KODLANGAN ALOQANI PAYDO BO‘LISHI VA RIVOJLANISH TARIXI

Farmanov M.G

Chirchiq oliy tank qo‘mondonlik muhandislik Qo‘shinlar kundalik faoliyati va qo‘shinlarni boshqarish kafedrasi, Aloqa va axborot tizimlari sikli o‘qituvchisi, podpolkovnik

Annotatsiya: *Ushbu maqolada kodlangan aloqa tushunchasi uning kelib chiqish tarixi, qanday maqsadlarda qo‘llanilgani, keyinchalik qo‘shinlarni boshqarishda ham qo‘llash usul va uslublari to‘g‘risida va unga qoyilgan talablar shu bilan birga harbiy maqsadlarda qollashning ijobiy natijalari boyicha ma’lumotlar keltirib o‘tilgan.*

Kalit sozlar: *Kodlangan aloqa, vijener shifri, kriptografiya, enigma mashinasi, simmetrik va assimetrik shifrlash, kvant kriptografiyasi.*

Annotation: *This article presents the concept of coded communication, its history of origin, the purposes for which it was used, the methods and techniques of its later use in commanding troops, the requirements placed on it, as well as the positive results of its use for military purposes.*

Keywords: *Coded communication, Vigenère cipher, cryptography, enigma machine, symmetric and asymmetric encryption, quantum cryptography.*

Hozirgi raqamli texnologiyalar asrida qo‘shinlarni boshqarish tizimlarida axborotni himoya qilish, uni faqat kerakli shaxslar tomonidan tushuniladigan shaklda uzatish muhim masalaga aylangan. Bu jarayon kodlangan aloqa (kriptografiya) deb ataladi. Kodlangan aloqa axborotni shifrlash, ya’ni uni yashirin shaklga o‘zgartirish orqali amalga oshiriladi, shu maqsadda kuchli dasturiy ta'minot va hisoblash tizimlarini keng joriy etish sezilarli darajada oshirildi. Biroq, bunday tizimlarning joriy etilishi juda qadimgi davrlarga borib taqaladi.

Boshlang‘ich davr (Qadimgi davrlar) Kodlangan aloqa insoniyat tarixi davomida axborotni yashirin saqlash va uni faqat tegishli shaxslar o‘qiy olishi uchun qo‘llanilgan. Dastlabki kodlash usullari oddiy bo‘lib, asosan harflarni almashtirishga asoslangan.

Misr va Mesopotamiya: Qadimgi Misrda maxfiy yozuvlar (ierogliflar) marosimlarda va sirli bilimlarni uzatishda ishlatilgan.

Skitala (yunonlar): Qadimgi Spartada maxfiy xabarlar tayoqchaga o‘ralgan pergamentga yozilgan – bu “skitala” deb atalgan.

Sezar shifri (miloddan avvalgi I asr): Rim imperatori Yuliy Sezar harflarni ma’lum sondagi harflar bilan siljitib, oddiy lekin samarali shifr yaratgan.

O‘rta asrlar Bu davrda diniy va harbiy maqsadlarda kriptografiya keng qo‘llanilgan.

Arab olimlari: IX asrda arab matematiklari, ayniqsa Al-Kindiy, statistik tahlil usullaridan foydalanib, shifrlarni ochish ustida ishlagan.

Templar ritsarlari va muqaddas urushlar davrida diniy ordenlar o‘z maxfiy yozish tizimlariga ega bo‘lishgan.

Leon Battista Alberti (XV asr): “kriptografiyaning otasi” sifatida tanilgan, u birinchi bo‘lib ko‘p alfavitli shifrlash usulini ishlab chiqqan (polialfavit shifrlash).

Renessans va Yangi davr-Vijener shifri (XVI asr): Fransuz diplomati Blez Vijener tomonidan taklif qilingan polialfavit shifr bo‘lib, uzoq vaqt davomida “shifrlab bo‘lmaydigan” deb hisoblangan.

Fridrix Vilgelm va nemis kriptografiyasi: XVIII-XIX asrlarda Yevropada diplomatik yozishmalarda maxfiy aloqa keng rivoj topdi.

XX asr – Zamonaviy kriptografiya asosi-Enigma mashinasi (1930–40-yillar): Ikkinchi jahon urushida nemislar tomonidan ishlatilgan shifrlash qurilmasi. Uni yechish ingliz matematiklari, ayniqsa Alan Turing tomonidan amalga oshirilgan.

AES, RSA, DES algoritmlari: XX asr oxirlarida kompyuterlar paydo bo‘lishi bilan matematik asoslangan kuchli kriptografik algoritmlar ishlab chiqildi.

XXI asr – Raqamli era-Internet xavfsizligi: Bugungi kunda kodlangan aloqa internetdagi barcha maxfiy operatsiyalar (bank operatsiyalari, ijtimoiy tarmoqlar, davlat aloqalari) uchun asosiy rol o‘ynaydi.

Simmetrik va assimetrik shifrlash: Raqamli imzo, autentifikatsiya, elektron kalitlar orqali ishlovchi tizimlar keng qo‘llanilmoqda.

Kvant kriptografiyasi: So‘nggi yillarda kvant mexanikasiga asoslangan aloqa tizimlari ishlab chiqilmoqda – bu shifrlashni yanada mukammal qiladi.

Kodlangan aloqaning turlari

Kodlangan aloqa bir nechta turlarga bo‘linadi. Har biri o‘zining afzallik va qo‘llanish sohasiga ega.

1. Simmetrik shifrlash

Bu usulda bir xil kalit yordamida ham shifrlash, ham yechish amalga oshiriladi. Yuboruvchi va qabul qiluvchi bir xil kalitga ega bo‘lishi kerak.

Afzalliklari:

- tez ishlaydi;
- kichik hajmdagi ma’lumotlar uchun qulay.

Kamchiliklari:

- kalitni xavfsiz uzatish muammosi mavjud.

Misollar:

- DES (Data Encryption Standard);
- AES (Advanced Encryption Standard).

2. Assimetrik shifrlash

Bu usulda ikkita kalit ishlatiladi: biri – ochiq (public), ikkinchisi – maxfiy (private). Ochiq kalit bilan shifrlangan ma’lumotni faqat maxfiy kalit yecha oladi.

Afzalliklari:

- kalitlar almashinuvi xavfsiz;
- autentifikatsiya va raqamli imzoni qo‘llab-quvvatlaydi.

Kamchiliklari:

- simmetrik shifrlashga nisbatan sekinroq ishlaydi.

Misollar:

- RSA (Rivest-Shamir-Adleman);
- ElGamal algoritmi.

3. Raqamli imzo

Bu maxsus shifrlash turi bo‘lib, xabarning haqiqiy yuboruvchisini aniqlash va xabar o‘zgartirilmaganligini tasdiqlashda qo‘llaniladi. Asosan, huquqiy va moliyaviy tizimlarda keng qo‘llanadi.

4. Hashlash (Bir yo‘nalishli shifrlash)

Bu usulda axborot ma’lum matematik formulalar asosida yagona uzunlikdagi kodga aylantiriladi. Uni yana ochiq matnga aylantirib bo‘lmaydi. Parollar va fayl tekshiruvida ishlatiladi.

Misollar:

- MD5;
- SHA-1;
- SHA-256.

Xulosa qilib shuni ta’kidlash lozimki, kodlangan aloqa insoniyat tarixining har bir bosqichida – harbiy, diniy, diplomatik va texnologik sohalarda – muhim rol o‘ynab kelgan.

Uning rivojlanishi axborot xavfsizligining yangi bosqichlarga ko‘tarilishiga olib keldi, hamda kelajakda ham muhim rol o‘ynaydi.

FOYDALANILGAN ADABIYOTLAR:

1. Stallings, W. Cryptography and Network Security: Principles and Practice.

2. Kaufman, C., Perlman, R., & Speciner, M. Network Security: Private Communication in a Public World.

3. O‘zbekiston Respublikasi axborot xavfsizligi to‘g‘risidagi qonunlari.

4. Oliy ta’lim darsliklari va ma’ruzalar to‘plami.