KIBERXAVFSIZLIKNI TA'MINLASHDA ZAMONAVIY KRIPTOGRAFIK ALGORITMLARNING SAMARADORLIGINI TAHLIL QILISH

O'razboyeva Farangiz
Toshkent davlat iqtisodiyot universiteti To'rtko'l fakulteti 2-kurs talabasi

KIRISH: *Kriptografiya – raqamli axborotni himoyalashning eng muhim vositasi bo'lib, u ma'lumotlarning maxfiyligi, yaxlitligi va autentifikatsiyasini ta'minlaydi. Kiberxavfsizlik tizimlarida shifrlash, raqamli imzo va kalit almashish mexanizmlari aynan kriptografik algoritmlarga asoslanadi. Zamonaviy tarmoqlarda AES, RSA, ECC kabi algoritmlar standartga aylangan, ammo kvant kompyuterlar paydo bo'lishi bilan ularning barqarorligi qayta baholanishi zarur.*

Kalit so'zlar: *kiberxavfsizlik, kriptografiya, AES, RSA, ECC, post-kvant kriptografiya, CRYSTALS-Kyber, raqamli imzo, ma'lumotlarni shifrlash, axborot xavfsizligi, kvant kompyuterlar, algoritm samaradorligi, tarmoq xavfsizligi, kalit almashish, kriptotizimlar.*

AES — simmetrik blok shifri bo'lib, 128-bit blok va 128/192/256-bit kalit uzunliklarida ishlaydi. U yuqori tezlik, past resurs talabi va ishonchliligi bilan ajralib turadi. Zamonaviy protsessorlar AES-NI kabi apparat qo'llab-quvvatlashni ta'minlagani sababli bu algoritm TLS, Wi-Fi (WPA2/3), VPN va ma'lumotlar bazalarida keng qo'llaniladi. AES-128 amaliy jihatdan yorilmagan, biroq Grover algoritmi sababli kvant sharoitida 256-bitli versiyadan foydalanish tavsiya etiladi. RSA — ochiq kalitli kriptotizim bo'lib, katta butun sonlarni faktorizatsiya qilishning murakkabligiga asoslanadi. U TLS, elektron imzolar va sertifikatlash tizimlarida ishlatiladi. 3072-bitli RSA kaliti 128-bit xavfsizlik darajasini beradi. Afzalligi — sinovdan o'tgan ishonchli tizim, kamchiligi esa katta kalitlar va hisoblash yukidir. Shuningdek, Shor algoritmi yordamida RSA kvant kompyuterlar tomonidan yorilishi mumkin. Shu sababli RSA kelgusida post-kvant algoritmlarga o'rin bo'shatadi.ECC elliptik egri chiziqlardagi diskret logarifm muammosiga asoslangan. 256-bitli ECC kaliti RSA-3072 darajasidagi xavfsizlikni beradi, lekin resurs sarfi 10 barobar kamroq. Bu ECCni mobil qurilmalar va IoT tizimlarida eng samarali algoritmga aylantiradi. U ECDSA, ECDH, TLS va kriptovalyutalarda keng qo'llaniladi. Kvant tahdidiga nisbatan esa ECC ham zaif hisoblanadi, ammo klassik tizimlarda yuqori samaradorlikni ta'minlaydi. Kvant kompyuterlar RSA va ECCni yengib o'tishi mumkinligi sababli, yangi algoritmlar ishlab chiqilmoqda. NIST tomonidan tavsiya etilgan CRYSTALS-Kyber (kalit enkapsulyatsiya), CRYSTALS-Dilithium (raqamli imzo) va SPHINCS+ (hash-asosli imzo) 2024-yilda PQC standartlari sifatida qabul qilindi.
Kyber lattice matematikasiga asoslanib, tezkor ishlash va kichik kalit hajmiga ega. U tarmoq protokollarida RSA yoki ECC o'rnini bosishga mo'ljallangan. NTRU esa boshqa lattice asosli algoritm bo'lib, tez ishlashi va kichik resurs talabi bilan

ajraladi. Hozirda u ham NIST tomonidan tavsiya etilgan alternativalar sirasiga kiradi. Kvant kompyuterlar paydo bo‘lishi bilan hozirgi algoritmlar xavfsizligi pasayadi. Masalan, Shor algoritmi RSA va ECCni to‘liq yoradi, Grover esa AES xavfsizligini yarmiga kamaytiradi. Shu sababli 2030-yilgacha RSA-2048 va ECC-224 kabi kalitlar eskirgan deb e’tirof etiladi. “Hozir yig‘ib, keyin ochish” (harvest now, decrypt later) strategiyasi bilan hujumchilar bugun shifrlangan ma’lumotni saqlab, kelajakda kvant yordamida ochishi mumkin. Bu esa post-kvant yechimlariga o‘tishni tezlashtiradi.

Amaliy tanlov mezonlari

Tarmoq xavfsizligi: AES-GCM ma’lumot shifrlash uchun, ECC yoki Kyber esa kalit almashish uchun.

Mobil qurilmalar: energiya va xotira cheklovi sabab ECC yoki ChaCha20 afzal.

IoT tizimlari: NIST tomonidan 2025-yilda qabul qilingan Ascon oilasidagi yengil kriptografiya algoritmlari ishlatiladi.

Moliya va hukumat tizimlari: uzoq muddatli xavfsizlik uchun AES-256, ECDSA va PQC algoritmlari kombinatsiyasi tavsiya etiladi.

Xulosa Zamonaviy kriptografik algoritmlar kiberxavfsizlikni ta’minlashda hal qiluvchi rol o‘ynaydi. AES, RSA va ECC hozirgi tizimlar uchun samarali bo‘lsa-da, kvant kompyuterlar ularni zaiflashtiradi. Shu sababli dunyo miqyosida post-kvant kriptografiyaga o‘tish jarayoni boshlandi. NIST tomonidan tavsiya etilgan Kyber, Dilithium va SPHINCS+ algoritmlari kelajakning asosiy himoya vositalariga aylanadi. Kriptografik tizimlarni yangilash, standartlarga moslash va kvantga tayyorgarlik — yaqin o‘n yillikda kiberxavfsizlikning eng muhim yo‘nalishlaridan biri bo‘lib qoladi.

Foydalanilgan adabiyotlar

1. Stallings, W. Cryptography and Network Security: Principles and Practice. — 8th ed. — Pearson, 2023.

2. Menezes, A., van Oorschot, P., Vanstone, S. Handbook of Applied Cryptography. — CRC Press, 2021.

3. National Institute of Standards and Technology (NIST). Post-Quantum Cryptography Standards – CRYSTALS-Kyber and Dilithium. — NIST, 2024.

4. Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. — Wiley, 2022.

5. Bernstein, D. J., Lange, T. Post-Quantum Cryptography. — Springer, 2017.

6. Berson, T. The Case for AES-256. — IEEE Security & Privacy Journal, Vol. 19, No. 4, 2021.

7. Kurbatov, A. A. Zamonaviy kriptografik algoritmlar va ularning kiberxavfsizlikdagi o‘rni. — “Axborot texnologiyalari” jurnali, №3, 2022.

8. ISO/IEC 18033-3: Information Technology — Security Techniques — Encryption Algorithms. — International Organization for Standardization, 2019.

9. Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P. Post-Quantum Key Encapsulation from Module-LWE (CRYSTALS-Kyber). — IEEE European Symposium on Security and Privacy, 2020.

10. O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi. Kiberxavfsizlik konsepsiyasi. — Toshkent, 2023.