SHIFRLASH HAQIDA UMUMIY TUSHUNCHA.

Meyliqulova Mahbuba Musulmonovna

Qarshi Muhandislik-Iqtisodiyot Instituti akademik litseyi

Informatika fani o'qituvchisi

Annotatsiya. Shifrlash - bu avtorizatsiya qilingan foydalanuvchilarga unga kirish huquqini taqdim etishda ruxsatsiz shaxslardan yashirish uchun ma'lumotni qayta o'zgartirish. Asosan, shifrlash uzatilayotgan ma'lumotlarning maxfiyligini ta'minlashga xizmat qiladi.

Kalit so'zlar. Maxfiylik, axborot xavfsizligi, transformatsiya, algoritm, ma'lumot, avtorizatsiya, Shifrlash.

Har qanday shifrlash algoritmining muhim xususiyati bu algoritm uchun mumkin bo'lgan to'plamdan ma'lum bir transformatsiyani tanlashni tasdiqlaydigan kalitdan foydalanish hisoblanadi. Agar foydalanuvchilarda haqiqiy kalit bo'lsa, ular avtorizatsiya qilinadi. Butun murakkablik va aslida shifrlash vazifasi bu jarayon qanday amalga oshirilganligidadir. Umuman olganda, shifrlash ikkita tarkibiy qismdan iborat - shifrlash va parolni ochish. Shifrlash axborot xavfsizligining uchta holatini ta'minlaydi Maxfiylik Shifrlash ma'lumot uzatish yoki saqlash paytida ruxsatsiz foydalanuvchilardan ma'lumotlarni yashirish uchun ishlatiladi. Butunlik Shifrlash ma'lumot uzatish yoki saqlash paytida o'zgartirilishining oldini olish uchun ishlatiladi. Aniqlik. Shifrlash ma'lumot manbaini autentifikatsiya qilish va ma'lumotni yuboruvchiga unga ma'lumot yuborilganligini rad qilishining oldini olish uchun ishlatiladi. Shifrlangan ma'lumotni o'qish uchun qabul qiluvchi tomonga kalit va dekolifator kerak (shifrlash algoritmini amalga oshiradigan qurilma). Shifrlash g'oyasi shundan iboratki, buzg'unchi shifrlangan ma'lumotlarni ushlagan va ular uchun kalitga ega bo'lmagan holda uzatilgan ma'lumotni o'qiy olmaydi va o'zgartira olmaydi. Bundan tashqari, zamonaviy kriptotizimlarda (ochiq kalit bilan) ma'lumotlarni shifrlash, shifrlash uchun turli xil kalitlardan foydalanish mumkin. Biroq, kriptovalyutaning rivojlanishi bilan siz yopiq matnni kalitsiz shifrlash

imkonini beradigan texnikalar paydo bo'ldi. Ular uzatilgan ma'lumotlarning matematik tahliliga asoslangan. SHifrlash dasturlari fayllar xavfsizligini ta’minlashda yoki qattiq disklarda shifrlangan ma’lumotlar xajmini yaratishda ishlatiladi. Bu ma’lumotlarni rasshifrovka qilish uchun, odatda, parolni kiritish yoki shaxsiy kalitlarni ishlatish talab etiladi. Barcha axborotlarni shifrlangan fayllarda yoki arxivlarda saqlanishi kerakli fayllar to’plamini arxiv uchun nusxalashni yengillashtiradi, chunki ular endi ma’lum joyda joylashgan bo’ladi. Shifrlashning standart usullari (Milliy yoki xalqaro) shifrlarni yechishga mustaxkamlik darajasini oshirish uchun shifrlashni bir nechta etaplar (qadamlar) amalga oshiradi, bularning har birida tanlangan kalitga (yoki kalitlarga) qarab shifrlashni turli klassik usullari ishlatiladi. Shifrlashning prinsipial har xil ikkita standart usullari mavjud: shifrlash va shifrlarni yechishda (simmetrik shifrlash yoki ochiq kalitli tizimlar –• Private – key sistems) bir xil kalitlarni ishlatib shifrlash. Shifrlash uchun ochiq kalitlarni va yopiq kalitlarni shifrlarni yechish uchun• (simmetrik bo‘lmagan shifrlash) foydalanib shifrlash. Shifrlashni standart usullarini qo‘llashda algoritmlarning aniq matematik ifodalash juda qiyin. Foydalanuvchilar uchun birinchi navbatda har xil usullarning ishlatish xususiyatlari muhim (shifrni yechishda mustaxkamlik darajasi, shifrlash va shifrni yechish tezligi, kalitlari tartibi va tarqatish qulayligi). Shifrni yechishda eng yuqori mustaxkamlikni cheksiz uzunlik maskalarni qo‘llaganda ta’minlanadi, bu esa ketmaketliklar tasodifiy generatori bilan hosil bo‘lgan (aniqrog‘i psevdo-tasodifiy). Bunday generator apparatli yoki dasturli vositalari yordamida oson hal qilinadi masalan, bu esa teskari bog‘lamali siljish registr yordamida halaqit qilishga chidamli ikkilik kodni hisoblashda qo‘llaniladi. SHifrlash – akslantirish jarayoni: ochiq matn deb ham nomlanadigan matn shifrmatnga almashtiriladi. Deshifrlash – shifrlashga teskari jarayon. Kalit asosida shifrmatn ochiq matnga akslantiriladi. Ko'pchiligimiz ma'lumotlarni uzatmasdan oldin shifrlash zarurligini tushunamiz. Shifrlash bu oddiy matnni (ya'ni oddiy ma'lumotlar) shifrlangan matnga (ya'ni maxfiy 8 ma'lumotlar) tarjima qilish jarayoni. Shifrlash jarayonida oddiy matnlar kalit va algoritm yordamida shifrlangan

matnga tarjima qilinadi. Ma'lumotni o'qish uchun, kalit va algoritmdan foydalanib, shifrlangan matnni hal qilish kerak (ya'ni oddiy matnga tarjima qilingan). Shifrlash algoritmi - bu kalitning raqamli qiymatlari va oddiy matn qatoridagi belgilarning raqamli qiymatlari uchun qo'llaniladigan matematik operatsiyalar ketma-ketligi. Natijalar shifrlangan matndir. Kalit kattaroq bo'lsa, shifrlangan matn xavfsizroq bo'ladi. Har qanday shifrlash algoritmi bilan hal qilinishi kerak bo'lgan asosiy muammo bu kalitlarni taqsimlashdir. Xavfsiz aloqani o'rnatish uchun kalitlarni ularga kerak bo'lganlarga qanday etkazasiz? Muammoning echimi kalitlar va algoritmlarning xususiyatlariga bog'liq. Shifrlash Qabul qilgich kalit juftligini hosil qiladi va ochiq kalitni yuboruvchiga uzatadi.Yuboruvchi tasodifiy nosimmetrik kalitni yaratadi va undan katta hajmdagi xabarni shifrlash uchun foydalanadi. Yuboruvchi xabarni simmetrik kalit bilan shifrlaydi. Yuboruvchi nosimmetrik kalitni qabul qiluvchining ochiq kaliti bilan shifrlaydi. Yuboruvchi shifrlangan nosimmetrik kalit va shifrlangan xabarni bog'laydi. Yuboruvchi shifrlangan xabarni qabul qiluvchiga uzatadi.

FOYDALANILGAN ADABIYOTLAR RO’YXATI.

1. Akbarov D. Ye. “Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanilishi” – Toshkent, 2008
2. Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Ma’lumotlarni shifrlash algoritmi. O‘z DSt 1105:2009.
3. Ismoilova, M., Maqsudova, G., Sharipova, S., & Yuldasheva, D. (2022). COMPARATIVE TYPOLOGY: TYPES, SUBJECT MATTER, TASKS, APPROACHES AND CLASSIFICATION. *Science and innovation*, *1*(B7), 1544-1546.
4. Boxodirova, F., Isroilova, D., Abduraxmanov, M., & Yuldasheva, D. (2022). DIFFICULTIES IN TEACHING THE GRAMMATICAL FEATURES OF CONJUNCTIONS. *Science and innovation*, *1*(B7), 1421-1422.

5. Artikbayeva, Z. A., & Egamova, G. A. (2022). Boshlang ‘ich sinf ona tili darsliklarida so ‘z birikmasi yuzasidan berilgan bilimlar tahlili. *Science and Education*, *3*(2), 734-739.

6. Sadikov, E. (2022). TIL O ‘QITISHDA PRAGMATIKA MASALALARI: TA’RIFLAR, TANQIDLAR, TAHLILLAR VA TALQINLAR. *ЦЕНТР НАУЧНЫХ ПУБЛИКАЦИЙ (buxdu. uz)*, *24*(24).

7. Ахмедова, Н. А., Нурмухамедова, Н. С., & Алиева, К. К. (2022). Ведение больных бронхиальной астмой в сочетании с ишемической болезнью сердца.

8. Алиева, К. К., Ахмедова, Н. А., & Арипов, Ш. Ш. (2022). *Прогнозирование риска переломов у женщин фертильного возраста с ревматоидным артритом* (Doctoral dissertation, Санкт-Петербург).

9. Ахмедова, Н. А. (2022). The role of genes regulating inflammatory mediators in the etiopathogenesis of chronic pancreatitis.

10. Bozorova, D. B. (2015). SOME NOTES OF VARIABILITY IN THE UZBEK LINGUISTICS. *Theoretical & Applied Science*, (4), 135-138.

11. Ашурбаева, Р. К. (2020). Интеграционый подход в системе образования. In *Colloquium-journal* (No. 12 (64), pp. 61-63). Голопристанський міськрайонний центр зайнятості.

12. Yuldasheva, D., & Ashurbayeva, R. Asadova Sh., Yusupova D. Use of an Integrative Research on the Education System. Scopus: International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-4, November 2019.

13. Ashurbaeva, R. K. The Concept Of Integration And Its Application In Formation Soi: 1.1/Tasdoi: 10.15863. Tas.

14. Ashurbayeva, R. Q. (2022). SHARQDA INTEGRATIV TA’LIMOTNING ILDIZI. *European International Journal of Multidisciplinary Research and Management Studies*, *2*(08), 89-92.