“JOURNAL OF SCIENCE-INNOVATIVE RESEARCH IN UZBEKISTAN” JURNALI
VOLUME 2, ISSUE 10, 2024. OCTOBER
ResearchBib Impact Factor: 9.654/2024 ISSN 2992-8869

SHIFRLASH HAQIDA UMUMIY TUSHUNCHA.

p.f.f.d., dots. **Mingboyev Ulugbek Xujayevich**
Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universitetining Jizzax filiali
m_ulugbek1977@mail.ru

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.

Ma'lumotlarni shifrlash axborot xavfsizligi sohasida qo'llaniladigan usul bo'lib, ma'lumotlarning maxfiyligini himoya qilish uchun ishlatiladi. Ma'lumotlarni shifrlash ma'lumotlarni o'qish yoki tushunishni qiyinlashtirish uchun matematik algoritmlardan foydalangan holda uni turli xil ma'lumotlar sifatida yashirish orqali ma'lumotlarni shifrlaydi. Bu faqat ma'lum bir kalitga ega bo'lganlar tomonidan o'qilishi va tushunilishi mumkin bo'lgan ma'lumotlarni yaratadi. Ma'lumotlarni shifrlash ayniqsa nozik ma'lumotlarni saqlash yoki uzatishda qo'llaniladi. Masalan, kredit karta ma'lumotlari yoki sog'liqni saqlash yozuvlari kabi shaxsiy ma'lumotlarni saqlash yoki uzatishda ma'lumotlarni shifrlashdan foydalanish mumkin. Ma'lumotlarni shifrlash, agar ma'lumotlar buzilgan bo'lsa, undan zararli odamlar tomonidan foydalanilmasligini ta'minlaydi.

Ma'lumotlarni shifrlash ham dasturiy, ham apparat darajasida amalga oshirilishi mumkin. Ma'lumotlarning shifrlanishi ma'lumotlar saqlanadigan yoki uzatiladigan vositaga qarab farq qilishi mumkin. Misol uchun, agar ma'lumotlar bulutga asoslangan saqlash xizmatida saqlansa, ma'lumotlarni shifrlash bulutli provayder tomonidan ta'minlanishi mumkin. Agar ma'lumotlar mahalliy kompyuterda saqlansa, ma'lumotlarni shifrlashdan foydalanish uchun dasturiy ta'minot yoki apparatga asoslangan yechimdan foydalanish mumkin.

Teknik Servis o'z mijozlariga xavfsiz ma'lumotlarni saqlash tizimlari xizmatlarini taqdim etadigan texnologiya kompaniyasidir. Xavfsiz ma'lumotlarni saqlash tizimlari xizmati biznes va jismoniy shaxslar uchun ularning ma'lumotlarining xavfsizligi uchun muhimdir. Texnik xizmat mijozlarga o'z ma'lumotlarini xavfsiz saqlashga yordam berish uchun apparat, dasturiy ta'minot va tajriba bilan ta'minlaydi.

Xavfsiz ma'lumotlarni saqlash tizimlari xizmati mijozlar ma'lumotlarini xavfsiz saqlash va boshqarish uchun zarur texnologiyalarni o'z ichiga oladi. Texnik xizmat o'z mijozlarining ma'lumotlarini shifrlash, zaxiralash va turli joylarda

mijozlar ma'lumotlarini saqlash kabi usullardan foydalangan holda himoya qiladi. Shunday qilib, mijozlar ma'lumotlarini yo'qotish, o'g'irlash yoki noto'g'ri ishlatish kabi xavflar minimallashtiriladi.

Texnik xizmat o'z mijozlariga ma'lumotlarni boshqarish jarayonlarida ham yordam beradi. Ular mijozlar ma'lumotlarini saqlash, zaxiralash va ularga kirish bo'yicha mutaxassislar maslahatlarini taklif qilishadi. Shunday qilib, mijozlar o'z ma'lumotlarini yanada samarali boshqarishlari va ma'lumotlarni boshqarish jarayonlarida samaraliroq bo'lishlari mumkin.

Xavfsiz ma'lumotlarni saqlash tizimlari xizmati mijozlarning turli ehtiyojlariga qarab sozlanishi mumkin. Texnik xizmat o'z mijozlarining biznes ehtiyojlari, ma'lumotlar miqdori va byudjetiga qarab turli xil paketlarni taklif qiladi. Ushbu paketlar mijozlarning turli ehtiyojlariga mos ravishda moslashtirilishi mumkin.

Texnik xizmatning xavfsiz ma'lumotlarni saqlash tizimlari xizmati mijozlar ma'lumotlari xavfsizligini ta'minlash uchun eng yangi texnologiyalardan foydalanadi. Texnik xizmat o'z mijozlari ma'lumotlarini doimiy ravishda kuzatib borish va yangilanishini ta'minlaydi. Shunday qilib, mijozlar ma'lumotlari doimo xavfsiz bo'lib qoladi.

Texnik xizmat mijozlar ma'lumotlarini xavfsiz saqlash va boshqarish uchun zarur apparat, dasturiy ta'minot va tajriba bilan ta'minlaydi. Siz darhol biz bilan bog'lanish orqali ma'lumotlaringizni himoya qilishingiz mumkin.

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. www.ziyouz.com