«MA'LUMOTLARNI KODLASH VA SHIFRLASH»

Исманова Маргуба Нумоновна
МВД Наманганский академический лицей
учитель информатики,
Эл-почта: ismanovamarguba99@gmail.com

Annotatsiya: *Ushbu maqolada ma'lumotlarni kodlash va shifrlash usullari to'g'risida ma'lumot berib o'tilgan. Ayrim kodlash usullari alohida tahlil etilgan.*
Kalit so'zlar: *Kriptografiya, shifrlash, kodlash, algoritm, deshifrlash, almashtirish.*

КОДИРОВАНИЕ И ШИФРОВАНИЕ ДАННЫХ

Аннотация: *В этой статье представлена информация о том, как кодировать и шифровать данные. Некоторые методы кодирования анализируются отдельно.*
Ключевые слова: *Криптография, шифрование, кодирование, алгоритм, дешифрование, переключение.*

DATA CODING AND ENCRYPTION

Ismanova Marg'uba Numonovna
Ministry of Internal Affairs Namangan Academic Lyceum
Informatics teacher
, E-mail: ismanovamarguba99@gmail.com

Annotation: *This article provides information on how to encode and encrypt data. Some coding methods are analyzed separately.*
Keywords: *Cryptography, encryption, coding, algorithm, decryption, switching.*

Axborot so'zi lotincha "information" -tushuntirmoq, bayon etmoq so'zidan olingan bo'lib, zamonaviy fan va siyosatning asosiy tushunchalaridan biri bo'lib xizmat qiladi. Dastlab kishilar tomonidan og`zaki, keyinroq yozma yoki boshqa shakllar uzatilgan ma`lumot sifatida qaralgan bo'lsa, XX asrning o`rtalaridan boshlab insonlararo, inson-avtomat, avtomat-avtomat o`rtasidagi ma`lumot hamda hayvonlar va o`simliklardagi signal almashinuvi, hujayrada hujayraga muayyan belgilarning uzatilishi va shu kabilarni anglata boshlagan.

Axborotning muhimlik darajasi qadim zamonlardan ma'lum. SHuning uchun xam qadimda axborotni himoyalash uchun turli xil usullar qo'llanilgan. Ulardan biri – sirli yozuvdir. Undagi xabarni xabar yuborilgan manzil egasidan boshqa shaxs o'qiy olmagan. Asrlar davomida bu san'at – sirli yozuv jamiyatning yuqori tabaqalari, davlatning elchixona rezidentsiyalari va razvedka missiyalaridan tashqariga chiqmagan. Faqat bir necha o'n yil oldin hamma narsa tubdan o'zgardi, ya'ni axborot o'z qiymatiga ega bo'ldi va keng

tarqaladigan mahsulotga aylandi. Uni endilikda ishlab chiqaradilar, saqlaydilar, uzatishadi, sotadilar va sotib oladilar. Bulardan tashqari uni o'g'irlaydilar, buzib talqin etadilar va soxtalashtiradilar. Shunday qilib, axborotni himoyalash zaruriyati tug'iladi. Axborotni qayta ishlash sanoatining paydo bo'lishi axborotni himoyalash sanoatining paydo bo'lishiga olib keladi. Bu esa o'z navbatida axborot xavfsizligi tushunchasi kirib kelishiga sababchi bo'ldi.

Axborot xavfsizligining dolzarblashib borishi, axborotning strategik resursga aylanib borishi bilan izohlash mumkin. Bu zarurat axborotlarni kodlash hamda shifrlash jabhasida yanada ulkan ishlar amalga oshirishga turtki bo'ldi desak mubolag'a bo'lmaydi.

Kodlash - bir kodni belgilarini yoki belgilar guruhini boshqa kod belgilariga yoki belgilar guruhiga keltirish. Biror aloqa kanaliga yoki qandaydir boshqa qurilmaga 1243 axborot shaklini moslashtirish talab etilganda amalga oshiriladi. Masalan, harflar ketma-ketligi ko'rinishidagi axborotlar telegraf kodi yordamida ma'lum impulsi toklarga aylantiriladi. Bularni hisoblash qurilmasiga kiritilganda o'nli sistemadagi sonlar ikkilik sistemasiga o'zgartiriladi va boshqa kodlashdan ko'p sohalarda foydalaniladi.

Shifrlash - Kriptografik uslublardan foydalanishga asoslangan axborotni o'zgartirish jarayoni. Axborotni shifrlash uni begonalar tomonidan o'rganish yoki o'zgartirish imkoniyatini yo'qqa chiqaradi. Shuningdek, ma'lumotlarga va dasturlarga, ulardan noqonuniy foydalanish maqsadida, ruxsatsiz raqamli imzo tizimiga kirishning oldini olishni ta'minlaydi.

Shifrlashning ikki usuli mavjud:

- Simmetrik- Simmetrik shifrlashda, kodlash va kodni ochish uchun birgina kalitning o'zidan foydalaniladi;
- Asimmetrik- Asimmetrik shifrlashda ikkita kalitdan foydalaniladi. Ulardan biri (ochiq kalit) dastlabki matnni shifrmatnga o'girishni, ikkinchisi esa (yopiq kalit) dastlabki matnga o'girishni ta'minlaydi. Samaradorlikni yanada oshirish maqsadida simmetrik va asimmetrik shifrlash algoritmlari birgalikda ishlatiladi. Bu holatda simmetrik shifrlashdan ma'lumotlarni ochiq kanallar orqali uzatishda ma'lumotlarni shifrlashda, asimmetrik shifrlashdan esa simmetrik shifrlash algoritmlarining kalitlarini shifrlashda ishlatiladi.

Ma'lumotlarni shifrlash – bu axborot himoyaning dasturlar vositasining turlari va amaliyotda alohida o'rniga ega axborotni birdan bir ishonchli himoyasi.

"Shifrlash" tushunchasi "Kriptografiya" tushunchasiga qaraganda ko'proq ishlatadi. Kriptografiyani ichiga shifrlash kiradi va sonli ma'lumotlarni imkoni boricha almashtirishga bog'liq muammolarni hal etish usullarini qo'shimcha ko'rib chiqadi. Shifrlash algoritmi maxfiy emas ammo, yopilgan kalitni bilmasdan deshifrlash juda qiyin. Zamonaviy shifrlash dasturlari bu xususiyatini kalitdan foydalanib berilgan ochiq axborotni ko'p pog'onali qayta ishlash jarayonida ta'minlaydi. Umuman 1244 aytganda, shifrlash uchun foydalaniladigan har bir murakkab usullar (algoritmlar) nisbatan oddiy usullarni kombinatsiyasini ifodalaydi.

Shifrlash klassik algoritmlari bir-biridan quyidagicha farq qiladi:

- ❖ algoritmlash;
- ❖ o'rin almashtirish;
- ❖ gammalshtirish.

Almashtirish ishlatadigan alfavit o‘rniga alternativ alfavitlardan foydalanishni nazarda tutadi.

Oddiy almashtirish bo‘lsa, masalan, ingliz alfavit simvollari uchun quyidagi almashuvini taklif qilish mumkin: “cache” degan so‘z shifrlangan ko‘rinishda “usuxk” bo‘ladi. Biroq xolis olingan uzun matnda simvollarni ma’lum statistik chastotasini qaytarilishi yordamida xabarni shifrini yechish imkoniyati mavjud.

Ko‘p alfavitli almashtirishda shunday qilish mumkinki, shifrlangan matnda xamma simvollar bir xil chactotada uchrashi mumkin, bu esa shifrlangandagi alternativ alfavit va tartibni bilmasdan turib shifrni yechish ancha qiyinchiliklarga olib keladi.

Sonli kalit qaytarilmaydigan sonlardan unga tegishli kalit so‘zi esaqaytarilmaydigan simvollardan iborat. Kelib chiqadigan matn kalit tagiga qatormaqator yoziladi. Shifrlangan xabar ustunlarga kalit sonlariga qarab o‘sha tartibda yozib chiqishadi.

Shifrlashning klassik usullari almashtirish, o‘rnini almashtirish va gammalashtirish bular - to‘g‘ri chiziqli deyish mumkin shu ma’nodaki, shifrlangan xabarning uzuligi berilgan matnning uzunligiga teng. Chiziqli bo‘lmagani qayta tuzish mumkin.

Shuni ta’kidlash joizki, maxfiy va shaxsiy axborotlarga ruxsatsiz kirishdan himoyalash eng muhim vazifalardan biri hisoblanadi. Foydalanuvchilarning mulki huquqlarini himoyalash - bu ishlab chiqarilayotgan axborotlarni jiddiy iqtisodiy va boshqa moddiy hamda nomoddiy zararlar keltirishi mumkin bo’lgan turli kirishlar va o’g’irlashlardan himoyalash ishlab chiqaruvchining asosiy vazifalaridan biri bo’lib hisoblanadi. Buning uchun axborotni kodlash hamda shifrlash muhim sohasini takomillashtirish maqsadga muvofiq bo’lib hisoblanadi.

ADABIYOTLAR RO’YXATI:

1. Ganiev Salim Karimovich, G‘ulomov Sherzod Rajaboevich “Axborot nazariyasi va kodlash”, O‘quv qo‘llanma, prof. S.K. Ganiev tahriri ostida, Toshkent-2017.

2. Думачев В.Н. Теория информации и кодирования-Воронеж: Воронежский институт МВД России, 2012.

3. http//elib.buxdu.uz/index.php/pages/referatlar-mustaqil-ish-kursishi/item/14225-axborot-xavfsizligi-tushunchasi-va-axborotni-himoyalashmuammolari-axborot-kommunikatsion-tizimlar-va-tarmoqlarda-taxdidlarva-zaifliklar.

4. Richard E. Algebraic Codes for Data Transmission. Blahut Paperback. ISBN13:9780521556590 Subject: Communications and Signal processing. Publication date January 2012.

5. http//library.tuit.uz/lectures/infbozopas/Axb_naz_kod.pdf

6. https//uz.wikipedia.org/wiki/Kodlash

7. https//uz.atomiyme.com/kodlash-bu-belgisi-tizimlari-axborot-kodlashtirish

8. Теория информации: учеб. / В.А. Фурсов. - Самара: Изд-во Самар, гос. аэрокосм, ун-та, 2011.

9. https//uz.wikipedia.org/wiki/Shifrlash

10.https//hozir.org/malumotlarni-kodlash-va-shifrlash.html

11. www.aim.uz axborot portali