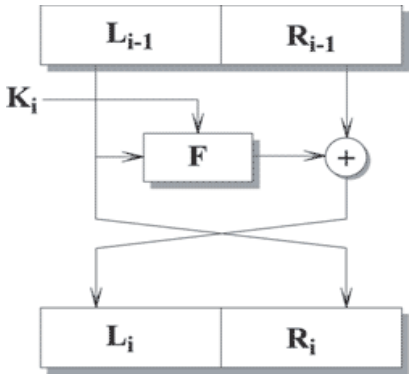
SIMMETRIK VA BLOKLI SHIFRLASH ALGORITMLARIDA FESTAL TARMOG'I O'RNI

Jumaboyev T.A. G'ayratov Z.K.
Muhammad Al-Xorazmiy nomidagi TATU
Samarqand filiali o'qutuvchisi
Meyliyev D. Nazarova M.Z
Muhammad Al-Xorazmiy nomidagi TATU
Samarqand filiali talabalari

Festal tarmoqlari eng keng tarqalgan, chunki ular nosimmetrik shifrlash algoritmlari uchun barcha talablarga javob beradi, juda sodda va ixchamdir.Festal tarmog'i quyidagi tuzilishga ega. Kirish bloki novdalar deb ataladigan teng uzunlikdagi subbloklarga bo'linadi. Masalan, agar blok 64 bit uzunlikda bo'lsa, har biri 32 bitdan iborat ikkita filial ishlatiladi. Har bir filial boshqasidan mustaqil ravishda qayta ishlanadi, shundan so'ng barcha filiallarning chapga tsiklik siljishi amalga oshiriladi. Bunday konvertatsiya bir necha tsikl yoki turda amalga oshiriladi. Ikki novda bo'lsa, har bir tur rasmda ko'rsatilgan tuzilishga ega:



1-rasm. Festal tarmog'i

Festal tarmog'ining davri

F funktsiyasi generatrix deb ataladi. Har bir tur bitta filial uchun a funktsiyasini hisoblash va boshqa filial bilan A natijasining XOR operatsiyasini bitma-bit bajarishdan iborat. Shundan so'ng, filiallar almashtiriladi. Turlarning optimal soni 8 dan 32 gacha deb ishoniladi. Eng muhimi shundaki, turlar sonini ko'paytirish algoritmning kriptovalyutasini sezilarli darajada oshiradi. Bu xususiyat Feishtel tarmog'ining faol tarqalishiga ta'sir qildi, chunki kriptovalyutaga ko'proq qarshilik

ko'rsatish uchun algoritmni o'zgartirmasdan raundlar sonini ko'paytirish kifoya. Zamonaviy algoritmlarda turlar soni aniqlanmagan, faqat ruxsat etilgan chegaralar ko'rsatilgan.

Festal tarmog'i, agar f funksiyasi bunday bo'lmasa ham, qayta tiklanadi, chunki shifrlash uchun F-1ni hisoblash talab qilinmaydi. Shifrni ochish uchun xuddi shu algoritm ishlatiladi, lekin shifrlangan matn kirishga beriladi va kalitlar teskari tartibda ishlatiladi.

Hozirgi vaqtda feishtel tarmog'ining turli xil turlari to'rt novdali 128 bitli blok uchun tobora ko'proq foydalanilmoqda. Har bir filialning o'lchamidan ko'ra novdalar sonining ko'payishi 32 bitli so'z protsessorlari hali ham eng mashhur bo'lib qolayotgani bilan bog'liq, shuning uchun 32 bitli so'zlarni ishlatish 64 bitli so'zlarga qaraganda samaraliroq.

Festal tarmog'i asosida qurilgan algoritmning asosiy xususiyati f funksiyasidir. turli xil variantlar boshlang'ich va yakuniy o'zgarishlarga ham tegishli. Oqartirish (oqlash) deb nomlangan shunga o'xshash transformatsiyalar kirish matnining dastlabki randomizatsiyasini amalga oshirish uchun amalga oshiriladi.

Ko'pgina blok algoritmlari Feishtel tarmog'idan foydalanishga asoslangan bo'lib, ularning barchasi tekis kalit maydoniga ega, bir nechta zaif kalitlarni istisno qilish mumkin.

Adabiyotlar ro’yxati:

1. Xasanov X.P. “Takomillashgan diamatritsalar algebralari va parametrli algebra asosida kriptotizimlar yaratish usullari va algoritmlari”, Toshkent, 2008y.
2. Akbarov D.Ye. “Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanilishi”, Toshkent, 2009y.
3. B. Shnayer «Prikladnaya kriptografiya»
4. V. Mao «Sovremennaya kriptografiya: teoriya i praktika», Izdatelskiy dom «Vilyams», 2005g.