TASHKILOT AXBOROT TIZIMLARIDA MA’LUMOTLARNI HIMOYALASH UCHUN ZAMONAVIY KRIPTOGRAFIK USULLAR TAHLILI

G‘ofurova Muxlisa G‘ulom qizi
Toshkent ijtomoiy innovatsiya universiteti talabasi
muxlisagofurova18@gmail.com

Annotatsiya: *Ushbu maqolada tashkilot axborot tizimlarida ma’lumotlar xavfsizligini ta’minlashda qo‘llaniladigan zamonaviy kriptografik usullar tahlil qilinadi. Simmetrik va assimmetrik shifrlash algoritmlari, xesh-funksiyalar, raqamli imzolar va transport qatlam xavfsizlik protokollari ko‘rib chiqiladi. Shuningdek, ma’lumotlarni uzatish va saqlash jarayonida kriptografiyaning o‘rni, afzalliklari va cheklovlari baholanadi. Tadqiqot natijalari asosida tashkilot axborot tizimlarida xavfsizlikni oshirish bo‘yicha tavsiyalar ishlab chiqiladi.*

Kalit so‘zlar: *axborot xavfsizligi, kriptografiya, simmetrik shifrlash, assimmetrik shifrlash, xesh-funksiyalar, raqamli imzo, TLS*

KIRISH

Raqamli transformatsiya jarayonlari natijasida tashkilot axborot tizimlarida qayta ishlanayotgan va saqlanayotgan ma’lumotlar hajmi keskin ortib bormoqda. Ushbu ma’lumotlar orasida shaxsiy, moliyaviy hamda tijorat siri bo‘lgan axborotlar mavjud bo‘lib, ularning maxfiyligi va yaxlitligini ta’minlash dolzarb masalaga aylangan.

Kiberhujumlar sonining ortib borishi va ma’lumotlar sizib chiqishi bilan bog‘liq holatlar kriptografik himoya vositalaridan samarali foydalanish zaruratini kuchaytirmoqda. Shu bilan birga, tashkilotlarda ko‘plab xodimlar va tashqi foydalanuvchilar mavjudligi, shifrlash kalitlarini boshqarish tizimining murakkabligi xavfsizlikni ta’minlashni yanada qiyinlashtiradi.

Mazkur maqolaning maqsadi – tashkilot axborot tizimlarida ma’lumotlarni himoyalashda zamonaviy kriptografik algoritmlarni tahlil qilish, ularning afzallik va kamchiliklarini aniqlash hamda xavfsizlikni oshirish bo‘yicha tavsiyalar ishlab chiqishdir [1].

Kriptografiyaning nazariy asoslari

Kriptografiya — ma’lumotlarni shifrlash orqali ularning maxfiyligi, yaxlitligi va autentikligini ta’minlovchi ilmiy va texnologik vositalar majmuasidir. Kriptografik himoya quyidagi asosiy vazifalarni bajaradi:

1-rasm. Kriptografik himoya asosiy vazifalari

Maxfiylik (Confidentiality): ma’lumotlar ruxsatsiz shaxslar tomonidan o‘qilmasligini ta’minlash.

Yaxlitlik (Integrity): ma’lumotlar uzatish yoki saqlash jarayonida o‘zgartirilmaganligini kafolatlash.

Autentifikatsiya (Authentication): foydalanuvchi va tizimning haqiqiyligini tasdiqlash.

Inkordan voz kechmaslik (Non-repudiation): yuboruvchi ma’lumot yuborilganini inkor qila olmasligini ta’minlash.

Zamonaviy kriptografiya matematik murakkablik nazariyasiga asoslanadi va hisoblash jihatdan buzilishi amalda imkonsiz bo‘lgan algoritmlardan foydalanadi [2].

Zamonaviy kriptografik usullar tahlili

1. Simmetrik shifrlash. Simmetrik shifrlashda shifrlash va deshifrlash jarayoni bitta umumiy kalit yordamida amalga oshiriladi. Bu algoritmlar yuqori tezlikda ishlashi bilan ajralib turadi, shuningdek, katta hajmdagi ma’lumotlar uchun qulay.

Keng qo‘llaniladigan algoritmlar: AES (Advanced Encryption Standard): Zamonaviy amamliyotda keng qo’llaniladigan algoritm hisoblanadi. U 128,192 va 256 bitli uzunliklarida ishlaydi. AES algoritimi blokli shifrlash prinsipi asosida qurilgan bo’lib, yuqori kriptobardoshlilikka ega.

DES (Data Encryption Standard): Tarixiy DES algoritmi esa bugungi kunda yetarli darajada xavfsiz emasligi sababli amaliyotga qo’llanilmaydi va tavsiya etilmaydi [3].

2. Assimmetrik shifrlash. Assimmetrik shifrlashda ochiq va yopiq kalitlar jufti ishlatiladi. Ochiq kalit orqali shifrlangan ma’lumot faqat yopiq kalit yordamida deshifrlanadi.

Keng qo‘llaniladigan algoritmlar: RSA algoritmi kata sonlarni faktorizatsiya qilishning murakkabligiga asoslangan. U ko’pincha kalit almashinuvi va raqamli imzoda ishlatiladi.

Diffie–Hellman algoritmi ochiq aloqa kanali orqali ikki tomon o’rtasida umumiy maxfiy kalit hosil qilish imkonini beruvchi assimmetrik kalit almashish mexanizmidir. Algoritm diskret logarifm muammosining hisoblash murakkabligiga asoslangan

bo'lib, zamonaviy TLS protokolida sessiya kalitini generatsiya qilishda keng qo'llaniladi [4].

3. Xesh funksiyalar va raqamli imzo. Ma'lumotni xeshlash uning yaxlitligini kafolatlash maqsadida amalga oshirilib, agar ma'lumot uzatilishi davomida o'zgarishga uchrasa, uni aniqlash imkoni mavjud bo'ladi. Xesh-funksiyalarda odatda kiruvchi ma'lumotning uzunligi o'zgaruvchan, chiqishda esa o'zgarmas uzunlikdagi qiymatni qaytaradi. Zamonaviy xesh funksiyalarga MD5, SHA1, SHA256, O'z DSt 1106:2009 larni misol keltirish mumkin.

Raqamli imzolar - ma'lumot yuboruvchi shaxsni autentifikatsiya qiladi va inkordan voz kechmaslikni ta'minlaydi.

Transport Layer Security protokoli (TLS)

Tarmoq orqali uzatilayotgan ma'lumotlarni himoyalashda TLS protokoli muhim ahamiyatga ega. Ushbu protokol mijoz va server o'rtasida xavfsiz kanal yaratib, ma'lumotlarning maxfiyligi, yaxlitligi hamda autentifikatsiyasini ta'minlaydi. TLS mexanizmi assimmetrik va simmetrik kriptografik algoritmlarni birgalikda qo'llashga asoslangan bo'lib, zamonaviy veb-ilovalar va axborot tizimlarida keng qo'llaniladi. Zamonaviy tizimlarda TLS 1.3 versiyasi yuqori darajadagi xavfsizlik va tezlikni ta'minlaydi.

TLS protokolida handshake jarayoni orqali mijoz va server o'rtasida xavfsiz aloqa o'rnatiladi. Ushbu jarayonda tomonlar o'zaro kriptografik algoritmlarni kelishib oladi, serverning haqiqiyligi sertifikat orqali tekshiriladi hamda sessiya kaliti yaratiladi. Natijada ma'lumotlar uzatish jarayoni simmetrik shifrlash yordamida himoyalangan holda amalga oshiriladi [5].

XULOSA

O'tkazilgan tahlil shuni ko'rsatadiki, tashkilot axborot tizimlarida kriptografik usullardan to'g'ri va kompleks foydalanish axborot xavfsizligini sezilarli darajada oshiradi. Simmetrik va assimmetrik shifrlash algoritmlarini birgalikda qo'llash, xesh-funksiyalar va raqamli imzolar yordamida ma'lumotlarning maxfiyligi, yaxlitligi va autentifikatsiyasi ta'minlanadi. Biroq samaradorlik faqat algoritm tanlashga bog'liq emas, balki ularning to'g'ri joriy etilishi, kalitlarni boshqarish va xodimlar bilim darajasiga ham bog'liq. Shu sababli tashkilotlarda zamonaviy kriptografik standartlardan foydalanish va xavfsizlik siyosatini muntazam yangilab borish tavsiya etiladi.

FOYDALANILGAN ADABIYOTLAR

1. Maxmudov R.X. Kriptografiya va axborotlarni himoyalash usullari. – Toshkent: Aloqachi, 2020. – 312 b.
2. Turg'unov B.Sh. Tarmoq xavfsizligi va kriptografik protokollar. – Toshkent: TATU nashriyoti, 2021. – 198 b.

3. Xudoyberdiyev O.T. Zamonaviy kriptografik algoritmlar tahlili va ularning samaradorligi. // Muhammad al-Xorazmiy nomidagi TATU ilmiy axborotnomasi. – 2023. – №2. – B. 67–74.
4. Yusupov S.Q. AES va RSA algoritmlarining taqqoslama tahlili. // Kompyuter tizimlari va axborot texnologiyalari. – 2021. – №4. – B. 88–96.
5. Karimov N.J. TLS protokolining xavfsizlik mexanizmlari va amaliy qo‘llanilishi. // Axborot kommunikatsiya texnologiyalari va telekommunikatsiya muammolari. – 2022. – №1. – B. 101–108.