AXBOROTNI YASHIRISH ZARURATI VA KRIPTOGRAFIYANING RIVOJLANISH BOSQICHLARI.

Abu Rayhon Beruniy nomidagi Urganch davlat universiteti
“Kompyuter ilmlari” kafedrasi katta o‘qituvchisi
Xudoyberganov Bozorboy Allamovich

Abu Rayhon Beruniy nomidagi Urganch davlat universiteti
“Kompyuter ilmlari” kafedrasi o‘qituvchisi
Yusupov Shuxrat Raximovich

Abu Rayhon Beruniy nomidagi Urganch davlat universiteti
“Kompyuter ilmlari” kafedrasi o‘qituvchisi
Xusainov Shixnazar Madaminovich

Abu Rayhon Beruniy nomidagi Urganch davlat universiteti
“Kompyuter ilmlari” kafedrasi o‘qituvchisi
Bekchanov Hikmat Mansurbek o'g'li

Annotatsiya

Ushbu maqolada axborot xavfsizligini ta'minlashda kriptografiyaning tutgan o‘rni, tarixiy rivojlanish bosqichlari hamda amaliy qo‘llanilishi yoritib berilgan. Yozma axborotlarni begona shaxslardan himoya qilish zarurati kriptografik metodlarning paydo bo‘lishiga olib keldi. Maqolada simmetrik va assimmetrik shifrlash tizimlarining xususiyatlari, DES, RSA va AES kabi standartlarning ahamiyati, hamda kriptotahlil usullari haqida so‘z boradi. Shuningdek,

kriptografiyaning elektron raqamli imzo, elektron to‘lov va kvant kriptografiyasi kabi zamonaviy yo‘nalishlardagi ahamiyati yoritilgan.

Kalit so'zlar: Kriptografiya, shifrlash algoritmlari, axborot xavfsizligi, simmetrik kriptotizim, assimmetrik kriptotizim, DES, RSA, AES, kriptotahlil, raqamli imzo, axborotni yashirish.

Jamiyat taraqqiyoti davomida yozuvning keng ommalashuvi natijasida xatlar va xabarlar orqali axborot almashish ehtiyoji vujudga keldi. Bunday axborot almashinuvi esa, o‘z navbatida, yozma ma’lumotlar mazmunini ruxsatsiz shaxslardan yashirish zaruratini keltirib chiqardi. Axborotni yashirishga qaratilgan metodlar shartli ravishda uchta asosiy guruhga bo‘linadi:

1. **Stenografik (maskirovka) usullar** – mavjud axborotni tashqi ko‘rinishda yashirishga yo‘naltirilgan bo‘lib, faktning o‘zini yashirishni ta’minlaydi.
2. **Kriptografik metodlar** – xat va ma’lumotlarni maxfiy belgilar yordamida kodlash orqali yashirishni nazarda tutadi. “Kriptografiya” atamasi yunoncha *kryptos* (yashirin) va *grapho* (yozmoq) so‘zlaridan kelib chiqqan bo‘lib, “yashirin yozuv” degan ma’noni anglatadi.
3. **Maxsus texnik vositalardan foydalanuvchi metodlar** – axborotni maxfiylashtiruvchi texnik qurilmalarga asoslangan bo‘lib, ayniqsa 1970-yillardan boshlab keng qo‘llanila boshlandi. Bu usullar shifrlashning yuqori tezlikda bajarilishini va yuqori darajadagi kriptobardoshlilikni ta’minlovchi samarali hisoblash vositalarining paydo bo‘lishi bilan rivojlandi.

Blokli shifrlash tizimlarining rivojlanishi

Zamonaviy kriptografiyada ilk amaliy kriptotizimlar sifatida blokli shifrlash tizimlari alohida o‘rin egallaydi. 1970-yilda AQSHda IBM kompaniyasi tomonidan ishlab chiqilgan va 1978-yilda rasmiy standart sifatida tasdiqlangan

DES (Data Encryption Standard) algoritmi blokli simmetrik shifrlash tizimlarining ilk namunasi bo‘ldi. DES algoritmining asosiy g‘oyaviy mualliflaridan biri Xorst Feystel bo‘lib, u keyinchalik boshqa ko‘plab simmetrik kriptosistemalarning (masalan, GOST 28147-89) asosini tashkil etuvchi blokli shifrlash modelini ishlab chiqqan.

Kriptotahlilning shakllanishi

DES algoritmining keng qo‘llanilishi kriptotahlil (kriptografik tahlil) yo‘nalishining rivojlanishiga ham turtki bo‘ldi. Aynan shu davrda chiziqli, differensial va boshqa murakkab hujum usullari shakllantirildi. Biroq ularning amaliyotda samarali qo‘llanilishi faqat yuqori quvvatli hisoblash texnologiyalarining rivojlanishi bilan bog‘liq bo‘ldi.

Assimmetrik kriptotizimlarga o‘tish

1970-yillarning ikkinchi yarmida zamonaviy kriptografiyada tub burilish ro‘y berdi – **assimmetrik kriptotizimlar** paydo bo‘ldi. Bu tizimlarda axborotni shifrlash va deshifrlash uchun turli kalitlar qo‘llaniladi, ya’ni maxfiy kalitni avvaldan uzatish shart emas. Bu g‘oya 1976-yilda Uitfild Diffi va Martin Xellman tomonidan chop etilgan “Zamonaviy kriptografiyaning yangi yo‘nalishlari” nomli ilmiy ishda asoslab berilgan.

Ular bilan bir vaqtda Ralf Merkli ham assimmetrik shifrlash g‘oyasini mustaqil ishlab chiqdi. Bir necha yil o‘tib, Ron Rivest, Adi Shamir va Leonard Adleman tomonidan katta tub sonlarni faktorizatsiya qilish muammosiga asoslangan birinchi amaliy assimmetrik kriptotizim – **RSA algoritmi** ishlab chiqildi. Ushbu yangiliklar kriptografiyada elektron raqamli imzo, elektron to‘lov tizimlari kabi yangi amaliy yo‘nalishlarning shakllanishiga olib keldi.

Yangi avlod kriptotizimlari

1980–1990-yillarda kriptografiyaning mutlaqo yangi yo‘nalishlari – **ehtimolli shifrlash, kvant kriptografiyasi** kabi konseptlar yuzaga keldi. Ularning amaliy qo‘llanilishi hozircha keng emas, ammo kelajakda katta salohiyatga ega yo‘nalishlar hisoblanadi.

Shu bilan birga, simmetrik kriptotizimlarni takomillashtirish jarayoni ham davom etdi. **Feystel tuzilmasiga ega bo‘lmagan shifrlash algoritmlari** – SAFER, RC6 va boshqalar ishlab chiqildi. 2000-yilda esa xalqaro ochiq tanlov asosida AQSH tomonidan yangi milliy standart – **AES (Advanced Encryption Standard)** algoritmi qabul qilindi.

Kriptografiyaning axborot xavfsizligidagi o‘rni

Kriptografiya bugungi kunda axborotning konfidensialligi, yaxlitligi va autentifikatsiyasini ta’minlovchi eng muhim va qudratli vositalardan biri hisoblanadi. U dasturiy va texnik himoya choralarining markazida turadi. Ayniqsa, portativ qurilmalarda, ma’lumotlarni jismoniy himoyalashning qiyinligi inobatga olinsa, faqat kriptografik vositalar orqali axborot o‘g‘irlanganda ham uning maxfiyligini saqlab qolish mumkin bo‘ladi.

Foydalanilgan adabiyotlar.

1. Коробейников А.Г., Гатчин Ю.А. Математические основы криптологии. Учебное пособие. Санкт-Петербург-2004.

2. Акбаров Д.Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланишлари. Тошкент. ”Ўзбекистон маркаси “, 2009. – 432 б.

3. «Ошкора калитли криптотизимларни криптотаҳлиллаш учун қуролу-воситалар ишлаб чиқиш ва уларни тадқиқ этиш» мавзуси бўйича бажарилган илмий-тадқиқот ишининг 1-8 -босқич ҳисоботлари. – ЎзААА

ФТМТМ, Тошкент, 2003.

4.Защита информации. Малый тематический выпуск. ТИИЭР, 1988 г, т.76, №5.

5.Kahn D. The codebreakers. N.-Y., 1967.

6. Саломаа А. Криптография с открытым ключом. М.,1997