BLOKLI SHIFRLASH ALGORITMLARIDA FEYSTEL TARMOG‘ININGQO’LLANILISHI.

Xolbo’tayeva Laziza Gulmurat qizi
O’zMU magistranti

Annotatsiya: Ushbu ilmiy tadqiqot ishida simmetrik blokli shifrlash algoritmlari uchun feystel tarmog’I va takomillashgan feystel tarmoq’lari ko’rib o’tildi. Feystel tarmog’ining i-raundi uchun matematik model va feystel tarmog’idagi qo’llaniluvchi parametrlar keltirilgan.

Kalit so’zlar: kriptografik algoritm, shifrlash, round akslantirish, bir tomonlama funksiya, feystel tarmog’i.

Аннотация: В данной исследовательской работе были рассмотрены сеть Фейстеля и улучшенные сети Фейстеля для алгоритмов симметричного блочного шифрования. Представлена математическая модель i-го раунда сети Фейстеля и параметры, используемые в сети Фейстеля.

Ключевые слова: криптографический алгоритм, шифрование, круглое зеркалирование, односторонняя функция, сеть Фейстеля.

Annotation: In this research work, the Feistel network and improved Feistel networks for symmetric block encryption algorithms were considered. The mathematical model for the i-round of the Feistel network and the parameters used in the Feistel network are presented.

Keywords: cryptographic algorithm, encryption, round of describe, one way function, Feistel cipher.

Аннотация: В данной исследовательской работе были рассмотрены сеть Фейстеля и улучшенные сети Фейстеля для алгоритмов симметричного блочного шифрования. Представлена математическая модель i-го раунда сети Фейстеля и параметры, используемые в сети Фейстеля.

Ключевые слова: криптографический алгоритм, шифрование, круглое зеркалирование, односторонняя функция, сеть Фейстеля.

Ma’lumotlarni himoyalash maqsadida IBM kompaniyasi, Stanford va MIT universitetlari hamkorligida 1970 yillarda kriptografiya sohasida ilmiy izlanishlar olib bordi. Ushbu loyiha IBM ilmiy tekshirish markazida DSc.Horst Feystel (Dr.Horst Feistel) rahbarligida olib borilgan ilmiy tadqiqot natijasida simmetrik blokli shifrlash algoritmlari uchun matematik model, algoritmning arxitekturasi taklif qilindi va Feystel tamog’i deb nomlandi.

Ushbu feystel tarmog’i asosida bir qancha simmetrik blokli shifrlash algorimlari yaratildi. Xususan FEAL, LOCI, Khufu, Khafre Blowfish, Lucifer, CAST, shuningdek, DES, GOST 28147-89 kabi standart shifrlash algoritmlarni keltirish mumkin**.**

Feystel tarmog'i quyidagicha ifodalanadi. Dastlab ochiq matn tanlanadi va algoritm qabul qilgan uzunlikdagi bloklarga ajratadi.

$$M = \{m_1, m_2, \cdots, m_p\} \quad (1)$$

bu yerda: $M - Ochiq\ matn,\ m_j\ (j = \overline{1..p}) - Ochiq\ matn\ blogi,\ p - Ochiq\ matn\ bloklar\ soni$

Har bir m_j blok alohida shifrlanadi va shifrlanadigan blok uchun K kalitdan foydalaniladi.

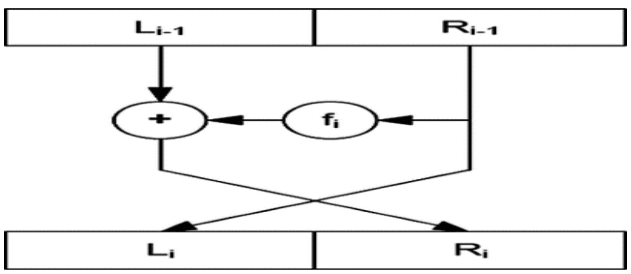
Shifrlash jarayoni bir nechta raundlaridan iborat bo’lib, raundlar soni (n, $n \in N$) algoritm bardoshliligidan kelib chiqib belgilanadi.

Dastlab shifrlanadigan blok m_j ikkita, chap L_0 va o’ng R_0 qismlarga ajratiladi.

$$m_j = \{L_0, R_0\} \quad (2)$$

Ushbu qismlar birinchi raund uchun kiruvchi element hisoblanadi.

Har bir blok uchun quyidagi shifrlash amalga oshiriladi.



1-rasm. Feystel tarmog‘i i raundi arxitekturasi

Bu yerda :

n – raundlarning umumiy soni

$i = \{1,2 \cdots n\}, i \in N$

L_i*- Ochiq matnning chap qismi*

R_i*- Ochiq matnning o’ng qismi*

$K -$ *Shifrlash uchun berilgan dastlabki kalit.*

k_i*- Dastlabki K kalitdan algoritmda ko'rsatilgan qoida bilan hosil qilinadigan raund kalitlari.*

$K = \{k_1, k_2, \dots, k_n\}$ (3)

$F = f(R_{i-1}, k_i)$*- Akslantirish funksiyasi*

Feystel tarmog’ida shifrlash (4) va shifrni ochish (5) jarayonlarinin matematik modeli quyidagicha bo’ladi.

$$\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus F(R_{i-1}, k_i) \end{cases} \quad (4)$$

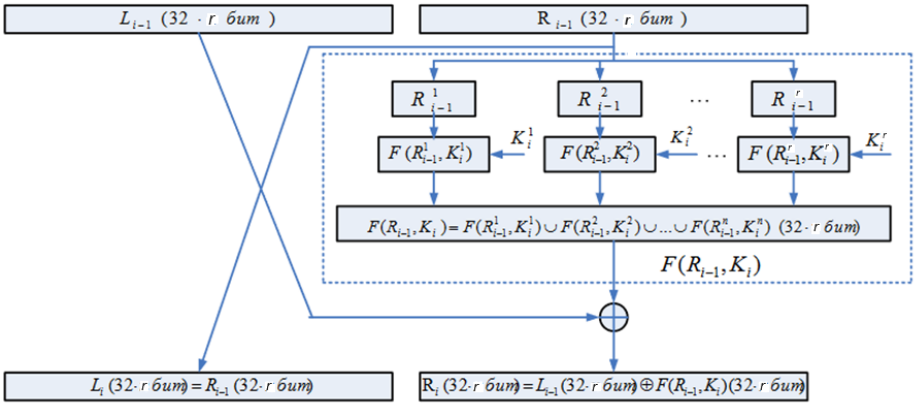
bunda $i -$ *raunddagi shifrma'lumot –* $i + 1$ *raund uchun kiruvchi ma'lumot hisoblanadi.*

Barcha raundlarlar bajarilish natijasida shifrmalumot hosil bo’ladi.

$$\begin{cases} R_{i-1} = L_i \\ L_{i-1} = R_i \oplus F(L_i, k_i) \end{cases} \quad (5)$$

bunda shifrni ochish jarayonida $i + 1 -$ *raunddagi shifrma'lumot* $i-$ *raund uchun kiruvchi va kalitlar teskari tartibda qo’llaniladi.*

Katta hajmdagi malumotlarda umumiy feystal tarmog’ida algoritm qabul qilgan uzunlikdagi bloklarga ajratib shifrlash ko’p vaht talab etadi. Mana shunday masalani yechish uchun Feystel tarmog'i quyidagicha takomillashtiriladi:



2-rasm. *Takomillashgan Feystel tarmog'i –i raundi*.

Bu yerda:

- Shifrlanishi kerak bo'lgan ochiq ma'lumot bloklari uzunligi 64 r bitga teng.

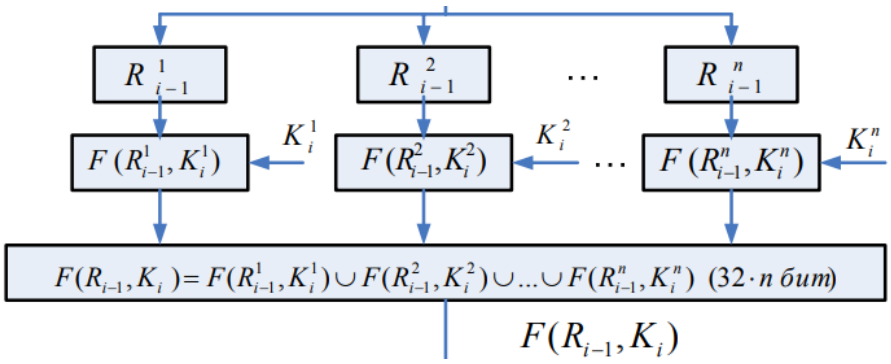
$$r \in N$$

- Kalit uzunligi $|K| \cdot r$ bitga teng.
- $K_i = K_i^1 K_i^2 \ldots K_i^r -$ i-raund qism kalitlari birlashmasi.
- $i = \{1,2 \cdots n\}, i \in N$
- Feystel tarmog'i R – o'ng va L– chap qismlari uzunliklari:

$|L| = |R| = 32 \cdot r$ bitga teng.

- $L_{i-1}(32 \cdot r\ bit)$ - i -raund chap qismi.
- $R_{i-1}(32 \cdot r\ bit)$ - i -raund o'ng qismi.
- $R_{i-1}^1(32\ bit), R_{i-1}^2(32\ bit),\ldots, R_{i-1}^r(32\ bit)$ - i -raund o'ng qismning 32 bitlik bo'laklari.
- $F\left(R_{i-1}^1, K_i^2\right), F\left(R_{i-1}^2, K_i^2\right),\cdots, F(R_{i-1}^r, K_i^r) - i$ -raund Feystel funktsiyasining mos akslantirishlari.

1.3-rasmdagi sxemaga ko'ra dastlab ochiq matn (M) 64 ga karrali qilib olinadi$(64 \cdot r\ bit)$. So'ngra chap ($L_{i-1}(32 \cdot r\ bit)$) va o'ng ($R_{i-1}(32 \cdot r\ bit)$) qismga bo'linadi. O'ng qism va raund kaliti $F(R_{i-1}, K_i)$ funksiyaga kiradi.



3-rasm Takomillashgan feystal tarmog'idagi funksiya sxemasi

- $R^1_{i-1}(32\ bit), R^2_{i-1}(32\ bit), \ldots, R^r_{i-1}(32\ bit)$ - i -raund chap qismning 32 bitlik bo'laklari.
- $K_i = \{K^1_i, K^2_i, \ldots, K^n_i\}$ - i -raund kalitining n ta qismiy bo'laklari.
- $F\left(R^1_{i-1}, K^2_i\right), F\left(R^2_{i-1}, K^2_i\right), \cdots, F(R^r_{i-1}, K^r_i) - i$ -raund Feystel funktsiyasining mos akslantirishlari.
- $F(R_{i-1}, K_i) = F(R^1_{i-1}, K^1_i) \cup F\left(R^2_{i-1}, K^2_i\right) \cup \ldots \cup F(R^r_{i-1}, K^r_i)$ – funksiyaning so'ngi natijasi.

Funksiyadan natija chiqqandan so'ng chap qism($L_{i-1}(32 \cdot r\ bit)$) bilan XOR($\oplus$)lanadi va keying raundga o'tadi.

Takomillashgan Feystel tarmog'i – i raundi matematik modeli quyidagicha ifodalanadi:

$$\begin{cases} L_i(32 \cdot r\ bit) = R_{i-1}(32 \cdot r\ bit) \\ R_i(32 \cdot r\ bit) = L_{i-1}(32 \cdot r\ bit) \oplus F(R_{i-1}, k_i)(32 \cdot r\ bit) \end{cases} \quad (6)$$

Yuqorida takomillashgan va asosiy Feystel tarmog'i sxemasidan ko'rinib turibdiki, takomillashgan Feystel tarmog'ida takomillashtirish parametri r ga bog'liq bo'lgan holda bir nechta $F\left(R^1_{i-1}, K^2_i\right), F\left(R^2_{i-1}, K^2_i\right), \cdots, F(R^r_{i-1}, K^r_i)$ – Feystel funktsiyalari uchraydi. Bu esa r ga bog'liq holda bir necha Feystel tarmog'iga asoslangan algoritmlar funktsiyalaridan yoki bir necha S- bloklardan foydalanish imkonini beradi. Shuningdek, r ga bog'liq ravishda kalit uzunliklari ham ortib boradi, ya'ni $r=1$ da kalit uzunligi 256 bit bo'lsa, $r=2$ da kalit uzunligi 512 va hokazo bo'ladi.

Kalit uzunligi va takomillashtirish parametri r orasida quyidagicha bog'liqlik o'rnatish mumkin.

$$l_1 = l \cdot r \qquad (7)$$

bu yerda $-l$ asosiy algoritm kaliti uzunligi, $-l_1$ takomillashgan algoritm kaliti uzunligi

Yuqorida aytib o'tganimizdek, kalit jadvali shifrni ochish uchun teskari bo'lsa, xuddi shu tuzilma shifrlash va parolni hal qilish uchun ishlatilishi mumkin. Bu shifrlarni tadbiq qilish uchun juda foydali, chunki shifrlashning barcha kaliti shifrni ochish uchun teskari yo'nalishda qayta o'rnatilishi shart emas.

Feistel shifrlarining yana bir muhim afzalligi shundaki, F funksiyaning teskarisi bo'lishi shart emas. Ko'pgina shifrlar shifrlashda amalga oshirilgan ochiq matnning har bir o'zgarishini teskari bo'lishini talab qiladi, shunda shifrlangan malumotni deshifrlash mumkin. Feystel tuzilmasidan foydalanadigan shifrlar uchun bu shart emasligi sababli, u funktsiyalar uchun yangi imkoniyatlarni ochadi**.**

Takomillashgan Feystel tarmog'ida esa takomillashtirish parametri n ga bog'liq holda shifrlash algoritmi xossalari va bardoshliligini saqlab qolgan holda algoritm kaliti uzunligini oshirib borish imkoniyati mavjud. Bu esa, o'z navbatida, hisoblash texnikasi qurilmalarining takomillashuvi natijasida algoritm kaliti uzunligi to'liq tanlash usuliga bardoshsiz bo'lib qolishining oldini oladi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

1. **Akbarov D.E. "Axborot xavfsizligini ta'minlashning kriptografik usullari va ularning qo'llanilishi" Toshkent** . 2008 – 83-84 b.
2. S.K. Ganiyev, A.A. Ganiyev, Z.T. Xudoyqulov "Kiberxavfsizlik Asoslari" Toshkent-2020. 20-21 b.
3. Scarfone K. et al. Guide to storage encryption technologies for end user devices //NIST Special Publication. 2007. 800 b.
4. Konheim, A.G. Horst Feistel: the inventor of LUCIFER, the cryptographic algorithm that changed cryptology. *J Cryptogr Eng*
5. D.Y. Akbarov, P.F Xasanov, X.P Xasanov, O,P Axmedova, I.U.Xolimtayeva "Kriptografiyaning matematik asoslari". O'quv qo'llanma. Toshkent– 2018 . 36 b.