

SIMMETRIK KRIPTOTIZIMLARDA O'RNIGA QO'YISH ALGORITMLARINING QIYOSIY TAHLILI VA AMALIY AHAMIYATI

Abdazimov Saidaminxo'ja Zoirxo'ja o'g'li

*O'zbekiston Respublikasi IIV Akademiyasi Raqamli texnologiyalar va axborot
xavfsizligi kafedrasida o'qituvchisi;*

Djamatov Mustafa Xatamovich

*O'zbekiston Respublikasi IIV Akademiyasi Raqamli texnologiyalar va axborot
xavfsizligi kafedrasida katta o'qituvchisi;*

Annotatsiya: *Shifrlash jarayonida o'rniga qo'yish va o'rin almashtirish akslantirishlarining kombinatsiyalaridan birgalikda foydalanilsa, bunday shifrlash algoritmi kompozitsion shifrlash sinfiga kiradi. Shifrlash algoritmlari, kalitlardan foydalanish turlariga ko'ra, simmetrik va nosimmetrik sinflarga bo'linadi. Agar shifrlash va deshifrlash jarayonlari bir xil kalit bilan amalga oshirilsa, bunday shifrlash algoritmi simmetrik shifrlash algoritmi sinfiga kiradi.*

Kalit so'zlar: *Kompozitsion shifrlash, algoritmi, simmetrik, nosimmetrik, blokli shifrlash, alifboli shifrlash, shifr ma'lumot, ANSI kodi, ASCII kodi.*

Аннотация: *Когда в процессе шифрования используется комбинация замещения и отражения замещения, такой алгоритм шифрования относится к составному классу шифрования. Алгоритмы шифрования делятся на симметричные и асимметричные классы в зависимости от типа используемого ключа. Если процессы шифрования и дешифрования выполняются с одним и тем же ключом, такой алгоритм шифрования относится к классу симметричных алгоритмов шифрования.*

Ключевые слова: *Составное шифрование, алгоритм, симметричное, асимметричное, блочное шифрование, алфавитное шифрование, шифрование информации, код ANSI, код ASCII.*

Annotation: *When a combination of substitution and reflection substitution is used in the encryption process, such an encryption algorithm belongs to a composite encryption class. Encryption algorithms are divided into symmetric and asymmetric classes depending on the type of key used. If the encryption and decryption processes are performed with the same key, such an encryption algorithm belongs to the class of symmetric encryption algorithms.*

Keywords: *Composite encryption, algorithm, symmetric, asymmetric, block encryption, alphabet encryption, encryption information, ANSI code, ASCII code.*

Shifrlashda kalitlardan foydalanish qoidasiga ko'ra shifrlar simmetrik va nosimmetrik sinflarga bo'linishi ta'kidlanib, agar shifrlash va deshifrlash jarayonlari mos ravishda maxfiy ma'lumotni jo'natuvchi va qabul qilib oluvchi tomonidan bitta kalit bilan amalga oshirilsa, bunday algoritmi simmetrik shifrlash sinfiga kirishi

ta'riflangan. Agar shifrlash jarayonida biror akslantirish orqali ochiq ma'lumot alifbosi belgilari shifirma'lumot alifbosi belgilariga almashtirilsa, bunday akslantirishga asoslangan shifrlash algoritmi o'rniga qo'yishga asoslangan shifrlash sinfiga kiradi.

Agar shifrlash jarayonida biror akslantirish orqali ochiq ma'lumot alifbosi belgilarining o'rinlari almashtirilsa, bunday shifrlash algoritmi o'rin almashtirishga asoslangan shifrlash sinfiga kiradi. O'rin almashtirishga asoslangan shifrlash algoritmlarida ochiq ma'lumotni tashkil etuvchi alifbo belgilarining ma'nosi shifirma'lumotda ham o'zgarasdan qoladi. O'rniga qo'yishga asoslangan shifrlash algoritmlarida shifirma'lumotni tashkil etuvchi alifbo belgilari ma'nosi ochiq ma'lumotni tashkil etuvchi alifbo belgilarining ma'nosi bilan bir xil bo'lmaydi.

Shifrlash jarayonida o'rniga qo'yish va o'rin almashtirish akslantirishlarining kombinasiyalaridan birgalikda foydalanilsa, bunday shifrlash algoritmi kompozision shifrlash sinfiga kiradi. Umuman olganda, o'rniga qo'yishga asoslangan shifrlash algoritmlari akslantirishlarining matematik modellari ko'p qiymatli funksiyalar bilan ifodalansada, amalda bir qiymatli (teskarisi mavjud bo'lgan, qaytar) funksiyalar bilan ifodalanuvchi akslantirishlarni qo'llash qulaylik tug'diradi. Umumiy holda, o'rniga qo'yishga asoslangan shifrlash algoritmlari bir qiymatli va ko'p qiymatli shifrlash sinfiga bo'linadi. Bir qiymatli shifrlash algoritmlarida ochiq ma'lumot alifbosi belgilarining har biriga shifirma'lumot alifbosining bitta belgisi mos qo'yiladi. Ko'p qiymatli shifrlash algoritmlarida ochiq ma'lumot alifbosi belgilarining har biriga shifirma'lumot alifbosining ikkita yoki undan ortiq chekli sondagi belgilari mos qo'yiladi, ya'ni ochiq ma'lumot alifbosining biror x_i belgisiga shifirma'lumot alifbosining chekli $\{y_{i1}, y_{i2}, \dots, y_{it}\}$ to'plamdan olingan biror y_{ij} , ($1 \leq j \leq t$) belgisi mos qo'yiladi.

Shifrlash algoritmlari, kalitlardan foydalanish turlariga ko'ra, simmetrik va nosimmetrik sinflarga bo'linadi. Agar shifrlash va deshifrlash jarayonlari bir xil kalit bilan amalga oshirilsa, bunday shifrlash algoritmi simmetrik shifrlash algoritmi sinfiga kiradi. Agar shifrlash jarayoni biror k_1 kalit bilan amalga oshirilib, deshifrlash jarayoni $k_2 \neq k_1$ bo'lgan k_2 kalit bilan amalga oshirilib, k_1 kalitni bilgan holda k_2 kalitni topish yechilishi murakkab bo'lgan masala bilan bog'liq bo'lsa, bunday shifrlash algoritmi nosimmetrik shifrlash algoritmi sinfiga taalluqli bo'ladi.

Shifrlash jarayoni ochiq ma'lumotni ifodalovchi elementar (masalan: bit, yarim bayt, besh bit, bayt) belgilarni shifirma'lumotni ifodalovchi elementar belgilarga akslantirish asosida amalga oshirilsa, bunday shifrlash algoritmi oqimli (uzluksiz) shifrlash sinfiga kiradi.

Shifrlash jarayoni ochiq ma'lumot alifbosi belgilarining ikki va undan ortiq chekli sondagi birikmalarini shifirma'lumot alifbosi belgilarining birikmalariga akslantirishga asoslangan bo'lsa, bunday shifrlash algoritmi blokli shifrlash sinfiga kiradi.

Shifrlash jarayonida ochiq ma'lumot alifbosining biror alohida olingan a_i belgisi har doim shifirma'lumot alifbosining biror fiksirlangan b_j belgisiga almashtirilsa, bunday shifrlash algoritmi bir alifboli shifrlash sinfiga kiradi. Agar shifrlash jarayonining har xil bosqichlarida ochiq ma'lumot alifbosining biror alohida olingan a_i

belgisi shifirma'lumot alifbosining har xil b_j, b_l, \dots, b_t belgilariga almashtirilsa, bunday shifrlash algoritmi ko'p alifboli shifrlash sinfiga kiradi.

Shifrlash jarayonida ochiq ma'lumot alifbosi belgilari yoki alifbo belgilari birikmalari biror amal bajarish bilan shifirma'lumot alifbosi belgilari yoki ularning birikmalariga almashtirilsa, bunday shifrlash algoritmi gammalashtirilgan shifrlash sinfiga kiradi.

Quyida o'rniga qo'yish va o'rin almashtirishga asoslangan shifrlash algoritmlarining turkumlarining matematik asoslari alohida-alohida ko'rib chiqiladi.

Oddiy o'rniga qo'yishga asoslangan shifrlash algoritmlarining jadvali va analitik matematik modellari

Shifrlash algoritmlari ochiq ma'lumot alifbosi belgilarini shifirma'lumot belgilariga akslantirishdan iborat ekanligi yuqorida ta'kidlangan edi. Akslantirishlar funksiyalari (kalit deb ataluvchi noma'lum) parametrغا bog'liq holda: jadval va analitik (formulasi) ifoda ko'rinishlarida berilishi mumkin. O'rniga qo'yishga asoslangan shifrlash algoritmlarining dastlabki namunalari bo'lgan tarixiy shifrlash algoritmlarining deyarli hammasi jadval ko'rinishida ifodalanadi. Ular haqidagi to'liq ma'lumotlar [1] da mavjud. O'rniga qo'yishga asoslangan shifrlash algoritmlarining umumiy xususiyatini hisobga olib, bu sinfdagi algoritmlarni 4.1- jadval ko'rinishida quyidagicha ifodalash mumkin.

4.1- jadval

O'rniga qo'yishga asoslangan shifrlash algoritmlari

Ochiq ma'lumot alifbosi (kirillcha belgilar)	A	B	Ya
Shifirma'lumot alifbosi (ikkilik sanoq tizimi belgilari)	$x_0^0 x_1^0 x_2^0 x_3^0 x_4^0$	$x_0^1 x_1^1 x_2^1 x_3^1 x_4^1$	$x_0^{31} x_1^{31} x_2^{31} x_3^{31} x_4^{31}$

Kirillcha alifbo belgilari soni 32 ta, shu 32 ta har xil belgilarni bitlar bilan ifodalash uchun besh bit kifoya, ya'ni $2^5 = 32$. Keltirilgan 4.1- jadvaldan foydalanib, kirillcha alifboda ifodalangan ochiq malumot belgilarini ularga mos keluvchi ikkilik sanoq tizimidagi besh bitlik belgilarga almashtirib shifirma'lumot hosil qilinadi, ya'ni $x_j^i \in \{0;1\}$. Agarda, keltirilgan jadvalda ochiq ma'lumot alifbosi belgilariga shifirma'lumot alifbosining qanday besh bitlik belgilari mos qo'yilganligi noma'lum bo'lsa, bu jadval kalit bo'lib, shifirma'lumotdan ochiq ma'lumotni tiklash masalasi murakkablashadi. Bunday shifrlash jarayonini ifodalovchi algoritm kalitlarining umumiy soni $32!$ bo'lib, ushbu

$$n! \approx \left(\frac{n}{e}\right)^2 \sqrt{2\pi n}$$

Stirling formulasiga ko'ra quyidagicha $32! = \left(\frac{32}{2.7}\right)^{32} \sqrt{2 \cdot 3.14 \cdot 32} >$

$$\left(\frac{32}{2.7}\right)^{32} \sqrt{2 \cdot 2 \cdot 32} > \left(\frac{32}{2.7}\right)^{32} \sqrt{2 \cdot 2 \cdot 32} = 2^{96} \cdot 2^3 \cdot \sqrt{2} > 2^{99}$$

hisoblanadi. Bunday holat esa kalitni bilmagan holda deshiflash jarayonini amalga oshirishni jiddiy murakkablashtiradi.

Agarda ochiq ma'lumot kompyuterdan foydalanilgan holda tuzilib, standart ASCII kodi alifbosi belgilaridan iborat bo'lib, shifirma'lumot standart ASCII kodi alifbosi belgilarini birini boshqasi bilan almashtirishdan iborat bo'lgan o'rniga qo'yishga asoslangan shifrlash algoritmini qo'llash natijasida hosil qilingan bo'lsa, u holda shifrlash jarayoni asosini quyidagi o'rniga qo'yish almashtirish 4.2- jadvali tashkil etadi.

4.2- jadval

O'rniga qo'yish almashtirish (ASCII kodi alifbosi belgilari asosida) jadvali

Ochiq ma'lumot alifbosi (standart ASCII kodi belgilari)	ASCII	ACII ₁	ASCII ₂₅₅
Shifr ma'lumot alifbosi (ikkilik sanoq tizimi belgilari)	$x_0^0 x_1^0 \dots x_7^0$	$x_0^0 x_1^0 \dots x_7^0$	$x_0^{255} x_1^{255} \dots x_7^{255}$

Bu yerda $x_i^j \in \{0;1\}$ bo'lib, standart ASCII kodi alifbosi 256 ta har xil belgilarini bitlar bilan ifodalash uchun sakkiz bit kifoya, ya'ni $2^8 = 256$.

Bu shifrlash jarayonini ifodalovchi algoritm kalitlarining umumiy soni $256!$ bo'lib, ushbu $n! \approx \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$ – Stirling formulasiga ko'ra quyidagicha

$$256! = \left(\frac{256}{2.7}\right)^{256} \sqrt{2 \cdot 3.14 \cdot 256} > \left(\frac{256}{4}\right)^{256} \sqrt{2 \cdot 2 \cdot 256} > \left(\frac{4 \cdot 2^6}{4}\right)^{256} \sqrt{2 \cdot 2 \cdot 2^8} \\ = 2^{6 \cdot 56} \cdot 2^5 = 2^{1541}$$

hisoblanadi. Bunday holat esa kalitni bilmagan holda deshifrlash jarayonini amalga oshirishni yetarli darajada murakkablashtiradi.

Yuqorida keltirilgan jadvallar o'rniga qo'yishga asoslangan shifrlash algoritmlarining eng oddiy ko'rinishlari modelini ifodalaydi. Ya'ni shifrlash jarayonida shifr qiymatlar deb ataluvchi ochiq ma'lumot alifbosi belgilariga mos keluvchi shifrbelgilar deb ataluvchi shifirma'lumot alifbosi belgilari o'zgarmaydi.

Agarda ochiq ma'lumot kompyuterdan foydalanilgan holda tuzilib, standart ASCII kodi alifbosi belgilarini kengaytirilgan kompyuter standart ANSI kodi alifbosi belgilaridan iborat bo'lib, shifirma'lumot standart ANSI kodi alifbosi belgilarini birini boshqasi bilan almashtirishdan iborat bo'lgan o'rniga qo'yishga asoslangan shifrlash algoritmini qo'llash natijasida hosil qilingan bo'lsa, u holda shifrlash jarayoni asosini quyidagi o'rniga qo'yish almashtirish 4.3- jadvali tashkil etadi.

4.3- jadval

O'rniga qo'yish almashtirish (ANSI kodi alifbosi belgilari asosida) jadvali

Ochiq ma'lumot alifbosi (standart ANSI kodi belgilari)	ANSI ₀	ANSI ₁	ANSI _{2³²-1}
Shifirma'lumot alifbosi (ikkilik sanoq tizimi belgilari)	$x_0^0 x_1^0 \dots x_{31}^0$	$x_0^1 x_1^1 \dots x_{31}^1$	$x_0^{2^{32}-1} x_1^{2^{32}-1} \dots x_{31}^{2^{32}-1}$

Oddiy o'rniga qo'yishga asoslangan shifrlash algoritmlarining analitik (formulali) ifodasini ikkita teng kuchli to'plamlar, ya'ni elementlari soni teng bo'lgan to'plamlar, elementlari ustida o'rnatilgan o'zaro bir qiymatli akslantirishlardan (funktsiyalardan) iborat deb tushunish mumkin. Bunday akslantirishlar har doim teskarisiga ega bo'ladi, ya'ni o'zaro bir qiymatlilik xossasi akslantirishning teskarisi mavjudligining yetarlilik shartini ta'minlaydi. O'zaro bir qiymatli funktsiya odatda chiziqlilik xossasiga ega. Masalan, yuqorida keltirilgan jadvalli oddiy o'rniga qo'yishga asoslangan shifrlash algoritmlarining modellarini mos ravishda ularning ushbu ko'rinishdagi:

$$f(x_i) = kx_i + b \pmod{32}, i = 0, 1, \dots, 31;$$

$f(x_j) = kx_j + b \pmod{256}, j = 0, 1, \dots, 255;$ $f(x_l) = kx_l + b \pmod{2^{32}}, l = 0, 1, \dots, 2^{32} - 1;$ analitik (formulali) ifodalari bilan almashtirish mumkin, bu yerda k va b o'zgarmas sonlar. $f(x_i)$ -funktsiya chiziqsiz bo'lsa, u ko'p qiymatli bo'lib, uning teskarisini har doim ham analitik (formulali) ko'rinishda ifodalash imkoni mavjud bo'lavermay, umumiy ko'rinishda to'plamga tegishlilik ifodasiga ega bo'ladi:

$$f^{-1}(y) = \{x_1, x_2, \dots, x_i\}.$$

Bir qiymatli va ko'p qiymatli o'rniga qo'yishga asoslangan shifrlash algoritmlarining matematik modellari

O'rniga qo'yishga asoslangan shifrlash algoritmlari, ularning asosini tashkil etuvchi akslantirishning bir qiymatli yoki ko'p qiymatligiga ko'ra, bir qiymatli va ko'p qiymatli sinflarga bo'linadi.

Agar o'rniga qo'yishga asoslangan shifrlash algoritmida ochiq ma'lumot alifbosi belgilarining har biriga shifirma'lumot alifbosining bitta belgisi mos qo'yilsa, bunday algoritm bir qiymatli o'rniga qo'yishga asoslangan shifrlash algoritmi sinfiga kiradi. Ochiq ma'lumot alifbosi belgilari x_1, x_2, \dots, x_N deb belgilansa, masalan, lotin alifbosi belgilari uchun $N = 26$, kirill alifbosi belgilari uchun $N = 32$, standart ASCII kodi alifbosi belgilari uchun $N = 256$ va hokazo. Shifirma'lumot alifbosi belgilari y_1, y_2, \dots, y_M deb belgilansa, u holda bir qiymatli o'rniga qo'yishga asoslangan shifrlash algoritmining umumiy holdagi modeli 4.4- jadval ko'rinishda quyidagicha ifodalanadi:

4.4- jadval

O'rniga qo'yishga asoslangan shifrlash algoritmining umumiy modeli

Ochiq ma'lumot alifbosi belgilari	x_1	x_2	x_N
Shifirma'lumot alifbosi belgilari	y_{i_1}	y_{i_2}	y_{i_N}

Bu yerda $y_{ij} \in \{y_1, y_2, \dots, y_M\}$. Bu yerda M soni N sonidan qancha katta bo'lsa, ya'ni shifr belgilar to'plamining quvvati shifr qiymatlar to'plamining quvvatidan qancha katta bo'lsa, kalitlarni ifodalovchi mumkin bo'lgan barcha jadvalar soni shuncha ko'p bo'lib, bunday shifrlash algoritmining kriptobardoshlilik ortadi. Analitik ifodasining umumiy ko'rinishi ushbu chiziqli funksiyadan iborat: $y_{ij} = kx_j + b \pmod{N}$ bo'lib, bu yerda $j = 0, 1, \dots, M - 1; i = 0, 1, \dots, N - 1$.

Misol sifatida quyidagi (2x26)-o'lchamli 4.5- jadvalni keltirish mumkin.

4.5- jadval

(2x26) - o'lchamli jadval

Ochiq ma'lumot alifbosi (lotincha belgilar 26 ta)	A	B	...	Z
Shifirma'lumot alifbosi (kirillcha belgilar 32 ta)	I	L	..	U

Ko'p qiymatli shifrlash algoritmlarida ochiq ma'lumot alifbosi belgilarining har biriga shifirma'lumot alifbosining ikki yoki undan ortiq chekli sondagi belgilari mos qo'yiladi, ya'ni ochiq ma'lumot alifbosining biror x_i belgisiga shifirma'lumot alifbosining chekli $\{y_{i1}, y_{i2}, \dots, y_{it}\} \in \{y_1, y_2, \dots, y_M\}$ to'plamidan olingan biror y_{ij} , $(1 \leq j \leq t)$, belgisi mos qo'yiladi. Ko'p qiymatli o'rniga qo'yishga asoslangan shifrlash algoritmining umumiy holdagi modeli 4.6-jadval ko'rinishida quyidagicha ifodalanadi.

4.6- jadval

Ko'p qiymatli o'rniga qo'yishga asoslangan shifrlash algoritmining umumiy modeli

Ochiq ma'lumot alifbosi belgilari	x_1	x_2	...	x_N
Shifirma'lumot alifbosi belgilari	$\{y_{i1}^1, y_{i1}^2, \dots, y_{i1}^n\} = sh1$	$\{y_{i2}^1, y_{i2}^2, \dots, y_{i2}^n\} = sh2$...	$\{y_{iN}^1, y_{iN}^2, \dots, y_{iN}^n\} = shN$

Bu yerda: $y_{ij} \in \{y_1, y_2, \dots, y_M\}$. 4.6- jadvaldagi sh1, sh2, ..., shN - to'plamlar teng quvvatli bo'lsa, ya'ni elementlari soni teng bo'lsa, algoritm teng qiymatli o'rniga qo'yishga asoslangan shifrlash algoritmi bo'ladi, aks holda har xil qiymatli shifrlash algoritmi bo'ladi.

Agar $\max\{y_1, y_2, \dots, y_M\} + 1 = D$ bo'lsa, bu jadvalning analitik ifodasi:

$y_{ij} = f(x_d) \pmod{D}$ bo'ladi, bu yerda $f(\cdot)$ - iror o'zgaruvchan parametrga bog'liq yoki chiziqsizlik kabi ko'p qiymatlilik xossasiga ega bo'lgan funksiya, $1 \leq j \leq M, 1 \leq i \leq N$.

Misol sifatida quyidagi (2x32)-o'lchamli 4.7- jadvalni keltirish mumkin.

4.7- jadval

(2x32)-o'lchamli jadval

Ochiq ma'lumot alifbosi (kirillcha belgilar)	A	B	Ya
----------------------------------------------	---	---	-----	-----	----

Shifirma'lumot (standart ASCII kodi belgilari)	alifbosi	*, d, n	W, &, s, g	14, !, /, j, a
---------------------------------------------------	----------	---------	------------	-----	-----	----------------

Ko'p qiymatli shifrlash algoritmlarining apparat-texnik va apparat-dasturiy ta'minotlari nisbatan samarasiz bo'lganligi sababli amalda kam qo'llaniladi.

O'rniga qo'yishga asoslangan shifrlash algoritmlari, ularning asosidagi akslantirishni shifrlash jarayonida bosqichma-bosqich o'zgarib turishiga ko'ra bir alifboli va ko'p alifboli shifrlash sinflariga bo'linadi.

FOYDALANILGAN ADABIYOTLAR:

1. Коробейников А.Г., Гатчин Ю.А. Математические основы криптологии. Учебное пособие. Санкт-Петербург-2004.
2. Akbarov D.Y. Axborot xavfsizligini ta'minlashning kriptografik usullari va ularning qo'llanishlari. Toshkent. "O'zbekiston markasi", 2009.
3. Защита информации. Малый тематический выпуск. ТИИЭР, 1988 г, №5.
4. Саломова А. Криптография с открытым ключом. М.,1997.
5. Xasanov P.F., Isaev R.I., Xasanov X.P., Nazarova M.X. Axmedova O.P. Axborotning kriptografik muhofazasi tarixi (Ilmiy kriptografiya davri) // Aloqa dunyosi. – Toshkent, 2005, №2 (5).
6. Saidaminxo'dja Zoirxo'dja o'gli., Abdazimov ijtimoiy tarmoqlarda axborot xurujlarini tarqalish ehtimolligini bashoratlash va ulardan himoyalash usuli va modellari //Central Asian Research Journal for Interdisciplinary Studies (CARJIS). – 2022. – T. 2. – №. 5. – С. 109-115.
7. Мирзаева М. Б., Абдазимов С. З. Использование технологий искусственного интеллекта в сфере высшего образования. – 2022.