SIMMETRIK VA ASIMMETRIK SHIFRLASH TIZIMLARI

Ibodullayeva Shahzodabonu
Maxsus fanlar o‘qituvchisi

Annotatsiya: Ushbu maqolada zamonaviy axborot xavfsizligining asosi bo‘lgan simmetrik va asimmetrik shifrlash tizimlarining ishlash prinsiplari, afzalliklari va kamchiliklari qiyosiy tahlil qilinadi. Tadqiqot davomida ma’lumotlarni uzatishda maxfiylikni ta’minlashning matematik asoslari, kalitlarni boshqarish muammolari va har bir tizimning qo‘llanilish sohalari ko‘rib chiqiladi. Shuningdek, maqolada gibrid shifrlash usullari va kiberxavfsizlikda ushbu kriptografik algoritmlarning o‘rni haqida xulosalar keltirilgan.
Kalit so‘zlar: Kriptografiya, shifrlash, simmetrik algoritm, asimmetrik algoritm, ochiq kalit, maxfiy kalit, AES, RSA, axborot xavfsizligi, ma’lumotlarni himoyalash.

Bugungi axborotlashgan jamiyatda ma’lumotlarning xavfsizligi va maxfiyligini ta’minlash eng dolzarb masalalardan biri bo‘lib qolmoqda. Global tarmoqlar orqali uzatilayotgan trillionlab ma’lumotlar paketi kiberhujumlar va ruxsatsiz kirishlardan himoyalangan bo‘lishi shart. Bu jarayonda kriptografiya — ma’lumotlarni shifrlash va ularni begona shaxslar uchun tushunarsiz holatga keltirish fani markaziy o‘rinni egallaydi.

Kriptografik tizimlar asosan ikki yirik guruhga bo‘linadi: simmetrik va asimmetrik shifrlash.

- Simmetrik shifrlashda ma’lumotni shifrlash va deshifrlash (asliga qaytarish) uchun bitta umumiy maxfiy kalitdan foydalaniladi. Bu usul tezkorligi bilan ajralib tursa-da, kalitni xavfsiz kanal orqali uzatish muammosini tug‘diradi.
- Asimmetrik shifrlashda esa bir-biri bilan matematik bog‘langan ikkita — ochiq (public) va yopiq (private) kalitlar tizimi qo‘llaniladi. Bu tizim xavfsizlik darajasini oshiradi, biroq hisoblash quvvati va vaqt nuqtai nazaridan simmetrik usullardan ancha sekinroq ishlaydi.

Ushbu maqolaning maqsadi simmetrik va asimmetrik algoritmlarning texnik xususiyatlarini o‘rganish, ularning matematik modellarini solishtirish va zamonaviy bank tizimlari, davlat boshqaruvi hamda shaxsiy ma’lumotlarni himoyalashda qaysi usuldan foydalanish samaraliroq ekanligini aniqlashdan iborat. Shuningdek, maqolada har ikki

tizimning kuchli jihatlarini birlashtirgan gibrid tizimlar tahliliga ham alohida e’tibor qaratiladi.

Simmetrik va asimmetrik shifrlash tizimlari zamonaviy kiberxavfsizlikning ikki ustuni bo‘lib, ularning har biri ma’lumotlarni himoya qilishda o‘ziga xos mexanizmlar va matematik algoritmlarga tayanadi. Axborot texnologiyalari jadal rivojlanayotgan davrda ma’lumotlarning maxfiyligi, butunligi va haqiqiyligini ta’minlash nafaqat davlat ahamiyatiga molik tizimlar, balki oddiy foydalanuvchilarning kundalik muloqoti uchun ham hayotiy zaruriyatga aylandi. Kriptografiyaning asosiy vazifasi ochiq matnni begona shaxslar tushuna olmaydigan shifrlangan holatga keltirish va faqat vakolatli shaxsga uni qayta o‘qish imkonini berishdir. Bu jarayonda simmetrik shifrlash eng qadimgi va klassik usul hisoblanadi. Uning ishlash prinsipi juda sodda: ma’lumotni shifrlash uchun ham, uni asliga qaytarish uchun ham bir xil kalitdan foydalaniladi. Bu usulning asosiy ustunligi uning yuqori tezligidir. Simmetrik algoritmlar katta hajmdagi ma’lumotlarni, masalan, ma’lumotlar bazalarini yoki video oqimlarni real vaqt rejimida shifrlash uchun juda mos keladi. AES (Advanced Encryption Standard) kabi zamonaviy simmetrik algoritmlar butun dunyoda eng ishonchli standartlar sifatida tan olingan. Biroq, simmetrik tizimning eng katta zaif tomoni kalitlarni tarqatish muammosidir. Agar ikki tomon xavfsiz muloqot qilmoqchi bo‘lsa, ular avval umumiy maxfiy kalitni bir-birlariga xavfsiz yetkazib berishlari kerak. Agar kalit uzatish jarayonida begona qo‘lga tushsa, butun shifrlangan tizim o‘z qiymatini yo‘qotadi.

Asimmetrik shifrlash tizimi, shuningdek, ochiq kalitli kriptografiya deb ham ataladi, bu muammoni hal qilish uchun 1970-yillarda yaratilgan inqilobiy yondashuvdir. Bu tizimda bitta emas, balki matematik jihatdan o‘zaro bog‘langan ikkita kalit — ochiq (public) va yopiq (private) kalitlar juftligi qo‘llaniladi. Ochiq kalit hamma uchun ochiq bo‘lib, undan ma’lumotni shifrlashda foydalaniladi. Yopiq kalit esa faqat egasida saqlanadi va u shifrlangan ma’lumotni ochish (deshifrlash) uchun xizmat qiladi. Bu usulning go‘zalligi shundaki, ochiq kalit orqali shifrlangan ma’lumotni hatto o‘sha ochiq kalit bilan ham qayta ochib bo‘lmaydi — uni faqat unga mos keladigan yopiq kalit egasi o‘qiy oladi. RSA, El-Gamal va Elliptik egri chiziqli kriptografiya (ECC) kabi algoritmlar asimmetrik tizimning yorqin namunalaridir. Asimmetrik tizim kalitlarni xavfsiz tarqatish muammosini yo‘q qiladi, chunki maxfiy kalit hech qachon tarmoq orqali uzatilmaydi. Shuningdek, u elektron raqamli imzo texnologiyasini yaratishga imkon berdi, bu esa ma’lumotning aynan

kimdan kelganini va yo‘lda o‘zgartirilmaganini tasdiqlash imkonini beradi. Biroq, asimmetrik algoritmlarning matematik hisob-kitoblari juda murakkab bo‘lgani uchun ular simmetrik usullarga qaraganda yuzlab, hatto minglab marta sekinroq ishlaydi.

Bugungi kunda amaliyotda ushbu ikki tizimning kuchli tomonlarini birlashtirgan gibrid shifrlash tizimlari keng qo‘llaniladi. Masalan, biz kundalik hayotda foydalanadigan HTTPS protokoli (veb-saytlar xavfsizligi) aynan shu prinsiplarga asoslangan. Muloqotning boshida asimmetrik shifrlashdan foydalanib, tomonlar o‘zaro bir marta ishlatiladigan simmetrik seans kalitini almashib oladilar. Keyinchalik esa butun ma’lumotlar oqimi tezkor simmetrik algoritm orqali shifrlanadi. Bu yondashuv ham yuqori xavfsizlikni, ham yuqori tezlikni ta’minlash imkonini beradi. Shifrlash tizimlarining samaradorligi kalit uzunligi bilan ham belgilanadi. Simmetrik tizimda 256 bitli kalit juda kuchli hisoblansa, asimmetrik RSA tizimida shunday xavfsizlik darajasiga erishish uchun kalit uzunligi 3072 bit yoki undan ko‘proq bo‘lishi talab etiladi. Bu farq algoritmlarning matematik tabiatidan kelib chiqadi. Simmetrik tizimda kalitni topish uchun "brute-force" (barcha variantlarni sinab ko‘rish) hujumi talab etilsa, asimmetrik tizimda katta sonlarni ko‘paytuvchilarga ajratish kabi murakkab matematik muammolarga tayaniladi.

Kiberxavfsizlik sohasidagi mutaxassislar uchun simmetrik va asimmetrik shifrlashni to‘g‘ri tanlash tizimning unumdorligi va himoya darajasi o‘rtasidagi oltin muvozanatni topish demakdir. Kelajakda kvant kompyuterlarining paydo bo‘lishi hozirgi ko‘plab asimmetrik algoritmlarni zaif qilib qo‘yishi mumkinligi sababli, bugungi kunda post-kvant kriptografiyasi deb ataladigan yangi yo‘nalish ustida faol ish olib borilmoqda. Shunga qaramay, simmetrik va asimmetrik shifrlashning fundamental prinsiplari axborot xavfsizligining asosi bo‘lib qolaveradi. Xulosa qilib aytganda, simmetrik tizimlar tezlik va samaradorlikni, asimmetrik tizimlar esa kalitlarni boshqarish xavfsizligi va autentifikatsiyani ta’minlaydi. Ularning birgalikda qo‘llanilishi zamonaviy raqamli iqtisodiyot, elektron hukumat va global muloqot platformalarining xavfsiz ishlashiga imkon yaratadi. Har bir dasturchi yoki tarmoq xavfsizligi mutaxassisi ushbu ikki tizim o‘rtasidagi farqni chuqur tushunishi va ularni aniq vaziyatga qarab to‘g‘ri tadbiq eta olishi lozim.

Simmetrik va asimmetrik shifrlash tizimlarini qiyosiy tahlil qilish shuni ko‘rsatadiki, axborot xavfsizligini ta’minlashda ushbu ikki yondashuv bir-birini inkor etmaydi, balki to‘ldiradi. Simmetrik shifrlash o‘zining yuqori tezligi va hisoblash resurslariga bo‘lgan

kam talabi bilan katta hajmdagi ma’lumotlarni himoyalashda almashtirib bo‘lmas hisoblanadi. Biroq, kalitlarni xavfsiz taqsimlash muammosi uni global tarmoqlarda cheklangan holda qo‘llashga majbur qiladi. Asimmetrik shifrlash esa kalitlarni boshqarishning murakkab muammosini hal qilib, nafaqat maxfiylikni, balki elektron raqamli imzo orqali ma’lumotlarning haqiqiyligini tasdiqlash imkonini beradi.

Zamonaviy kriptografiyaning rivojlanish tendensiyasi ushbu ikki tizimning kuchli jihatlarini birlashtirgan gibrid modellarga tayanmoqda. Kelajakda kvant hisoblash texnologiyalari hozirgi algoritmlar uchun xavf tug‘dirsa-da, simmetrik va asimmetrik shifrlashning fundamental prinsiplari yangi avlod — post-kvant kriptografiyasi uchun asos bo‘lib xizmat qiladi. Axborot xavfsizligi mutaxassislari uchun har bir tizimning chegaralarini bilish va ularni aniq vaziyatga ko‘ra to‘g‘ri tanlash tizimning ishonchliligini ta’minlovchi eng muhim omildir.

Foydalanilgan adabiyotlar

1. G‘aniyev S.K., Karimov M.M., Tashev K.A. "Kriptografik usullar". — Toshkent: "Aloqachi", 2011.
2. Stallings, W. "Cryptography and Network Security: Principles and Practice" (8th Edition). — Pearson, 2020.
3. Schneier, B. "Applied Cryptography: Protocols, Algorithms, and Source Code in C". — Wiley, 2015.
4. Katz, J., & Lindell, Y. "Introduction to Modern Cryptography". — CRC Press, 2020.
5. O‘zbekiston Respublikasining "Elektron raqamli imzo to‘g‘risida"gi Qonuni. — Toshkent, 2022.