SIMMETRIK BLOKLI SHIFRLASH ALGORITMLARINING QO'LLASH SOHASI

Muxtoriddinov Muhammadyusuf Temirxon o'g'li
Toshkent axborot texnologiyalari universiteti, 705-21 guruh magistri
E-mail: muhammadyusuf0066@gmail.com

ANNOTATSIYA

Ma'lumotlarni shifrlash algoritmi, O'z DSt 1105:2009 standarti

Kalit so'zlar: blokli shifrlash, axborot xavfsizligi, kriptografiya

OF SYMMETRICAL BLOCK ENCRYPTION ALGORITHMS FIELD OF APPLICATION

ABSTRACT

Data encryption algorithm, Own DSt 1105:2009 standard

Key words: block encryption, information security, cryptography

Hozrigi zamon talabi hamda virtual olamning rivojlanish bosqichida juda ham ko'plab ma'lumotlar almashuv tizimlari ishlab chiqilgan, bunday jarayonlarda esa axborotni xavfsiz, to'liq almashish dolzarb masaladir. Buning uchun turli tizimlar orqali axborotlarni almashish va yetkazishda kriptografik algoritmlardan foydalanish samarali yechim bo'lib kelmoqda. Shuningdek, simmetrik blokli shifrlash algoritimi ko'plab sohalarda keng qo'llanilib kemoqda yani davlat hokimiyati, iqtisodiyot, harbiy, meditsina va boshqa ko'plab sohalarda muhim ma'lumotlarni shifrlangan holatda almashish bunga misol bo'la oladi. Hozirgi kunda bunga misol qilib Davlat hokimiyati barcha tarmoqlari organlarining, barcha shaxs toifalariga yagona standartda ximoyalangan elektron pochtani hamda elektron xujjat aylanishi tizimini

joriy etish mamlakatimizda dolzarb masala hisoblanadi. Bu vazifalarni umumdavlat aloqa va axborotlashtirish sohasining standartlariga asoslangan holda amalga oshiriladi. O‘z DSt 1105:2009 ma’lumotlarni simmetrik blokli shifrlash algoritmi standarti bo‘lib, mamlakatda himoyalangan elektron xujjat aylanishiga xizmat qilib kelmoqda.

Ushbu O‘z DSt 1105:2009 ma’lumotlarni shifrlash algoritmi standarti barcha turdagi electron axborot, ma’lumotlarni himoyalash, muxofazalash maqsadida kriptografik algoritm hisoblanadi. O‘z DSt 1105:2009 simmetrik blokli shifrlash algoritmi bo‘lib, zarur almashuv jarayonida axborotlarni shifrmatnga ya’ni shiflangan holatga o‘tkazadi hamda dastlabki axborotga qayta tiklash uchun ishlatiladi. Ma’lumotlarni shifrlash algoritmi 256 bit o‘lchamdagi axborotni simmetrik blokli shifrmatnga o‘tkazish hamda dastlabki axborotga shifrtmatnni o‘girishda 256 yoki 512 bit uzunlikdagi kriptografik kalit qo‘llaniladi.

Ma’lumotlarni shifrlash algoritmi hozirgi jarayonda dasturiy, apparat yoki appart-dasturiy kriptografik modullarda foydalanib kelinmoqda. Turli tashkilotlar, muassasalar hamda korxonalarda elektron hisoblash mashinalar tarmoqlarida asosan alohida hisoblash komplekslarida hamda elektron hisoblash mashinalarda, serverlarda saqlanuvchi va uzatiluvchi ma’lumotlarning kriptografik himoyasini amalga oshirishda markzur O‘z DSt 1105:2009 simmetrik blokli shifrlash algoritmi standartidan foydalaniladi.

Simmetrik kriptotizimlardan foydalanib turli xil sohalarda xabarlar, ma’lumotlar quyidagicha almashish jarayoni bo‘ladi va u uch bosqichda yuz beradi:

Birinchi bosqich, deylik A PC-1 qurilmadan xabar yuborishda qabul qiluvchi, deylik B PC-2 qurilmaga shifrlash key(kaliti) boshqacha qilib ayganda funksional kalitni, ushbu tarmoq, kanaldan emas biroq muhofazalangan ishonchli kanal tizimidan yuboradi, ma’lum qiladi.

Ikkinchi bosqichda, jo‘natuvchi A PC-1 shifrlash uchun tayyor belgilangan kaliti va funksional kaliti bilan dastlabki axborot, ma’lumotlar to‘plamini shifrmatnga

aylantiradi hamda ularning belgilangan manzil tomon ya'ni B PC-2 qurilmaga himoyalanmagan aloqa kanallaridan yo'naltiradi.

Uchinchi bosqichda, qabul qiluvchi B PC-2 shifrmatnlarni olish jarayonida A PC-1 qurilmadagi shifrlangan ma'lumotlarni shiflash kaliti va funksional kalit yordamida belgilangan tartibdagi dastlabi matnga qaytaradi hamda ikki tomon bu kalitlardan bir necha marta foydalanishi mumkin bo'ladi.

Ma'lumotlarni shifrlash algoritmini tushuntirish uchun axborotni shifrmatnga o'tkazish hamda o'girilgan shifrmatnni qayta dastlabki axborotga o'tkazish jarayonlarida qo'llaniladigan zarur matematik obektlarni bayon etish quyidagicha ta'riflanadi. Ma'lumotlarni shifrlash algoritmida modul arifmetikasining diamatritsalar algebrasidan foydalaniladi, bunda, hisoblashning qiyinlik darajasi matritsalar algebrasidagi singari bajariladi.

Shifrmatnga o'girish va dastlabki matnga o'girish protseduralarida foydalaniladigan diamatritsalar algebrasining asosiy amali diamatritsaning belgilangan mudul bo'yicha diamatritsaga teskarilash amali hisoblanadi. Bu amallarda ikki o'lchamli seans kaliti massivning maxsus tuzulmali 4x4 tartibli kvadrat diamatritsa bilan aks ettiriluvchi qismlari ishtirok etadi, maxsus tuzilmali diamatritsa uchun barcha diognal elementlar bir xilligi, 1-satrdagi nodiagnal elementlar, shuningdek 2-satrning boshi va oxiridagi elementlar, shunungdek 2-satrning boshi va oxiridagi elementlar ham birxilligi xosdir. 4x4 tartibli maxsus tuzilmali diamatritsa bayt darajasida 10 ta element asosida shakllanadi. Ya'ni deylik quyidagicha d_0, d_1, d_2, d_3, d_4, d_5, d_6, d_7, d_8, d_9, elementlar asosida shaklangan diamatritsa hosil qilinadi matematik ifodasida.

FOYDALANILGAN ADABIYOTLAR RO'YXATI: (REFERENCES)

1. Kuryazov D.M., Sattarov A.B., Axmedov B.B. Blokli simmetrik shifrlash algoritmlari bardoshliligini zamonaviy kriptotahlil usullari bilan baholash. O'quv qo'llanma. Toshkent. 2017

2. O'z DSt 1105:2009 Axborot texnologiyasi. Axborotning kripto-grafik muhofazasi. Atamalar va ta'riflar.