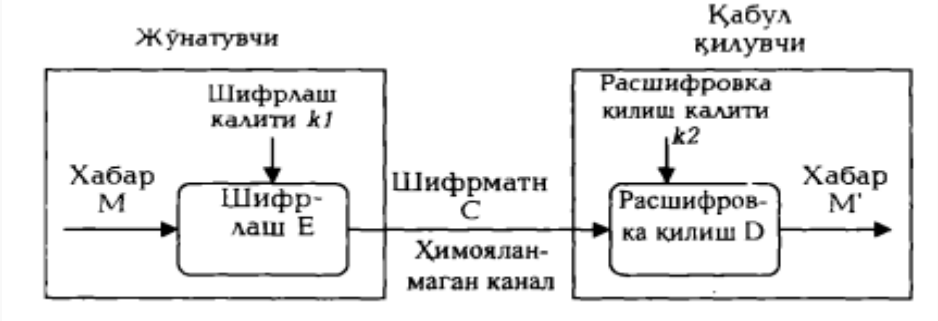
AXBOROTNI XIMOYALASHNING ASOSIY TUSHUNCHALARI

Jo’rayev Sirojbek O’rol o’g’li
Chilonzor tumani 1-son kasb-hunar maktabi Informatika va AT fani katta o’qituvchisi
Mirvaliyeva Komola Abdusattarovna
Chilonzor tumani 1-son kasb-hunar maktabi Informatika va AT fani katta o’qituvchisi
Ismatova Munisa Lutfullaqizi
Chilonzor tumani 1-son kasb-hunar maktabi Informatika va AT fani o’qituvchisi
Mardayev Sayfiddin Mengniyor o’g’li
Chilonzor tumani 1-son kasb-hunar maktabi Informatika va AT fani o’qituvchisi

Annotatsiya: *Ma'lumotlarni bitlar bo'yicha shifrlash va dastlabki matnga o'girish uchun oqimli shifrlarni dasturiy amalga oshirish unchalik qulay emas. Boshqa tomondan oqimli shifrlarni qurilmaviy amalga oshirish ancha oson. Oqimli shifrlar bilan shifrlashda gammalashtirishdan foydalaniladi. Gammaning o'zi esa shifrlash kaliti vazifasini bajaradi. Amalda oqimli shifrlarda shifr matn uzunligi maxfiy kalit uzunligidan bir necha marta uzunroq, kalitlar oqimi qandaydir davrga ega bo'lgan psevdotasodifiy bitlar ketma-ketligidan iborat bo'ladi.*

Kalit so’zlar*: Axborot, Axborot ximoyasi, Oqimli shifrlash, shifr matn, kalit bitlari, oqimli kriptotizimlar sinxron va asinxron.*

Axborotning ximoyalashning aksariyat mexanizmlari asosini shifrlash tashkil etadi. Axborotni shifrlash deganda ochiq axborotni (dastlabki matnni) shifrlangan axborotga o’zgartirish (shifrlash) va aksincha (rasshifrovka qilish) jarayoni tushuniladi. Shifrlash kriptotizimining umumlashtirilgan sxemasi A- rasmda keltirilgan.



A-rasm. Shifrlash kriptotizimining umumlashtirilgan sxemasi.

Uzatiluvchi axborot matni M kriptografik o’zgartirish E_{k1} yordamida shifrlanadi, natijada, shifrmatn C olinadi:

$$C = E_{k1}(M)$$

bu yerda, k1- shifrlash kaliti deb ataluvchi E funktsiyaning parametri. Shif- rlash kaliti yordamida shifrlash natijalarini o’zgartirish mumkin. Shifrlash kaliti muayyan

foydalanuvchiga yoki foydalanuvchilar guruhiga tegishli va ular uchun yagona bo'lishi mumkin. Muayyan kalit yordamida shifrlangan axborot faqat ushbu kalit egasi (yoki egalari) tomonidan rasshifrovka qilinishi mumkin. Axborotni teskari o'zgartirish quyidagi ko'rinishga ega:

$$M = D_{k2}(C)$$

D funktsiyasi E funktsiyaga nisbatan teskari funktsiya bo'lib, shifr matnni rasshifrovka qiladi. Bu funktsiya ham k2 kalit ko'rinishidagi qo'shimcha parametrga ega. k_1 va k_2 kalitlar bir ma'noli moslikka ega bo'lishlari shart. Bu holda rasshifrovka qilingan M axborot M ga ekvivalent bo'ladi. k_2 kaliti ishonchli bo'lmasa D funktsiya yordamida M ' = M dastlabki matnni olib bo'lmaydi. Kriptotizimlarning ikkita sinfi farqlanadi:

- simmetrik kriptotizim (bir kalitli);
- asimmetrik kriptotizim (ikkita kalitli).

Shifrlashning simmetrik kriptotizimida shifrlash va rasshifrovka qilish uchun bitta kalitning o'zi ishlatiladi. Demak, shifrlash kalitidan foydalanish xuquqiga ega bo'lgan har qanday odam axborotni rasshifrovka qilishi mumkin. Shu sababli, simmetrik kriptotizimlar maxfiy kalitli kriptotizimlar deb yuritiladi. Ya'ni shifrlash kalitidan faqat axborot atalgan odamgina foydalana olishi mumkin. Shifrlashning simmetrik kriptotizimi sxemasi B-rasmda keltirilgan.

B-rasm. Simmetrik shifrlash krigttotizimning sxemasi

Elektron xujjatlarni o'lchagichning konfidentsialligini simmetrik kriptotizim yordamida ta'minlash masalasi shifrlash kaliti konfidentsialligini ta'minlashga keltiriladi. Odatda, shifrlash kaliti ma'lumotlar fayli va massividan iborat bo'ladi va shaxsiy kalit eltuvchisida masalan, disketda yoki smart-kartada saqlanadi. Shaxsiy kalit eltuvchisi egasidan boshqa odamlarning foydalanishiga qarshi choralar ko'rilishi shart. Simmetrik shifrlash axborotni «o'zi uchun», masalan, egasi yo'qligida undan ruxsatsiz foydalanishni oldini olish maqsadida, shifrlashda juda qulay xisoblanadi. Bu tanlangan fayllarni arxivli shifrlash va butun bir mantiqiy yoki fizik disklarni shaffof (avtomatik) shifrlash bo'lishi mumkin. Simmetrik shifrlashning noqulayligi - axborot almashinuvi boshlanmasdan oldin barcha manzillar bilan maxfiy kalitlar bilan ayirboshlash zaruriyatidir. Simmetrik kriptotizimda maxfiy kalitni aloqaning umumfoydalanuvchi kanallari orqali uzatish mumkin emas. Maxfiy kalit junatuvchiga va qabul qiluvchiga kalitlar tarqatiluvchi ximoyalangan kanallar orqali uzatilishi kerak.

Xulosa: Demak, shifrlash kalitidan foydalanish huquqiga ega bo’lgan har qanday odam axborotni rasshifrovka qilishi mumkin. Shu sababli, simmetrik kriptotizimlar maxfiy kalitli kriptotizimlar deb yuritiladi. Ya'ni shifrlash kalitidan faqat axborot atalgan odamgina foydalana olishi mumkin.

FOYDALANILGAN ADABIYOTLAR:

1. S. K. G’aniyev , M. M. Karimov, K. A. Tashev AXBOROT XAVFSIZLIGI << ALOQACHI>> -2008 71-73 b.