KRIPTOGRAFIYANING ZAMONAVIY KO'RINISHI

O'zbekiston Milliy universiteti
Jizzax filiali talabalari
Tilavov Shahzod
Qahhorov Jasur
Ilmiy raxbar: ***Mamaraimov Abror***

Annotatsiya*: Ushbu ishda kriptografiyaning asosiy tushunchalari, uning tarixiy rivojlanishi, zamonaviy kriptografik usullar va texnologiyalar, axborot xavfsizligidagi o'rni haqida keng qamrovli ma'lumotlar keltirilgan. Shuningdek, kriptografik algoritmlar, kalitlar, shifrlash turlari va ularning qo'llanilish sohalari yoritilgan. Ishda kriptografiyaning amaliyotdagi roli, muammolari va kelajakdagi istiqbollari ham ko'rib chiqilgan.*

Kalit So'zlar: Kriptografiya, Shifrlash algoritmlari, Simmetrik shifrlash, Assimmetrik shifrlash, Hash funksiyasi, Raqamli imzo, Elektron imzo, Axborot xavfsizligi, Xavfsiz aloqa, Kvant kompyuterlar, Kriptotahlil, Blokcheyn texnologiyalari, Elektron tijorat xavfsizligi, Ma'lumotlar himoyasi, Raqamli xavfsizlik, Public Key Infrastructure (PKI), Key management (Kalitlarni boshqarish), Xavfsiz aloqa protokollari (SSL/TLS), Cryptanalysis, Digital certificates, Xakerlik (Hacking), Kryptograflik tizimlar.

Kirish

Zamonaviy kriptografiya asosan uch asosiy elementga tayanadi: maxfiylik (confidentiality), yaxlitlik (integrity) va autentifikatsiya (authentication). Maxfiylik – bu ma'lumotlarni faqat ruxsat etilgan shaxslar o'qiy olishini ta'minlaydi. Yaxlitlik esa, ma'lumotlar yetkazish jarayonida o'zgartirilmaganligini kafolatlaydi. Autentifikatsiya orqali esa tizim foydalanuvchining kimligini tekshiradi. Kriptografiya bu uch vazifani bajarar ekan, raqamli texnologiyalar rivoji bilan birgalikda kundalik hayotimizning ajralmas qismiga aylanib bormoqda. Ayniqsa, elektron pochta, onlayn bank xizmatlari, ijtimoiy tarmoqlarda ma'lumotlar almashinuvi, elektron to'lovlar va hukumat tizimlarida kriptografiyaga ehtiyoj nihoyatda yuqori.

Kriptografiya ikki asosiy turga bo'linadi: simmetrik va assimmetrik.

Simmetrik kriptografiyada bir xil kalit ma'lumotni shifrlash va uni qayta ochishda ishlatiladi. Bu usul tezkorligi bilan ajralib turadi, lekin kalitni ishonchli tarzda yetkazib berish muammosi mavjud. Assimmetrik kriptografiyada esa, ikkita kalit ishlatiladi – ochiq (public key) va yopiq (private key). Ochiq kalit orqali ma'lumot shifrlansa, faqat mos keluvchi yopiq kalit orqali uni qayta ochish mumkin. Bu usul xavfsizlik darajasi yuqoriligi bilan mashhur bo'lib, elektron imzo, raqamli sertifikatlar va onlayn xavfsiz aloqa protokollarida keng qo'llaniladi.

RSA, ElGamal, Diffie-Hellman, AES, DES, SHA, ECC kabi algoritmlar zamonaviy kriptografiyaning ustun poydevorini tashkil qiladi. Masalan, RSA – bu eng mashhur assimmetrik kriptografiya algoritmlaridan biri bo'lib, katta sonlarni faktorlarga ajratish qiyinligiga asoslangan. AES esa simmetrik kriptografiyaning zamonaviy namunasi bo'lib, tezligi va xavfsizligi sababli dunyo bo'ylab hukumat va

tijorat tashkilotlarida foydalaniladi. SHAx (Secure Hash Algorithm) oilasi esa raqamli imzolar va ma’lumotlarni tekshirishda muhim rol o‘ynaydi.

Kriptografik tizimlarning kuchi ularning matematik asoslarida, ayniqsa son nazariyasi, algebra, kombinatorika va ehtimollik nazariyasida mujassamdir. Ayniqsa, butun sonlar ustida ishlovchi funksiyalar, eng kam umumiy karrali, eng katta umumiy bo‘luvchi, modul amallari kabi tushunchalar kriptografiya uchun muhim hisoblanadi. Shu bilan birga, kriptografik tizimlar faqat nazariy jihatdan kuchli bo‘lishi yetarli emas, ular amaliyotda ham xavfsiz va samarali ishlashi kerak. Shuning uchun har bir yangi tizim yoki algoritm juda ko‘p sinovlardan, hujum modellari orqali tekshiruvlardan o‘tkaziladi.

Raqamli xavfsizlikning yanada rivojlanib borishi bilan bir qatorda, kriptografiyaga tahdid soluvchi yangi texnologiyalar ham paydo bo‘lmoqda. Masalan, kvant kompyuterlari rivojlanishi bilan hozirgi kriptografik algoritmlarning ba’zilari xavf ostida qolishi mumkin. Shu sababli, zamonaviy olimlar post-kvant kriptografiyasi deb nomlanuvchi yangi yo‘nalish ustida faol ishlamoqdalar. Bu yo‘nalishda kvant hisoblashga chidamli algoritmlar ishlab chiqilmoqda. Bular esa yaqin yillarda global axborot xavfsizligini ta’minlashda asosiy rol o‘ynashi mumkin.

Kriptografiya faqat kompyuterlar va internet bilan bog‘liq soha emas. U davlatlar orasidagi diplomatik muloqot, harbiy strategiyalar, mobil telefonlar, sun’iy yo‘ldoshlar va hattoki oddiy foydalanuvchilarning parollarini saqlash tizimlarida ham qo‘llaniladi. Ayniqsa, elektron hukumat, elektron sog‘liqni saqlash, elektron savdo va boshqa raqamli xizmatlarda foydalanuvchilar ishonchini ta’minlashda kriptografiya hal qiluvchi rol o‘ynaydi. U orqali ma’lumotlar muhofazasi kuchayadi, noqonuniy kirishlar oldi olinadi va tizim ishonchliligi oshadi.

Umuman olganda, kriptografiya axborot xavfsizligining yuragi hisoblanadi.

U nafaqat maxfiylikni ta’minlaydi, balki jamiyatdagi ishonch muhitini yaratadi. Har bir tashkilot yoki individual foydalanuvchi raqamli makonda o‘z ma’lumotlarini muhofaza qilishni istasa, kriptografiya vositalaridan foydalanishi shart. Shu boisdan kriptografiya nafaqat texnik, balki strategik va ijtimoiy ahamiyatga ega sohaga aylanmoqda. Bu yo‘nalishda ilmiy izlanishlar, texnologik yutuqlar va xalqaro standartlar har doim yangilanib boradi, bu esa axborot jamiyati rivoji uchun poydevor yaratadi.

Kriptografiya – bu ma’lumotlarni yashirish, ularni faqat belgilangan shaxslar tushuna oladigan shaklga keltirish san’atidir. U tarixan odamlar o‘zaro maxfiy muloqot qilishni istaganidan boshlab paydo bo‘lgan va rivojlangan. Dastlabki davrlarda kriptografiya oddiy harflarni almashtirish yoki matnlarni maxfiy yozish shaklida qo‘llanilgan bo‘lsa, hozirda u juda murakkab matematik algoritmlarga asoslangan, yuqori darajadagi xavfsizlikni ta’minlaydigan ilmiy sohaga aylangan.

Kriptografiyaning asosiy vazifasi ma’lumotlarni maxfiy saqlash, ularni yetkazish jarayonida o‘zgartirib yuborilishining oldini olish, manbani aniqlash va xabar muallifini tasdiqlashdan iborat.

Zamonaviy kriptografiya asosan uch asosiy elementga tayanadi: maxfiylik (confidentiality), yaxlitlik (integrity) va autentifikatsiya (authentication). Maxfiylik – bu ma’lumotlarni faqat ruxsat etilgan shaxslar o‘qiy olishini ta’minlaydi. Yaxlitlik esa, ma’lumotlar yetkazish jarayonida o‘zgartirilmaganligini kafolatlaydi.

Autentifikatsiya orqali esa tizim foydalanuvchining kimligini tekshiradi. Kriptografiya bu uch vazifani bajarar ekan, raqamli texnologiyalar rivoji bilan birgalikda kundalik hayotimizning ajralmas qismiga aylanib bormoqda. Ayniqsa, elektron pochta, onlayn bank xizmatlari, ijtimoiy tarmoqlarda ma’lumotlar almashinuvi, elektron to‘lovlar va hukumat tizimlarida kriptografiyaga ehtiyoj nihoyatda yuqori.

Kriptografiya ikki asosiy turga bo‘linadi: simmetrik va assimmetrik.

Simmetrik kriptografiyada bir xil kalit ma’lumotni shifrlash va uni qayta ochishda ishlatiladi. Bu usul tezkorligi bilan ajralib turadi, lekin kalitni ishonchli tarzda yetkazib berish muammosi mavjud. Assimmetrik kriptografiyada esa, ikkita kalit ishlatiladi – ochiq (public key) va yopiq (private key). Ochiq kalit orqali ma’lumot shifrlansa, faqat mos keluvchi yopiq kalit orqali uni qayta ochish mumkin. Bu usul xavfsizlik darajasi yuqoriligi bilan mashhur bo‘lib, elektron imzo, raqamli sertifikatlar va onlayn xavfsiz aloqa protokollarida keng qo‘llaniladi.

RSA, ElGamal, Diffie-Hellman, AES, DES, SHA, ECC kabi algoritmlar zamonaviy kriptografiyaning ustun poydevorini tashkil qiladi. Masalan, RSA – bu eng mashhur assimmetrik kriptografiya algoritmlaridan biri bo‘lib, katta sonlarni faktorlarga ajratish qiyinligiga asoslangan. AES esa simmetrik kriptografiyaning zamonaviy namunasi bo‘lib, tezligi va xavfsizligi sababli dunyo bo‘ylab hukumat va tijorat tashkilotlarida foydalaniladi. SHAx (Secure Hash Algorithm) oilasi esa raqamli imzolar va ma’lumotlarni tekshirishda muhim rol o‘ynaydi.

Kriptografik tizimlarning kuchi ularning matematik asoslarida, ayniqsa son nazariyasi, algebra, kombinatorika va ehtimollik nazariyasida mujassamdir. Ayniqsa, butun sonlar ustida ishlovchi funksiyalar, eng kam umumiy karrali, eng katta umumiy bo‘luvchi, modul amallari kabi tushunchalar kriptografiya uchun muhim hisoblanadi. Shu bilan birga, kriptografik tizimlar faqat nazariy jihatdan kuchli bo‘lishi yetarli emas, ular amaliyotda ham xavfsiz va samarali ishlashi kerak. Shuning uchun har bir yangi tizim yoki algoritm juda ko‘p sinovlardan, hujum modellari orqali tekshiruvlardan o‘tkaziladi.

Raqamli xavfsizlikning yanada rivojlanib borishi bilan bir qatorda, kriptografiyaga tahdid soluvchi yangi texnologiyalar ham paydo bo‘lmoqda. Masalan, kvant kompyuterlari rivojlanishi bilan hozirgi kriptografik algoritmlarning ba’zilari xavf ostida qolishi mumkin. Shu sababli, zamonaviy olimlar post-kvant kriptografiyasi deb nomlanuvchi yangi yo‘nalish ustida faol ishlamoqdalar. Bu yo‘nalishda kvant hisoblashga chidamli algoritmlar ishlab chiqilmoqda. Bular esa yaqin yillarda global axborot xavfsizligini ta’minlashda asosiy rol o‘ynashi mumkin.

Kriptografiya faqat kompyuterlar va internet bilan bog‘liq soha emas. U davlatlar orasidagi diplomatik muloqot, harbiy strategiyalar, mobil telefonlar, sun’iy yo‘ldoshlar va hattoki oddiy foydalanuvchilarning parollarini saqlash tizimlarida ham qo‘llaniladi. Ayniqsa, elektron hukumat, elektron sog‘liqni saqlash, elektron savdo va boshqa raqamli xizmatlarda foydalanuvchilar ishonchini ta’minlashda kriptografiya hal qiluvchi rol o‘ynaydi. U orqali ma’lumotlar muhofazasi kuchayadi, noqonuniy kirishlar oldi olinadi va tizim ishonchliligi oshadi.

Umuman olganda, kriptografiya axborot xavfsizligining yuragi hisoblanadi. U nafaqat maxfiylikni ta’minlaydi, balki jamiyatdagi ishonch muhitini yaratadi. Har bir tashkilot yoki individual foydalanuvchi raqamli makonda o‘z ma’lumotlarini

muhofaza qilishni istasa, kriptografiya vositalaridan foydalanishi shart. Shu boisdan kriptografiya nafaqat texnik, balki strategik va ijtimoiy ahamiyatga ega sohaga aylanmoqda. Bu yo‘nalishda ilmiy izlanishlar, texnologik yutuqlar va xalqaro standartlar har doim yangilanib boradi, bu esa axborot jamiyati rivoji uchun poydevor yaratadi.

Xulosa

Kriptografiya – zamonaviy axborot texnologiyalari xavfsizligining ajralmas qismi bo‘lib, bugungi raqamli dunyoda shaxsiy, tijorat va davlat axborotlarini ishonchli himoya qilish imkonini beradi. U insoniyat tarixida qadimdan boshlab mavjud bo‘lib kelgan bo‘lsa-da, ayniqsa so‘nggi o‘n yilliklarda Internet va elektron axborot almashinuvi kengaygani sari uning ahamiyati keskin ortdi. Kriptografik tizimlar yordamida ma’lumotlarni shifrlash, foydalanuvchini autentifikatsiya qilish, elektron raqamli imzo, xavfsiz aloqani ta’minlash kabi muhim funksiyalar bajariladi.

Zamonaviy kriptografiyada simmetrik va assimmetrik shifrlash, hash funksiyalar, raqamli imzolar, sertifikatlar va blokcheyn texnologiyalari kabi ko‘plab yondashuvlar qo‘llaniladi. Ayniqsa, bank sohalari, elektron tijorat, tibbiyot axborot tizimlari va davlat maxfiy xizmatlari kriptografiyadan keng foydalanadi. Bu esa, sohaga bo‘lgan talabni yanada oshiradi va mutaxassislar uchun dolzarb yo‘nalishga aylantiradi.

Shuningdek, kriptografiyaning rivojlanishi bilan bog‘liq xavflar – xakerlik, kalitlarni buzish texnologiyalari, kvant kompyuterlar tahdidi kabi muammolar mavjud. Bularning oldini olish uchun zamonaviy algoritmlar, kriptotahlil uslublari va xavfsizlik siyosatlari doimiy ravishda yangilanib borishi lozim.

Xulosa qilib aytganda, kriptografiya — bu faqat matematik asoslarga qurilgan nazariy bilimlar emas, balki amaliy jihatdan juda muhim, hayotiy ehtiyojlarga moslashgan, doimiy rivojlanayotgan ilmiy sohaga aylandi. U nafaqat axborotni himoya qiladi, balki insonlarning raqamli erkinligini va xavfsizligini ta’minlaydi.

Foydalanilgan adabiyotlar

1. Stallings, William. *Cryptography and Network Security: Principles and Practice*. Pearson Education, 2017.
2. Schneier, Bruce. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Wiley, 1996.
3. Menezes, A. J., van Oorschot, P. C., and Vanstone, S. A. *Handbook of Applied Cryptography*. CRC Press, 1996.
4. Singh, Simon. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Anchor Books, 2000.
5. Zubairjon Rakhmatov. *Axborot xavfsizligi va kriptografiya asoslari*, Toshkent Axborot Texnologiyalari Universiteti nashriyoti, 2022.
6. Dasturiy vositalar va axborot xavfsizligi bo‘yicha O‘zbekiston Respublikasi normativ hujjatlari (www.lex.uz).
7. Khan, Md. Asaduzzaman, and M. M. Hassan. “A Review of Cryptographic Techniques for Secure Communication.” *International Journal of Computer Applications*, 2014.