchli shifrlash algoritmlari: zamonaviy xavfsizlikning asosiy tayanchi

Introduction

Raqamli axborot davrida ma’lumotlar xavfsizligi tobora muhim ahamiyat kasb etmoqda. Bugungi raqamli davrda axborot har bir daqiqada almashiladi, uzatiladi va saqlanadi. Internet orqali yuborilayotgan har bir xat, bankdagi tranzaktsiya yoki shaxsiy hujjat himoyasiz bo‘lsa, turli tahdidlar ostida qoladi. Shu sababli axborotni himoyalashda shifrlash (kryptografiya) muhim vosita hisoblanadi. Shifrlash algoritmlari axborotni ruxsatsiz kirishlardan himoya qiladi. Ular ma’lumotlarni shifrlangan shaklga aylantirib, faqat maxsus kalitga ega bo‘lgan foydalanuvchilar uchun ochiq bo‘lishini ta’minlaydi. Ushbu maqolada hozirda eng zamonaviy shifrlash algoritmlarining turlari, eng kuchli va xavfsiz hisoblangan shifrlash algoritmlari, ularning ishlash mexanizmi, afzallik va kamchiliklari o‘rganiladi. Maqolaning maqsadi—zamonaviy shifrlash algoritmlari samaradorligini tahlil qilish va real xavfsizlikdagi o‘rnini ko‘rsatishdir, ularning kelajakdagi rivojlanish yo‘nalishlarini baholashdir..

Methods

Ushbu maqolada tahliliy yondashuv usuli qo‘llanildi. Ushbu tadqiqotda eng muhim shifrlash algoritmlari tahlil qilinadi: simmetrik (AES), assimetrik (RSA) va elliptik egri shifrlash (ECC). Algoritmlar tanlashda quyidagi mezonlarga asoslanildi:

- **Xavfsizlik darajasi** (kriptotahlilga chidamliligi)
- **Tezlik va samaradorlik** (amaliyotda ishlash tezligi)
- **Standartlashtirilganligi** (ISO, NIST yoki boshqa tashkilotlar tomonidan tasdiqlanganligi)
- **Algoritmlarni taqqoslash:** har bir algoritmning matematik asoslari, kalit uzunligi, hisoblash tezligi va xavfsizlik darajasi.
- Ommaboplik (real tizimlarda qo‘llanishi)

Ma’lumotlar uchun ochiq manbalar (NIST, IEEE maqolalari, rasmiy kriptografik hisobotlar) asos qilib olindi. Har bir algoritm bo‘yicha texnik tavsiflar, test natijalari va xavfsizlik tahlillari ko‘rib chiqildi.

Results

Quyidagi algoritmlar eng kuchli va keng qo‘llaniladigan algoritmlar qatoriga kiritildi:

✓ **1. AES (Advanced Encryption Standard)**

- **Turi**: Simmetrik blokli shifrlash.
- **Kalit uzunligi**: 128, 192, yoki 256 bit.
- **Afzallik**: Tez ishlaydi, rasmiy standart (FIPS 197), juda kuchli.
- **Kamchilik**: Kalit almashinuvi uchun alohida mexanizm kerak.

Tahlil natijalariga ko‘ra, AES simmetrik shifrlash algoritmlari orasida eng samarali va keng qo‘llaniladigan algoritm sifatida ajralib turadi. Uning 128, 192 va 256 bitli kalit uzunliklari zamonaviy xavfsizlik talablariga javob beradi.

AES (Advanced Encryption Standard) zamonaviy xavfsizlik tizimlarida keng qo‘llaniladigan simmetrik shifrlash algoritmi bo‘lib, quyidagi sohalarda muhim rol o‘ynaydi:

1. **Bank va moliyaviy tizimlar**:
   - Onlayn banking, kredit karta tranzaksiyalari va to‘lov tizimlarida (masalan, Visa, Mastercard) ma’lumotlarni shifrlash uchun ishlatiladi.
   - ATM’lar va POS terminallarida xavfsiz aloqa ta’minlaydi.
2. **Ma’lumotlar omborlari va bulutli xizmatlar**:
   - Google Cloud, AWS, Microsoft Azure kabi bulutli platformalarda ma’lumotlarni shifrlash uchun qo‘llaniladi.
   - Fayllarni saqlash va uzatishda (masalan, Dropbox, Google Drive) xavfsizlikni ta’minlaydi.
3. **Internet xavfsizligi**:
   - HTTPS protokollarida (SSL/TLS) veb-saytlar va foydalanuvchilar o‘rtasidagi aloqani shifrlash uchun ishlatiladi.
   - VPN (Virtual Private Network) va xavfsiz tunneling protokollarida ma’lumotlarni himoya qiladi.
4. **Mobil qurilmalar va IoT**:
   - Smartfonlar, planshetlar va IoT qurilmalarida (masalan, aqlli soatlar, uy xavfsizlik tizimlari) ma’lumotlarni shifrlash uchun ishlatiladi.
   - Android va iOS tizimlarida disk shifrlash (full-disk encryption) uchun qo‘llaniladi.
5. **Hukumat va harbiy tizimlar**:
   - Maxfiy ma’lumotlarni himoya qilish uchun davlat idoralari va harbiy tashkilotlarda keng qo‘llaniladi (NIST tomonidan tasdiqlangan).
   - Maxfiy hujjatlar va aloqa kanallarini shifrlashda ishlatiladi.
6. **Elektron pochta va xabarlar**:
   - Xavfsiz xabar almashish ilovalarida (masalan, Signal, WhatsApp) ma’lumotlarni shifrlash uchun foydalaniladi.
   - PGP (Pretty Good Privacy) va S/MIME kabi elektron pochta shifrlash protokollarida qo‘llaniladi.
7. **Ma’lumotlar bazasi xavfsizligi**:
   - SQL Server, Oracle va MySQL kabi ma’lumotlar bazalarida sezgir ma’lumotlarni (masalan, foydalanuvchi ma’lumotlari, moliyaviy hisobotlar) shifrlash uchun ishlatiladi.

✓ **2. RSA (Rivest-Shamir-Adleman)**

- **Turi**: Asimmetrik shifrlash.
- **Kalit uzunligi**: 2048–4096 bit.
- **Afzallik**: Elektron imzo, kalit almashinuvi uchun mos.
- **Kamchilik**: Sekin, katta hisoblash quvvatini talab qiladi.

RSA algoritmi assimetrik shifrlashda keng qo‘llaniladi, ammo katta kalit uzunliklari (2048 yoki 4096 bit) talab qiladi, bu esa hisoblash resurslarini ko‘p talab qiladi.

Quyida RSAning asosiy qo‘llanilish sohalari keltirilgan:

1. **Internet xavfsizligi**:
   - **SSL/TLS protokollari**: HTTPS veb-saytlarida (masalan, onlayn xaridlar, banking saytlari) xavfsiz aloqa uchun kalit almashinuvida ishlatiladi.
   - **VPN va xavfsiz tunnellar**: Ma’lumotlar uzatishda xavfsiz kalit almashishni ta’minlaydi.
2. **Raqamli imzo va autentifikatsiya**:
   - Hujjatlar va tranzaksiyalarni autentifikatsiya qilish uchun raqamli imzolar yaratishda qo‘llaniladi (masalan, elektron hujjatlar, dasturiy ta’minot imzolash).
   - Onlayn tizimlarda foydalanuvchi identifikatsiyasini tasdiqlashda ishlatiladi.
3. **Elektron pochta xavfsizligi**:
   - **PGP va S/MIME**: Xavfsiz elektron pochta xabarlarini shifrlash va imzolash uchun ishlatiladi (masalan, maxfiy xabar almashishda).
   - Xabarlarning yaxlitligini va avtorligini ta’minlaydi.
4. **Bank va moliyaviy tizimlar**:
   - Onlayn to‘lov tizimlarida (masalan, PayPal, Stripe) xavfsiz kalit almashinuvi va tranzaksiya tas-

diqlash uchun qo‘llaniladi.

- Raqamli sertifikatlar orqali autentifikatsiyani ta’minlaydi.

5. Hukumat va maxfiy aloqa:

- Maxfiy ma’lumotlarni uzatishda va davlat idoralarida xavfsiz aloqa kanallarini tashkil qilishda ishlatiladi.
- Raqamli sertifikatlar va xavfsiz autentifikatsiya tizimlarida qo‘llaniladi.

6. Dasturiy ta’minot va apparat xavfsizligi:

- Dasturiy ta’minotni autentifikatsiya qilish va litsenziyalarni himoya qilishda ishlatiladi.
- Aqlli kartalar va xavfsiz apparat modullari (HSM) da RSA kalitlari ishlatiladi.

7. Blokcheyn va kriptovalyutalar:

- Kriptovalyuta tranzaksiyalarini imzolash va tasdiqlashda (masalan, Bitcoin, Ethereum’da raqamli imzo sifatida).
- Xavfsiz hamyonlar va kalit boshqaruvida qo‘llaniladi.

RSAning asosiy afzalligi uning assimetrik tabiati bo‘lib, ochiq va yopiq kalitlar yordamida xavfsiz kalit almashinuvi va autentifikatsiyani ta’minlaydi. Ammo hisoblash murakkabligi tufayli u katta hajmdagi ma’lumotlarni shifrlashda kamroq ishlatiladi va ko‘pincha AES bilan birgalikda qo‘llaniladi.

RSA shifrlash algoritmini buzish tezligi.

RSA shifrlashini buzish uchun, eng katta masala, yirik sonlarni faktorlashdir. Ya’ni, katta butun sonni ikkita kichik sonlar ko‘paytmasiga ajratish juda qiyin bo‘ladi, ayniqsa, bu sonlar juda katta bo‘lsa.

Tezlikka ta’sir qiluvchi omillar:

1. Kalit uzunligi: RSA kalitlari qanchalik uzun bo‘lsa, ularni buzish shunchalik qiyin bo‘ladi. Misol uchun:

- 1024-bitlik kalitlar o‘rtacha 2000 yildan ortiq vaqt davomida buzilmasligi mumkin.
- 2048-bitlik kalitlar 2030-yillarda ham xavfsiz hisoblanadi.
- 4096-bitlik kalitlar esa yanada uzoq muddatli xavfsizlikni ta’minlaydi.

2. Kompüterning kuchi: Zamonaviy kompyuterlar yirik sonlarni faktorlashda juda kuchli bo‘lishi mumkin, ammo bugungi kunda mavjud bo‘lgan texnologiyalar bu ishni 1024 bitlik kalitlar uchun ma’lum bir vaqt ichida amalga oshirishi mumkin. Lekin 2048 bit yoki undan katta kalitlar bilan shifrlangan ma’lumotlarni buzish uchun ko‘proq vaqt talab etiladi.

3. Quantum kompyuterlar: Kvant kompyuterlar RSA algoritmini o‘zgartirishi mumkin, chunki ular Shor algoritmi yordamida faktorlashni ancha tezroq amalga oshirishi mumkin. Kvant kompyuterlari keng tarqalgan bo‘lishi bilan RSA algoritmi xavfsizligini tez orada buzishi mumkin.

RSA Shifrlashni buzish vaqti grafigi.

RSA algoritmining buzilish tezligi, kalit uzunligiga bog‘liq ravishda keskin farq qiladi. Quyidagi grafikda RSA kalit uzunligi va tahmin qilingan buzilish vaqti ko‘rsatilgan:

- 1024-bit kalitlar: 1 yildan ko‘proq
- 2048-bit kalitlar: 20-30 yil

4096-bit kalitlar: 100 yildan ko‘proq

✓ **3. Elliptic Curve Cryptography (ECC)**

- **Turi**: Asimmetrik shifrlash.
- **Afzallik**: Kichik kalit bilan yuqori xavfsizlik (160 bit ≈ 1024 bit RSA).
- **Kamchilik**: Yangi texnologiya, ayrim tizimlar uchun moslashmagan.

Elliptic Curve Cryptography (ECC) esa qisqa kalit uzunliklari (256 bit) bilan yuqori xavfsizlikni ta’minlaydi, bu uni mobil qurilmalar va IoT tizimlari uchun ideal qiladi.

Quyida ECCning asosiy qo‘llanilish sohalari keltirilgan:

1. Internet xavfsizligi:

- **SSL/TLS protokollari**: HTTPS veb-saytlarida (masalan, onlayn do‘konlar, ijtimoiy tarmoqlar) xavfsiz aloqa uchun kalit almashinuvi va raqamli sertifikatlarda ishlatiladi. ECC, RSAga nisbatan kamroq resurs talab qilganligi uchun afzal ko‘riladi.
- **VPN va xavfsiz tunnellar**: Ma’lumotlar uzatishda xavfsiz kalit almashinuvini ta’minlaydi.

2. Mobil qurilmalar va IoT (Internet of Things):

- Smartfonlar, planshetlar va IoT qurilmalarida (masalan, aqlli uy tizimlari, tibbiy sensorlar) xavfsiz aloqa va ma’lumot shifrlash uchun ishlatiladi.
- ECCning qisqa kalit uzunliklari (masalan, 256 bit) resurslari cheklangan qurilmalarda samarali ishlaydi.
- Android va iOS tizimlarida xavfsiz autentifikatsiya va ma’lumot shifrlashda qo‘llaniladi.

3. Raqamli imzo va autentifikatsiya:

- **ECDSA (Elliptic Curve Digital Signature Algorithm)**: Hujjatlar, dasturiy ta’minot va tranzaksiyalarni autentifikatsiya qilish uchun raqamli imzolar yaratishda ishlatiladi.
- Xavfsiz identifikatsiya tizimlarida (masalan, elektron pasportlar, raqamli sertifikatlar) qo‘llaniladi.

4. Blokcheyn va kriptovalyutalar:

- Bitcoin, Ethereum va boshqa kriptovalyutalarda tranzaksiyalarni imzolash va xavfsiz hamyonlarni boshqarishda ishlatiladi (masalan, ECDSA algoritmi orqali).
- Xavfsiz va samarali kalit juftliklarini yaratish uchun qo‘llaniladi.

5. Bank va moliyaviy tizimlar:

- Onlayn to‘lov tizimlari va banking xizmatlarida xavfsiz kalit almashinuvi va tranzaksiya tasdiqlash uchun ishlatiladi.
- Aqlli kartalar (masalan, kredit kartalari) va xavfsiz to‘lov tizimlarida qo‘llaniladi.

6. Hukumat va harbiy tizimlar:

- Maxfiy ma’lumotlarni shifrlash va xavfsiz

aloqa kanallarini tashkil qilishda ishlatiladi.

- NIST va boshqa xavfsizlik standartlari tomonidan tasdiqlangan ECC algoritmlari maxfiy tizimlarda keng qo‘llaniladi.

7. Elektron pochta va xabarlar:

- Xavfsiz xabar almashish ilovalarida (masalan, Signal, WhatsApp) kalit almashinuvi va autentifikatsiya uchun ishlatiladi.
- PGP va S/MIME kabi protokollarda raqamli imzo va shifrlash uchun qo‘llaniladi.

8. Xavfsiz apparat modullari (HSM):

- Xavfsiz kalitlarni saqlash va boshqarish uchun apparat modullarida (masalan, serverlar va xavfsizlik devorlari) ECC ishlatiladi.

✓ **4. ChaCha20 (stream cipher)**

- **Afzallik**: Mobil qurilmalarda samarali ishlaydi.
- **Kamchilik**: Kamroq standartlashtirilgan.

ChaCha20ning o‘ziga xos xususiyatlari :

❖ **AESga nisbatan afzalliklari**:

- AES apparat optimallashtiruviga (masalan, AES-NI) bog‘liq bo‘lsa, ChaCha20 dasturiy ta’minotda ham yuqori samaradorlikni ta’minlaydi.
- Mobil va IoT qurilmalarida kamroq quvvat sarflaydi.

❖ **Poly1305 bilan kombinatsiya**: ChaCha20 ko‘pincha Poly1305 autentifikatsiya algoritmi bilan birgalikda ishlatiladi (AEAD – Authenticated Encryption with Associated Data), bu ma’lumot yaxlitligi va autentiklikni ta’minlaydi.

❖ **Kvant hujumlariga chidamlilik**: ChaCha20 kvant kompyuterlariga qarshi AESga nisbatan bir oz ko‘proq chidamlilikni ta’minlaydi, chunki uning dizayni Grover algoritmi ta’sirini kamaytiradi.

Shifrlash algoritmi Daniel J. Bernstein tomonidan ishlab chiqilgan va Salsa shifrlash algoritmining rivojlangan versiyasi sifatida 2008-yilda taqdim etilgan. ChaCha20, ayniqsa, AESga muqobil sifatida resurslari cheklangan muhitlarda va tezkor shifrlash talab qilinadigan sohalarda keng qo‘llaniladi. Quyida ChaCha20 haqida asosiy ma’lumotlar va uning qo‘llanilish sohalari keltirilgan:

1. Internet xavfsizligi:

- **TLS/SSL**: ChaCha20 TLS 1.3 protokolida AESga muqobil sifatida ishlatiladi, ayniqsa mobil qurilmalar va past quvvatli tizimlarda (Google Chrome, Firefox, Android tizimlarida qo‘llaniladi).
- **VPN va xavfsiz tunnellar**: OpenVPN va WireGuard kabi xavfsiz aloqa protokollarida ChaCha20 tezkor va xavfsiz shifrlash uchun qo‘llaniladi.

2. Mobil qurilmalar va IoT:

- Smartfonlar, planshetlar va IoT qurilmalarida (masalan, aqlli soatlar, sensorlar) ChaCha20ning kam resurs talab qilishi tufayli ishlatiladi.
- Android va iOS tizimlarida xavfsiz aloqa va ma’lumot shifrlash uchun qo‘llaniladi.

3. Xabarlar va elektron pochta:

- Xavfsiz xabar almashish ilovalarida (masalan, Signal, WhatsApp) ChaCha20 xavfsiz kalit almashinuvi va ma’lumot shifrlashda ishlatiladi.
- ChaCha20-Poly1305 kombinatsiyasi (autentifikatsiya bilan shifrlash) xabar yaxlitligini ta’minlaydi.

4. Bulutli xizmatlar va ma’lumotlar omborlari:

- Bulutli xizmatlarda (masalan, Google Cloud, AWS) ma’lumotlarni shifrlash uchun ishlatiladi, ayniqsa AES apparat optimallashtiruvi mavjud bo‘lmagan muhitlarda.
- Fayllarni xavfsiz saqlash va uzatishda qo‘llaniladi.

5. Blokcheyn va kriptovalyutalar:

- Kriptovalyuta tizimlarida (masalan, Monero, Zcash) tranzaksiyalar va hamyon ma’lumotlarini shifrlashda ishlatiladi.
- ChaCha20ning tezkor ishlashi uni blokcheyn ilovalarida samarali qiladi.

6. **Hukumat va maxfiy aloqa**:

- Maxfiy ma’lumotlarni shifrlash va xavfsiz aloqa kanallarini tashkil qilishda qo‘llaniladi, ayniqsa resurslari cheklangan qurilmalarda.

Kvant hisoblashning rivojlanishi RSA va ECC algoritmlariga tahdid solishi mumkin, ammo AES kvant hujumlariga nisbatan barqarorroq.

Tahlil va Munozara

Yuqoridagi algoritmlar turli sohalarda o‘z o‘rniga ega. AES, RSA va ECC algoritmlari zamonaviy xavfsizlik tizimlarining asosini tashkil qiladi.

AES tezkor va samarali bo‘lib, hozirda simmetrik shifrlashda sanoat standarti hisoblanadi va davlat darajasidagi axborot almashinuvida, ma’lumotlar omborlari va bulutli xizmatlarda keng qo‘llaniladi.

RSA esa kalitlar almashinuvi va elektron raqamli imzolar uchun ajralmas vositadir. Shunga qaramay, RSAning hisoblash murakkabligi tufayli sekin ishlashi ECC algoritmining ko‘proq ishlatilishiga olib kelmoqda, ayniqsa resurslar cheklangan mobil qurilmalarda.

Yangi avlod algoritmlaridan biri bo‘lgan **ChaCha20** esa Google va boshqa kompaniyalar tomonidan TLS (HTTPS) xavfsizlik protokollarida ishlatilmoqda, ayniqsa tezlik va soddaligi bilan ajralib turadi.

Kelajakda kvant kompyuterlarning rivojlanishi mavjud algoritmlarni zaiflashtirishi mumkin. Shu sababli hozirda **Post-Quantum Cryptography** (Kvantga chidamli shifrlash) bo‘yicha izlanishlar kuchaymoqda.

Xulosa

Shifrlash algoritmlari zamonaviy raqamli xavfsizlikning yuragi hisoblanadi. AES, RSA, ECC kabi algoritmlar har kuni milliardlab ma’lumotlarni tahdidlardan asramoqda. Biroq texnologiya rivojlanib borar ekan, yangi xavflar paydo bo‘lmoqda. Shuning uchun kriptografik algoritmlar muntazam yangilanib borilishi va xavfsizlik bo‘yicha izlanishlar davom ettirilishi zarur. Har bir tashkilot va foydalanuvchi axborot xavfsizligini ta’minlashda zamonaviy va kuchli algoritmlardan foydalanishni o‘zining ustuvor vazifasi deb bilishi kerak.

Adabiyotlar ro‘yxati

1. National Institute of Standards and Technology (NIST). (2001). FIPS PUB 197. Advanced Encryption Standard (AES).
2. Rivest, R., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems.
3. Bernstein, D. J. (2008). ChaCha, a variant of Salsa20.
4. Smart, N. P. (2003). Cryptography: An Introduction.
5. Bos, J., Costello, C., Naehrig, M., & Stebila, D. (2015). Post-quantum key exchange for TLS.