AXBOROTLARNI KRIPTOGRAFIK HIMOYALASH USULLARI

Alibekov Sayfulla Abdug‘aniyevich

Toshkent davlat agrar universiteti dotsenti, f.-m.f.n.

Bugungi kunda axborot texnologiyalari sohasi rivojlanishi natijasida uning turli yo‘nalishlari paydo bo‘lmoqda. Jumladan, axborot xavfsizligi shulardan biri hisoblanadi. Aynan axborot xavfsizligi bizning hayotimizda muhim rol o‘ynaydi desak, adashmagan bo‘lamiz. Chunki, texnalogiyalar asrida yasharkanmiz bizning barcha shaxsiy ma’lumotlarimizni o‘z holicha saqlash uchun axborot xavfsizligi zarur hisoblanadi. Axborot xavfsizligining bir qancha rivojlanib borayotgan bo‘limlari bo‘lib, bulardan kriptografiya bo‘limiga alohida to‘xtalib o‘tishimiz o‘rinlidir.

“Kriptografiya” atamasi dastlab “yashirish, yozuvni berkitib qo‘ymoq” ma’nosini bildirgan. Birinchi marta u yozuv paydo bo‘lgan davrlardayoq aytib o‘tilgan. Hozirgi vaqtda kriptografiya deganda har qanday shakldagi, ya’ni diskda saqlanadigan sonlar ko‘rinishida yoki hisoblash tarmoqlarida uzatiladigan xabarlar ko‘rinishidagi axborotni yashirish tushuniladi. Kriptografiyani raqamlar bilan kodlanishi mumkin bo‘lgan har qanday axborotga nisbatan qo‘llash mumkin. Maxfiylikni ta’minlashga qaratilgan kriptografiya kengroq qo‘llanilish doirasiga ega. Aniqroq aytganda, kriptografiyada qo‘llaniladigan usullarning o‘zi axborotni ximoyalash bilan bog‘liq bo‘lgan ko‘p jarayonlarda ishlatilishi mumkin. Kriptografiya axborotni ruxsatsiz kirishdan himoyalab, uning maxfiyligini ta’minlaydi. Masalan, to‘lov varaqlarini elektron pochta orqali uzatishda uning o‘zgartirilishi yoki soxta yozuvlarning qo‘shilishi mumkin. Bunday hollarda axborotning yaxlitligini ta’minlash zaruriyati paydo bo‘ladi. Umuman olganda kompyuter tarmog‘iga ruxsatsiz kirishning mutlaqo oldini olish mumkin emas, lekin ularni aniqlash mumkin. Axborotning yaxlitligini tekshirishning bunday jarayoni, ko‘p hollarda, axborotning haqiqiyligini ta’minlash deyiladi. Kriptografiyada qo‘llaniladigan usullar ko‘p bo‘lmagan o‘zgartirishlar bilan axborotlarning haqiqiyligini ta’minlashi mumkin.Nafaqat axborotning kompyuter tarmog‘idan

ma’nosi buzilmasdan kelganligini bilish, balki uning muallifdan kelganligiga ishonch hosil qilish juda muxim. Axborotni uzatuvchi shaxslarning haqiqiyligini tasdiqlovchi turli usullar ma’lum. Eng universal protsedura parollar bilan almashuvdir, lekin bu juda samarali bo‘lmagan protsedura. Chunki parolni qo‘lga kiritgan har qanday shaxs axborotdan foydalanishi mumkin bo‘ladi. Agar ehtiyotkorlik choralariga rioya qilinsa, u holda parollarning samaradorligini oshirish va ularni kriptografik usullar bilan himoyalash mumkin, lekin kriptografiya bundan kuchliroq parolni uzluksiz o‘zgartirish imkonini beradigan protseduralarni ham ta’minlaydi.

Kriptologiya ikki yo‘nalish, ya’ni kriptografiya va kriptotaxlildan iborat. Kriptografiyaning vazifasi xabarlarning maxfiyligini va haqiqiyligini ta’minlashdan iborat. Kriptotahlilning vazifasi esa kriptograflar tomonidan ishlab chiqilgan himoya tizimini ochishdan iborat.

Ochiq kalitli asimmetriyali tizimda ikkita kalit qo‘llaniladi. Biridan ikkinchisini xisoblash usullari bilan aniqlab bo‘lmaydi. Birinchi kalit axborot jo‘natuvchi tomonidan shifrlashda ishlatilsa, ikkinchisi axborotni qabul qiluvchi tomonidan axborotni tiklashda qo‘llaniladi va u sir saqlanishi lozim. Ushbu usul bilan axborotning maxfiyligini ta’minlash mumkin. Agar birinchi kalit sirli bo‘lsa, u holda uni elektron imzo sifatida qo‘llash mumkin va bu usul bilan axborotni autentifikatsiyalash, ya’ni axborotning yaxlitligini ta’minlash imkoni paydo bo‘ladi.

Kriptografiya - ma’lumotlarni o‘zgartirish usullarining to‘plami bo‘lib, ma’lumotlarni himoyalash bo‘yicha quyidagi ikkita asosiy muammolarni hal qilishga yo‘naltirilgan: maxfiylik; yaxlitlilik. Maxfiylik orqali yovuz niyatli shaxslardan axborotni yashirish tushunilsa, yaxlitlilik esa yovuz niyatli shaxslar tomonidan axborotni o‘zgartira olmaslik haqida dalolat beradi. Bu yerda kalit qandaydir ximoyalangan kanal orqali jo‘natiladi. Umuman olganda, ushbu mexanizm simmetriyali bir kalitlik tizimiga taalluqlidir. Assimmetriyali ikki kalitlik kriptografiya tizimida himoyalangan kanal bo‘yicha ochiq kalit jo‘natilib, maxfiy kalit jo‘natilmaydi. Yovuz niyatli shaxslar o‘z maqsadlariga erisha olmasa va kriptotaxlilchilar kalitni bilmasdan turib, shifrlangan axborotni tiklay olmasa, u

holda kriptotizim kriptomustahkam tizim deb aytiladi. Kriptotizimning mustahkamligi uning kaliti bilan aniqlanadi va bu kriptotaxlilning asosiy qoidalaridan biri bo‘lib xisoblanadi. Ushbu ta’rifning asosiy ma’nosi shundan iboratki, kriptotizim barchalarga ma’lum tizim hisoblanib, uning o‘zgartirilishi ko‘p vaqt va mablag‘ talab qiladi, shu bois ham faqatgina kalitni o‘zgartirib turish bilan axborotni ximoyalash talab qilinadi. Simmetriyali kriptotizim asoslari Kriptografiya nuqtai-nazaridan shifr – kalit demakdir va ochiq ma’lumotlar to‘plamini yopiq (shifrlangan) ma’lumotlarga o‘zgartirish kriptografiya o‘zgartirishlar algoritmlari majmuasi hisoblanadi. Kalit – kriptografiya o‘zgartirishlar algoritmining ba’zi bir parametrlarining maxfiy holati bo‘lib, barcha algoritmlardan yagona variantini tanlaydi.

Sehrli kvadrat axborotni himoyalash usulida, katakchalarga 1 dan boshlab sonlar yozilgan, undagi har bir ustun, satr va diagonal bo‘yicha sonlar yig‘indisi bitta songa teng bo‘lgan kvadrat shaklidagi jadvalga aytiladi. Sehrli kvadratga sonlar tartibi bo‘yicha belgilar kiritiladi va bu belgilar satrlar bo‘yicha o‘qilganda matn hosil bo‘ladi.

Misol. 4x4 o‘lchovli sehrli kvadratni olamiz, bu yerda sonlarning 880 ta har xil kombinatsiyasi mavjud. Quyidagicha ish yuritamiz: 16 3 2 13 5 10 11 8 9 6 7 12 4 15 14 1. Boshlang‘ich matn sifatida quyidagi matnni olamiz: DASTURLASH TILLARI va jadvalga joylashtiramiz: i s a l u t i a sh r l l t r a d. Shifrlangan matn jadval elementlarini satrlar bo‘yicha o‘qish natijasida tashkil topadi: ISAL UTIA SHRLL TRAD.

Almashtirish usullari sifatida quyidagi usullarni keltirish mumkin:

- Sezar usuli;
- Affin tizimidagi Sezar usuli;
- Tayanch so‘zli Sezar usuli va boshqalar.

Sezar usulida almashtiruvchi harflar k ta siljish bilan aniqlanadi. Yuliy Sezar bevosita k=3 bo‘lganda ushbu usuldan foydalangan. k=3 bo‘lganda va alifbodagi harflar m=26 ta bo‘lganda quyidagi jadval hosil qilinadi.

Misol: Matn sifatida SAMARQAND so‘zini oladigan bo‘lsak, Sezar usuli natijasida quyidagi shifrlangan yozuv hosil bo‘ladi: VDPDUTDQG.

Sezar usulining kamchiligi bu bir xil harflarning, o‘z navbatida, bir xil harflarga almashishidir.

Foydalanilgan adabiyotlar

1. Abduganievich, A. S., & Marsilovna, S. R. (2022, February). Features of the professional activity of a computer science teacher in the modern conditions of the organization of the educational process. In Conference Zone (pp. 195-198).

2. Abdukadirov, A., Zakirov, S., Mamarajabov, O., & Sayfulla, A. (2021). Conditions for the development of students' information competence in the aspect of the development of distance learning in the humanities. In International Conference on Information Science and Communications Technologies: Applications, Trends and Opportunities, ICISCT 2021.

3. I.U. Nazarov, & S.A. Alibekov. (2022). Using modular technologies in creating electronic course. World Bulletin of Social Sciences, 8, 81-84. Retrieved from https://scholarexpress.net/index.php/wbss/article/view/727

4. S. A.Alibekov, L. K. Bagbekova. Masofaviy ta’lim tizimi – o‘qitishning zamonaviy usuli sifatida. Fizika, matematika va informatika ilmiy-uslubiy jurnal 2023. 200-b.

5. Алибеков, С., & Багбекова, Л. (2022). The role of independent education in the educational system. Современные тенденции инновационного развития науки и образования в глобальном мире, 1(3), 35-37.

6. Bagbekova Laylo Kadirbergenovna, Khusanbayev Elmurod Ubaydulla ugli Methodology for organizing the process of distance education and its teaching. (2023). E Conference World, 2, 160-164. https://econferenceworld.org/index.php/ecw/article/view/42

7. Laylo, B., & Javakhir, N. (2023, November). Place of self-education in the education system. In E Conference World (No. 2, pp. 138-142).

8. Kadirbergenovna, B. L. (2023, November). Distance education system as a modern method of training. In E Conference World (No. 2, pp. 97-102).

9. Kadirbergenovna, B. L. (2023, November). Methodology for organizing the process of distance education and its teaching. In E Conference World (No. 2, pp. 160-164).

ЗАМОНАВИЙ ШАРОИТДА МАКТАБ ДИРЕКТОРИНИНГ БОШҚАРУВ ФАОЛИЯТИНИ ЎРГАНИШНИНГ НАЗАРИЙ АСОСЛАРИ

Бектурдиев Қадирбай Бекбусинович

А.Авлоний номидаги Миллий тадқиқот институти мустақил тадқиқотчиси

Барча педагогик тизимларда изчил ўзгаришларни амалга ошириш таълим муассасаларини бошқаришда янги шахсий ва касбий фазилатларни, билим ва кўникмаларни эгаллашни тақозо этади. Таълим жараёнини бошқариш эса бошқарув илми, инновация ва самарали усуллардан фойдаланиш тамойиллари асосида қурилиши зарур.

Фалсафада фаолият инсоннинг дунёга муносабатининг ўзига хос усули - объектив фаолият сифатида қаралади. Социологияда фаолият деганда ижтимоий воқеликнинг мавжуд бўлиш ва ривожланиш йўли, ижтимоий фаолликнинг намоён бўлиши, теварак-атрофдаги дунёни мақсадли акс эттириш ва ўзгартириш тушунилади. Психологик-педагогик тадқиқотларда фаолият категорияси субъектнинг моддий ва мўнавий маданиятнинг муайян объектив маҳсулотини ишлаб чиқариш ва яратишга қаратилган фаолияти сифатида тақдим этилади.

А.Н.Леонтиев, Б.Ф.Ломов, А.В.Петровский, С.Л.Рубинштейнлар директорнинг бошқарув фаолиятини асослаш ва тадқиқ қилишнинг назарий шарти асосида фаолиятни психологик таҳлил қилишни ишлаб чиққанлар.

Маълумки, ҳар қандай фаолият мақсад мотивлари ва мотивларига асосланган бир қатор ҳаракатлардан иборат. С.Л.Рубинштейннинг фикрича