18-mavzu. Axborotni Kriptografik Himoyalash

Reja:

1. **Kriptografiya Turlari**
2. **Kriptografik Himoyalash Elementlari**
3. **Kriptografik Himoyalashning Qo‘llanilishi kamchiliklari**

Axborotni kriptografik himoyalash — axborotni uchinchi shaxslar tomonidan o‘qib bo‘lmaydigan holatga keltirish orqali himoya qilish usuli hisoblanadi. Kriptografik himoya ko‘p jihatdan ma’lumotlarning xavfsizligini ta’minlash uchun ishlatiladi va ayniqsa raqamli axborot almashinuvida muhim rol o‘ynaydi.

1. **Simmetrik kriptografiya** (yoki bir kalitli): Bu usulda ma’lumotni shifrlash va shifrdan chiqarish uchun bitta umumiy kalit ishlatiladi. Simmetrik kriptografiya tez ishlaydi, lekin kalitni xavfsiz yetkazish zarurati yuzaga keladi. Masalan, **AES** (Advanced Encryption Standard) algoritmi.
2. **Asimmetrik kriptografiya** (yoki ikki kalitli): Bu usulda ikkita kalitdan foydalaniladi: biri ma’lumotni shifrlash uchun (ommaviy kalit), ikkinchisi esa shifrdan chiqarish uchun (xususiy kalit). Asimmetrik kriptografiya ma’lumotlarni xavfsiz uzatish uchun juda qulaydir, lekin u simmetrik kriptografiyaga nisbatan sekinroq. Masalan, **RSA** va **ECC** algoritmlari.
3. **Gibrid kriptografiya**: Simmetrik va asimmetrik kriptografiya usullarini birlashtiradi. Asimmetrik kriptografiya kalitlarni almashish uchun, simmetrik esa ma’lumotlarni shifrlash uchun ishlatiladi.

1. **Shifrlash va Shifrdan Chiqish**: Ma’lumotni shifrlashda o‘zgartirilgan holda uzatiladi, shifrdan chiqarish jarayonida asl holatiga qaytariladi.
2. **Kalit Boshqaruvi**: Kriptografik himoyalashning ishonchli amalga oshirilishi kalitlarni xavfsiz boshqarish va tarqatish jarayonlariga bog‘liq.
3. **Xeshlash**: Ma’lumotlarning yaxlitligini tekshirish uchun foydalaniladi. Masalan, **SHA-256** xesh algoritmi keng qo‘llaniladi. Xeshlash funksiyasi orqali ma’lumotlar qisqa, o‘zgarmas xesh-kodga aylantiriladi.
4. **Elektron Raqamli Imzo**: Ma’lumotning haqiqiyligini va jo’natuvchining identifikatsiyasini tasdiqlash uchun ishlatiladi. Bu ma’lumotlarga kiritilgan o‘zgarishlarni aniqlash imkonini beradi.

Kriptografik Himoyalash Dasturlari

1. **PGP (Pretty Good Privacy)**: Elektron pochta va fayllarni shifrlash uchun ishlatiladi.

2. **SSL/TLS**: Internet tarmoqlari orqali uzatilayotgan ma’lumotlarning xavfsizligini ta’minlash uchun ishlatiladi.
3. **VPN (Virtual Private Network)**: Tarmoqda maxfiy va xavfsiz aloqa o‘rnatadi.

Kriptografik Himoyalashning Qo‘llanilishi

Bank va moliya tizimlari: Internet-banking xizmatlari orqali amalga oshiriladigan tranzaktsiyalarda kriptografiya ishlatiladi.
Elektron tijorat: Kredit karta va boshqa moliyaviy ma’lumotlarni himoya qilish uchun SSL/TLS sertifikatlari qo‘llaniladi.
Davlat tashkilotlari: Maxfiy axborotlarni himoya qilish uchun yuqori darajadagi shifrlash algoritmlari qo‘llaniladi.

Kriptografik Himoya Kamchiliklari

Kalitni boshqarishdagi qiyinchiliklar: Kalitlarni himoyalash va almashish jarayonida maxfiylikni ta’minlash muammolari yuzaga keladi.
Algoritmlarning buzilish ehtimoli: Zamonaviy texnologiyalar yordamida ayrim kriptografik algoritmlar buzilishi mumkin.

Kriptografik himoyalash axborot xavfsizligini ta’minlashda samarali va ishonchli vosita hisoblanadi. U davlat, biznes va boshqa sohalarda ma’lumotlarni himoya qilish, maxfiyligini saqlash va yaxlitligini ta’minlash uchun keng qo‘llaniladi.