KRIPTOGRAFIK ALGORITMLAR: AES, RSA VA ECC TAQQOSLASH

Suyunov Kamoliddin Nurali o‘g‘li
Rahmatov Komiljon Inomjon o‘g‘li
Boboqulov Nozimbek Baxtiyor o’g’li
Imamaliyev Aybek Turapbayevich
Muhammad Al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti
Kiber xavfsizlik fakulteti axborot xavfsizligi kafedrasi o‘qituvchisi

Annotatsiya: Ushbu maqolada zamonaviy axborot xavfsizligining asosiy elementlari hisoblangan AES (Advanced Encryption Standard), RSA (Rivest–Shamir–Adleman) va ECC (Elliptic Curve Cryptography) algoritmlarining asosiy tamoyillari va ularning samaradorlik, xavfsizlik darajasi hamda resurslardan foydalanish nuqtayi nazaridan taqqoslanadi. Tadqiqotda algoritmlarning matematik asoslari, ishlash tezligi, kalit uzunligi va xavfsizlikka ta’siri amaliy misollar asosida tahlil qilinadi. Maqola kriptografiya sohasida optimal tanlovni amalga oshirishda ilmiy va amaliy jihatdan yordam beradi.

Kalit so‘zlar: AES, RSA, ECC, kriptografiya, simmetrik shifrlash, assimetrik shifrlash, xavfsizlik, samaradorlik, kalit uzunligi.

Axborot texnologiyalari rivojlanib borayotgan sari ma’lumotlarni himoya qilish dolzarb masalaga aylanmoqda. Kriptografiya bu maqsadga erishishda asosiy vosita bo‘lib xizmat qiladi. Har xil turdagi kriptografik algoritmlar mavjud bo‘lib, ulardan eng keng tarqalgani — AES, RSA va ECC hisoblanadi. Ularning har biri o‘ziga xos matematik asos, ishlash prinsipi va afzalliklarga ega. Ushbu maqolada mazkur algoritmlar o‘zaro taqqoslab tahlil qilinadi.

Kriptografiya axborot texnologiyalarining eng muhim sohalaridan biri bo‘lib, u ma’lumotlarni maxfiy saqlash, uzatish va autentifikatsiya qilish imkonini beradi. Har kuni internet orqali yuborilayotgan milliardlab xabarlar va tranzaksiyalar ishonchli va himoyalangan bo‘lishi kerak. Shunday maqsadlarda AES, RSA va ECC kabi algoritmlar keng qo‘llaniladi. Ularning har biri o‘ziga xos matematik asosga ega bo‘lib, ma’lumotlar xavfsizligini turlicha ta’minlaydi. Ushbu maqolada ushbu uch asosiy algoritm texnik va amaliy jihatdan taqqoslanadi.

Kriptografik algoritmlar — AES, RSA va ECC — zamonaviy xavfsizlik tizimlarining asosini tashkil etadi. Ular turli maqsadlarda ishlatiladi va har biri o‘ziga xos xususiyatlarga ega. Quyida ularni har tomonlama taqqoslab, batafsil tahlil qilamiz: algoritmlarning turi, xavfsizlik darajasi, tezlik, resurs talabi, qo‘llanilishi, afzallik va kamchiliklari, shuningdek, kelajakdagi kvant kompyuterlarga chidamliligi kabi

jihatlarni ko‘rib chiqamiz.

Algoritmlarning turi va asosiy maqsadi

- AES (Advanced Encryption Standard):

- Turi: Simmetrik kalitli algoritm.

- Maqsadi: Ma'lumotlarni shifrlash va maxfiyligini ta'minlash. Masalan, fayllar, tarmoq aloqalari yoki butun disklar shifrlanadi.

- Ishlash prinsipi: Bitta maxfiy kalit yordamida ma'lumotni shifrlaydi va ochadi. Shifrlash va ochish jarayonlari bir xil kalitdan foydalanadi, shuning uchun kalitni xavfsiz saqlash va almashish juda muhim.

- Struktura: Blokli shifr bo‘lib, 128-bitli bloklarda ishlaydi. Kalit uzunligi 128, 192 yoki 256 bit bo‘lishi mumkin.

- Misollar: Disk shifrlash (BitLocker), tarmoq shifrlash (SSL/TLS), VPN.

- RSA (Rivest-Shamir-Adleman):

- Turi: Asimmetrik kalitli algoritm.

- Maqsadi: Kalit almashinuvi, raqamli imzo yaratish va kichik hajmdagi ma'lumotlarni xavfsiz uzatish.

- Ishlash prinsipi: Ikkita kalit — ochiq (public) va maxfiy (private) — ishlatiladi. Ochiq kalit bilan shifrlangan ma'lumotni faqat maxfiy kalit ochadi. Bu kalit almashinuvi va autentifikatsiya uchun ideal.

- Struktura: Katta raqamlarni faktorizatsiya qilish muammosiga asoslanadi. Matematik jihatdan ikkita katta tub sonning ko‘paytmasini tahlil qilish qiyinligiga tayanadi.

- Misollar: SSL/TLS sertifikatlari, raqamli imzolar, kalit almashinuvi.

- ECC (Elliptic Curve Cryptography):

- Turi: Asimmetrik kalitli algoritm.

- Maqsadi: RSAga o‘xshash maqsadlarga xizmat qiladi (kalit almashinuvi, raqamli imzo), lekin kichikroq kalit uzunliklari bilan yuqori xavfsizlikni ta'minlaydi.

- Ishlash prinsipi: Elliptik egri matematikasiga asoslanadi. Diskret logarifm muammosining elliptik egri versiyasiga tayanadi, bu esa kichik kalitlar bilan samarali xavfsizlikni ta'minlaydi.

- Struktura: Elliptik egri nuqtalarining guruh operatsiyalariga asoslanadi. Kalit uzunligi odatda 160-521 bit orasida bo‘ladi.

- Misollar: Mobil qurilmalarda shifrlash (WhatsApp), raqamli imzolar (ECDSA), blokcheyn tizimlari (Bitcoin, Ethereum).

Xavfsizlik darajasi

- AES:

- Kalit uzunligi: 128, 192 yoki 256 bit.

- Xavfsizlik: Hozirgi kunda eng xavfsiz simmetrik algoritmlardan biri. To‘g‘ri qo‘llanilganda (kalit uzunligi yetarli bo‘lsa), hech qanday jiddiy zaiflik aniqlanmagan.

- Hujumlar: Brute-force hujumlari (kalitni taxmin qilish) faqat kalit uzunligi qisqa bo‘lganda (masalan, 128-bitdan kam) amaliy bo‘lishi mumkin. 256-bitli AES uchun hozirgi kompyuterlar bilan brute-force deyarli imkonsiz.

- Zaifliklar: Algoritmning o‘zi xavfsiz bo‘lsa-da, noto‘g‘ri amalga oshirilishi (masalan, kalitni xavfsiz saqlamaslik yoki tasodifiy sonlar generatori zaif bo‘lishi) muammolarga olib keladi.

- Kvant kompyuterlar: Grover algoritmi kalit qidirish vaqtini kvadrat ildizigacha qisqartiradi, ya'ni 256-bitli AES 128-bitli xavfsizlikka tenglashtiriladi. Shu sababli, 256-bitli AES hali ham xavfsiz deb hisoblanadi.

- RSA:

- Kalit uzunligi: Odatda 2048 yoki 4096 bit, ba’zan 1024 bit (lekin hozir 1024 bit xavfsiz emas deb hisoblanadi).

- Xavfsizlik: Katta raqamlarni faktorizatsiya qilishning qiyinligiga asoslanadi. Hozirgi klassik kompyuterlar bilan 2048-bitli RSAni buzish amaliy emas.

- Hujumlar: Faktorizatsiya algoritmlari (masalan, Shor algoritmi kvant kompyuterlarda) yoki kalit uzunligi qisqa bo‘lsa (1024 bit yoki undan kam) zaifliklar aniqlangan.

- Zaifliklar: Kalit uzunligi qanchalik katta bo‘lsa, xavfsizlik shunchalik yuqori, lekin hisoblash resurslari ham ko‘p talab qilinadi. Kalitlarni noto‘g‘ri boshqarish yoki tasodifiy sonlar generatori zaifligi xavfsizlikni pasaytiradi.

- Kvant kompyuterlar: Shor algoritmi yordamida kvant kompyuterlar RSAni osonlikcha buzishi mumkin, chunki bu algoritm faktorizatsiyani polinomial vaqtda amalga oshiradi.

Xulosa

AES, RSA va ECC algoritmlari turli ehtiyojlar uchun mos keladi:

- AES – katta hajmdagi ma’lumotlarni tez va xavfsiz shifrlash uchun ideal.
- RSA – ochiq kalit infratuzilmasi (PKI) talab etiladigan holatlar uchun.
- ECC – kam resursli tizimlarda maksimal xavfsizlikni ta’minlash uchun qulay.

Mobil qurilmalarda ECC asosidagi algoritmlarni joriy etish tavsiya etiladi.

Ma’lumotlar bazasini shifrlashda AESdan foydalanish maqsadga muvofiq.

Kalitlar almashinuvi va imzo yaratishda RSA o‘rniga ECCga o‘tish dolzarb.

Adabiyotlar:

1. Volume 3 | Issue 4 | 2022 Cite-Factor: 0,89 | SIS: 1,12 SJIF: 5,7 | UIF: 6,1 Kuralov, Y. A., Makhmudova, D. M., (2020). METHODOLOGY OF DEVELOPING CREATIVE COMPETENCE IN STUDENTS WITH PROBLEMATIC EDUCATION. European Journal of Research and Reflection in Educational Sciences Vol. 8 No. 4, 2020, Part IIISSN 2056-5852, 142-146.

2. Akhmedov, B. A., Majidov, J. M., Narimbetova, Z. A., Kuralov, Yu. A. (2020).

Active interactive and distance forms of the cluster method of learning in development of higher education. Экономика и социум, 12(79), 805-808.
3. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 2001. – 376 с.
4. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М., 2002 – 816 с.
5. Жўраева, Н. В., Султанов, Р. О., Абдуллаева, С. А., Рахимжонова, В. А. (2020). Systematization of word combinations in the uzbek language. Наука и Мир, 2(6), 6568.
6. Sultanov R. O., Yusupov M. R. (2020). Ta'limda matematika fanini o'qitishdagi muammolar va ularning yechimida axborot kommunikatsiya texnologiyalarining ahamiyati. O`zMU xabarlari, 2(1/2/1), 144-147.
7. Султанов, Р. О. (2020). Idea блокли шифрлаш алгоритмини такомиллаштириш методлари. Academic Research in Educational Sciences, 1(3), 397-404.