MASSIV ELEMENTLARINI UZLUKSIZ ALMASHTIRISHGA ASOSLANGAN UZLUKSIZ SHIFRLASH ALGORITMI

Rahmatullayev Ilhom Raxmatullayevich,
Mavlonov Obid Nizomovich
Muhammad al-Xorazmiy nomidagi Toshkent
axborot texnologiyalari universiteti
Ilhom9001@gmail.com

Annotatsiya: Ushbu ishda massiv elementlarini uzluksiz almashtirishga asoslangan uzluksiz shifrlash algoritmlarining qurilishi va ularning xavfsizligini ta'minlashda psevdotasodifiy sonlar generatoridan foydalanishning ahamiyati ko‘rib chiqilgan. Ishlab chiqilgan algoritm, bir o‘lchovli P-massiv va ikki o‘lchovli S-massivdan iborat bo‘lib, kirish parametrlari sifatida kalit massivi, siqish jadvali va bir baytli psevdotasodifiy hosil qilingan bayt qabul qiladi. Algoritmning asosiy bosqichlari, jumladan boshlang‘ich holatdan P-massivni aralashtirish, kalit massiv yordamida P-massivni qayta ishlash va tasodifiy bloklar generatsiyasi ko‘rsatib o‘tilgan. Taklif etilgan usulning samaradorligi va xavfsizligi, AES standartida foydalanilgan S-jadval sifatidagi ixtiyoriy bardoshli jadvalga asoslanadi. Shuningdek, HMAC algoritmini sanoq rejimida foydalanishga asoslangan psevdotasodifiy sonlar generatorining amalga oshirilishi tavsiflanadi.

Kalit so‘zlar: Uzluksiz shifrlash algoritmi, Massiv elementlari, Psevdotasodifiy sonlar generatori, RC4, ISAAC, P-massiv, S-massiv, HMAC, AES, Kalit massivi, Shifrlash, dekodlash, Xavfsizlik, kriptografiya.

Uzluksiz shifrlash algoritmlarini qurishda massiv elementlari o‘rnini almashtirishga asoslangan psevdotasodifiy sonlar generatoridan foydalanish keng tarqalgan. Masalan, mashhur RC4 va ISAAC uzluksiz shifrlash usullari aynan massiv elementlari o‘rnini almashtirishga asoslangan. Shu boisdan, massiv elementlari o‘rnini almashtirishga asoslangan psevdotasodifiy sonlar generatori ishlab chiqildi.

Ushbu algoritm tizimli-nazariy yondashuv asosida yaratilgan bo‘lib algoritm asosini bir o‘lchovli P-massiv, ikki o‘lchovli S – chiziqsiz massiv tashkil etadi.

Kirish parametrlari:

- K[] - kalit massivi bir o‘lchovli o‘zgaruvchan uzunlikka ega bo‘lib 16 bayt (umumiy holda 128 bit) dan katta;
- P[] – uzunligi 256 ga teng va elementlari bir baytli qiymatlardan iborat bir o‘lchovli massiv;
- S[,] – 16 qator va 16 ustunga ega ikki o‘lchovli massiv ko‘rinishidagi siqish

jadvali bo‘lib elementari yarim baytli qiymatlardan iborat;

- T – bir baytli psevdotasodifiy hosil qilingan bayt.

Algoritm tarkibidagi kriptografik akslantirishlar:

- $(j + P[i] + K[j])\ \%\ 256$ – yig‘indining 256 bo‘yicha qoldig‘ini hisoblash;
- $R = S(P[i] \gg 4, P[i]\&0xF)$ – bir baytli P[i]-qiymatni S-massividan o‘tkazish orqali yarim baytli R-qiymatga keltirish;
- $Swap(P[j], P[i])$– P - massivning j-chi va i-nchi elementlari o‘rnini almashtirish;
- $T \oplus m_n$ - XOR amali orqali bir baytli ochiq ma’lumot va gamma elementlarini qo‘shish.

Algoritm jarayoni bosqichlari: (1-rasm)

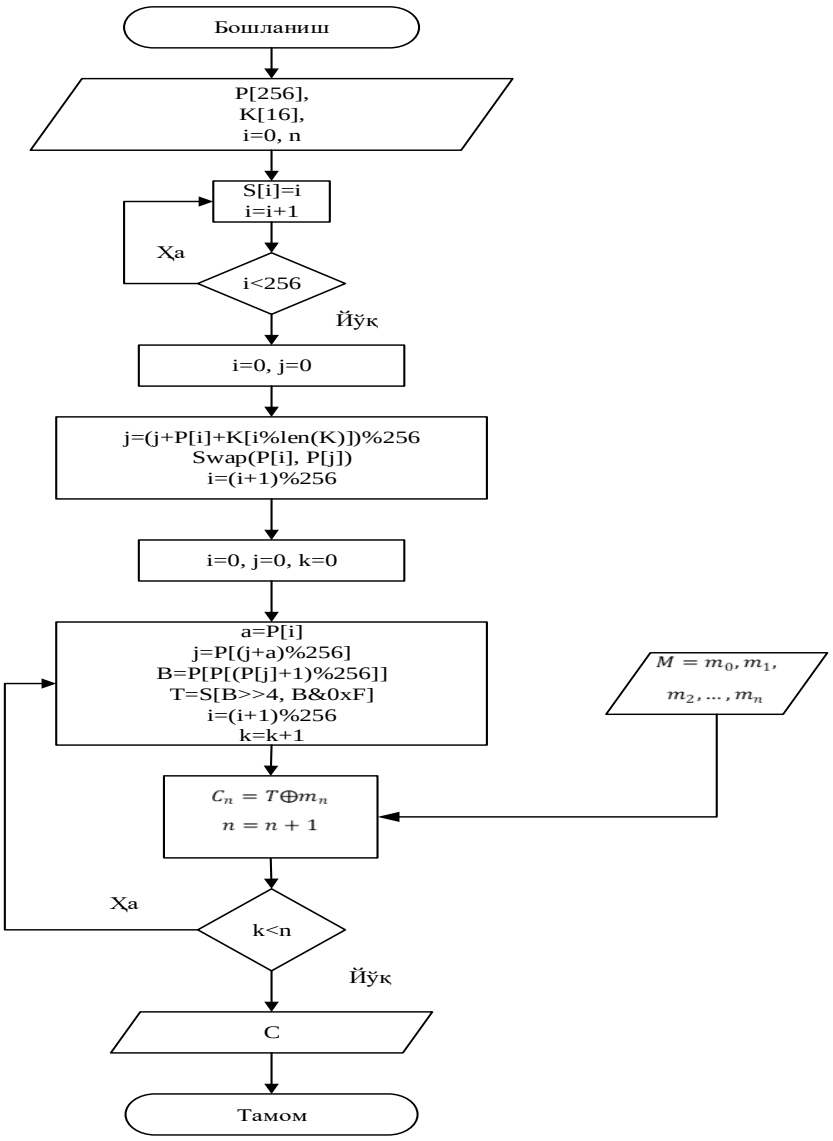
1. Boshlang‘ich holatda P-massiv 0 dan 255 gacha bo‘lgan sonlar bilan ketma-ket chiziqli o‘sish tartibida to‘ldirilib chiqiladi;
2. So‘ng K[] kalit massiv yordamida P-massivni aralashtirish quyidagicha amalga oshiriladi:

$$\text{Dastlabki holatda } i = 0, j = 0$$
$$j = (j + P[i] + K[i\%len(K)])mod256$$
$$Swap(P[i], P[j]) \text{ o‘rni almashtiriladi}$$
$$i = (i + 1)\ mod\ 256$$
$$\text{bunda } i = 0 \text{ dan } 256 \text{ gacha o‘zgaradi.}$$

3. $i = 0$ va $j = 0$ dan talab etilgan baytlar sonicha quyidagi amallar bajariladi:

$$a = P[i]$$
$$j = P[(j + a)\%mod256]$$
$$B = P[P[(P[j] + 1)\%mod256]]$$
$$T = S[B \gg 4, B\&0xF]$$
$$C = T \oplus m_n$$
$$i = i + 1$$

Taklif etilgan psevdotasodifiy sonlar generatorining blok-sxemasining umumiy ko‘rinishi quyidagi 1-rasmda keltirilgan. Ushbu generatorda S jadval juda muhim bo‘lib, hosil bo‘lgan baytlarni chiziqsizligini kafolatlaydi. Shu sababli, S jadval sifati ixtiyoriy bardoshli jadvalni olish mumkin. Mazkur holatda esa AES standartida foydalanilgan S jadvaldan foydalanildi. Ushbu jadval quyida keltirilgan (1-jadval).



1-rasm. Massiv elementlari o‘rnini bog‘liqsiz almashtirishga asoslangan psevdotasodifiy sonlar generatori algoritmining blok sxemasi

1-jadval

AES standartida foydalanilgan S jadval

	Y															
	3	c	7	b	2	b	f	5	0	1	7	b	e	7	b	6
	a	2	9	d	a	9	7	0	d	4	2	f	c	4	2	0
	7	d	3	6	6	f	7	c	4	5	5	1	1	8	1	5
	4	7	3	3	8	6	5	a	7	2	0	2	b	7	2	5
	9	3	c	a	b	2	a	0	2	b	6	3	9	3	f	4

	3	1	0	d	0	c	1	b	a	b	e	9	a	c	8	f
	0	f	a	b	3	d	3	5	5	9	2	f	0	c	f	8
	1	3	0	f	2	d	8	5	c	6	a	1	0	f	3	2
	d	c	3	c	f	7	4	7	4	7	e	d	4	d	8	3
	0	1	f	c	2	a	0	8	6	e	8	4	e	e	b	b
	0	2	a	a	9	6	4	c	2	3	c	2	1	5	4	9
	7	8	7	d	d	5	e	9	c	6	4	a	5	a	e	8
	a	8	5	e	c	6	4	6	8	d	4	f	d	d	b	a
	0	e	5	6	8	3	6	e	1	5	7	9	6	1	d	e
	1	8	8	1	9	9	e	4	b	e	7	9	e	5	8	f
	c	1	9	d	f	6	2	8	1	9	d	f	0	4	b	6

MAS algoritmidan sanoq rejimida foydalanishga asoslangan psevdotasodifiy sonlar generatori. MAS algoritmlarini qurishni ko‘plab usullari mavjud bo‘lib, psevdotasodifiy sonlar generatori uchun uning xususiy holi hisoblangan – HMAC (Hashed MAC) algoritmi tanlab olindi. Bu yerda, HMAC algoritmini qurishda ixtiyoriy bardoshli va tezkor bo‘lgan xesh funksiyalardan foydalanish mumkin. HMAC algoritmini sanoq rejimida foydalanishga asoslangan psevdotasodifiy sonlar generatorining umumiy ko‘rinishi quyidagicha (2-rasm). Mazkur holda tanlangan xesh funksiya bardoshli bo‘lganda blokli shifrlashga olingan farazlar HMAC uchun ham o‘rinli bo‘ladi.

Sanoq rejimiga asoslangan uzluksiz shifrlash algoritmini amalga oshirish o‘zida bir qancha jarayonlarni mujassamlashtiradi.

Shifrlash algoritmini dastlabki shakllantirish. Generatorni shakllantirish quyidagi funksiya orqali amalga oshiriladi:

func. HMAC_CTR_CIPHER_Initialization

Chiqish: S algortm holati

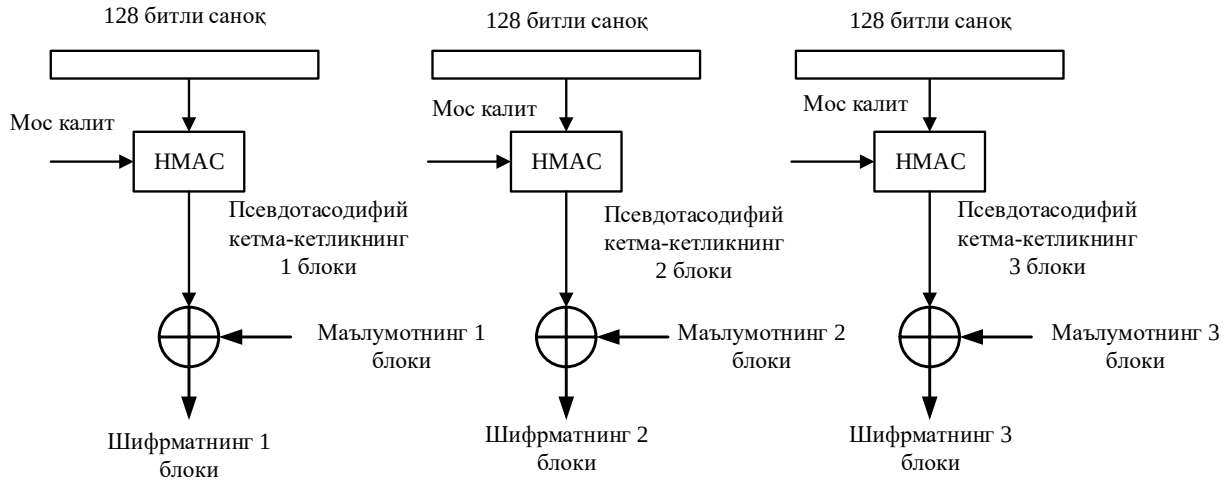
Kalit K, sanoq C ni nolga o‘rnatish

$(K, C) \leftarrow (0,0)$

$S \leftarrow (K, C)$ holatni paketlash

S holatni qaytarish.

Ushbu shakllantirishi bosqichi shifrni yangi ishga tushgan vaqtida amalga oshiriladi va bunda shifr holati nolga o‘rnatiladi. Mazkur holda generator holati $S = (K, C)$ dan iborat deb olingan. Bu yerda K kattalik shifrlash kalitini va C kattalik 128 bitli sanoqni anglatadi.



2-rasm. HMAC algoritmini sanoq rejimida foydalanishga asoslangan uzluksiz shifrlash usulining funksional sxemasi

Algortm holatini qayta qiymatlash. Algoritmni ishga tushirish uchun uni qayta qiymatlash talab etilib, buning uchun turli tasodifiy qiymatlar manbalaridan kalit K uchun haqiqiy tasodifiy qiymatlar talab etiladi. Algoritmni qayta qiymatlash quyidagi funksiya asosida amalga oshiriladi:

func. HMAC_CTR_CIPHER_Reseed

Input: S algoritm holati

Sanoqni birga oshirish

$C \leftarrow C + 1$

Algoritmni qiymatlangan kabi belgilash.

Ushbu operatsiya algoritm ishga tushgan vaqtda sanoqni shakllantirish uchun amalga oshiriladi. Bundan tashqari belgilangan Hash() funksiya sifatida ixtiyoriy bardoshli xesh-funksiyadan foydalanish mumkin.

Shifrlash. Qayta qiymatlangan generator holati orqali tasodifiy ketma – ketliklar blokini generatsiyalash quyidagi funksiya orqali amalga oshiriladi:

func. HMAC_CTR_CIPHER_GenerateBlocks

Kirish: S algoritm holati

M_i - shifrlanishi kerak bo‘lgan ma’lumot bloki (0<=i<k)

k – ma’lumotni HMAC chiqish qiymat uzunligiga bo‘lish natijasi

Chiqish: S - shifrmatn

Agar C!=0 **u holda**

For i=0,…,k-1 **do**

$r \leftarrow r||HMAC(K, C);$

$S \longleftarrow M_i \oplus r$

$C \leftarrow C + 1;$

Enddo

S ni qaytarish

Ushbu bosqichda qayta qiymatlangan algoritm holati va kalit yordamida tasodifiy bloklar generatsiya qilinadi hamla ma’lumotni shifrlash amalga oshiriladi. Buning uchun ushbu funksiyaga talab etiluvchi bloklar soni, algoritmning holati va ma’lumot kiritiladi. Har bir shifrlangan blokdan so‘ng sanoq qiymati birga oshib boradi.

Mazkur taklik etilgan uzluksiz shifrlash algoritmi uchun muhitga qarab xesh funksiyani tanlash mumkin. Masalan, tezkorlik talab qilinuvchi sharoitda MD5, MD4 kabi algoritmlardan va yuqori xavfsizlik darajasini talab qiluvchi sharoitlarda SHA256 kabi algoritmlardan foydalanish mumkin bo‘ladi.

Xulosa

Ushbu maqolada massiv elementlarini uzluksiz almashtirishga asoslangan uzluksiz shifrlash algoritmlarini qurishda psevdotasodifiy sonlar generatoridan foydalanish jarayonini o‘rganadi. Algoritmning asosi bir o‘lchovli P-massiv va ikki o‘lchovli S-massivdan iborat bo'lib, bu yondashuv mashhur RC4 va ISAAC uzluksiz shifrlash usullarida ham qo‘llanilgan.

Maqola, shifrlash jarayonida massiv elementlarining o‘rnini almashtirish mexanizmini va psevdotasodifiy sonlar generatorining qo'llanilishini batafsil bayon qiladi. Bu jarayon, kalit massivi, P-massiv va S-massiv kabi kirish parametrlarini o‘z ichiga oladi. Kriptografik akslantirishlar orqali ma'lumotlarni shifrlash va dekodlash jarayoni amalga oshiriladi.

Shuningdek, maqola HMAC (Hashed MAC) algoritmi asosidagi psevdotasodifiy sonlar generatorining blok-sxemasini va AES standartida foydalanilgan S-jadvalni tahlil qiladi. Bu jadvalning sifati va chiziqsizligi algoritmning samaradorligi uchun muhimdir.

Foydalanilgan adabiyotlar ro‘yxati

1. Rakhmatullaev I. Evaluation of new NSA stream encryption algorithm by integrated cryptanalysis method //Scientific Collection «InterConf». – 2023. – №. 164. – С. 242-248.
2. Raxmatullayebich R. I. STREAM ENCRYPTION ALGORITHMS AND THE BASIS OF THEIR CREATION //Central asian journal of mathematical theory and computer sciences. – 2022. – Т. 3. – №. 12. – С. 165-173.
3. Khudoykulov Z. T., Rakhmatullaev I. R., Umurzakov O. S. H. NSA algoritmining akslantirishlari tanlanishining xavfsizlik talablarini bajarilishidagi o ‘rni //INTERNATIONAL JOURNAL OF THEORETICAL AND APPLIED ISSUES OF DIGITAL TECHNOLOGIES. – 2023. – Т. 6. – №. 4. – С. 97-101.

4. Xudoyqulov Z. T., Rahmatullayev I. R., Boyqo‘ziyev I. M. Bardoshli statik S-bokslarni generatsiyalash algoritmi //INTERNATIONAL JOURNAL OF THEORETICAL AND APPLIED ISSUES OF DIGITAL TECHNOLOGIES. – 2023. – Т. 5. – №. 3. – С. 57-66.
5. Rakhmatullaev I. Self-synchronizing (asynchronous) Stream Encryption Algorithms //Scientific Collection «InterConf». – 2023. – №. 164. – С. 249-254.
6. Zaynalov N. R. et al. Classification and ways of development of text steganography methods //ISJ Theor Appl Sci. – 2019. – Т. 10. – №. 78. – С. 228-232.
7. Boyquziyev I., Saydullayev E., Rahmatullayev I. ELLIPTIK EGRI CHIZIQLARNING KRIPTOGRAFIYADA QO ‘LLANILISHI //DIGITAL TRANSFORMATION AND ARTIFICIAL INTELLIGENCE. – 2024. – Т. 2. – №. 1. – С. 71-76.
8. Rahmatullayev I. R. Algebraik kriptotahlil usuli va uning oqimli shifrlash algoritmlariga qo‘llanish asoslari: Algebraic Cryptanalysis Method and Basics of its Application to Stream Encryption Algorithm //International Journal of Theoretical and Applied Issues of Digital Technologies. – 2023. – Т. 4. – №. 2. – С. 96-102.
9. Xudoykulov Z. T., Rahmatullayev I. R. Yangi oqimli shifrlash algoritmlari va uning kriptotahlili //Milliy standart Ilmiy-texnik jurnali. – 2023. – С. 42-47.
10. Rahmatullayev I. R. Oqimli shifrlash algoritmlari va ularni vujudga kelish sabablari //International Journal of Theoretical and Applied Issues of Digital Technologies. – 2022. – Т. 2. – №. 2. – С. 119-128.
11. Zaynalov N. R. et al. UNICODE For Hiding Information In A Text Document //2020 IEEE 14th International Conference on Application of Information and Communication Technologies (AICT). – IEEE, 2020. – С. 1-5.
12. Rahmatullayev I., Xudoyqulov Z. T. Mavjud oqimli shifrlash algoritmlarining qiyosiy tahlili tahlili //Потомки Аль-Фаргани. – 2024. – Т. 1. – №. 1. – С. 129-134.
13. Kilichev D. et al. Errors in SMS to hide short messages //Artificial Intelligence, Blockchain, Computing and Security Volume 2. – CRC Press, 2024. – С. 735-740.
14. Rahmatullayev I., Umurzakov O. SHA oilasiga mansub xesh funksiyalar tahlili //Потомки Аль-Фаргани. – 2024. – Т. 1. – №. 1. – С. 85-92.
15. Rahmatullayev I. R., Saydullayev E. I., Karimov I. KRIPTOGRAFIYADA ELLIPTIK EGRI CHIZIQLARNING AHAMIYATI //Talqin va tadqiqotlar. – 2024. – №. 28.
16. Rahmatullayev I. et al. OQIMLI SHIFRLASH ALGORITMLARINING LOYIHALASH USULLARI //Talqin va tadqiqotlar. – 2024. – Т. 1. – №. 27.
17. Rakhmatullaevich R. I., Mardanokulovich I. B. Analysis of cryptanalysis methods applied to stream encryption algorithms //Artificial Intelligence, Blockchain, Computing and Security Volume 1. – CRC Press, 2024. – С. 393-401.
18. Rahmatullayev I., Karimov I. DASTURIY SHAKLDA FOYDALANISHGA QULAY OQIMLI SHIFRLASH ALGORTIMINI ISHLAB CHIQISH //Talqin va tadqiqotlar. – 2024. – №. 5 (42).
19. Rahmatullayev I. et al. OQIMLI SHIFRLAR VA ULARNI KRIPTOGRAFIYADAGI O ‘RNI //Interpretation and researches. – 2024. – Т. 2. – №. 3 (25).
20. Rahmatullayev I. OQIMLI SHIFRLASH ALGORITMLARI BARDOSHLILIGINI DIFFERENSIAL VA ALGEBRAIK KRIPTOTAHLIL USULLARI YORDAMIDA BAHOLASH //DIGITAL TRANSFORMATION AND ARTIFICIAL INTELLIGENCE. – 2024. – Т. 2. – №. 1. – С. 64-70.
21. Khudoykulov Z. T., Rakhmatullayev I. R. Development Of A Software Stream Encryption Algorithm //Electronic journal of actual problems of modern science, education and training. – 2023. – Т. 1. – С. 51-59.
22. Raxmatullayevich R. I. OQIMLI SHIFRLASH ALGORITMLARI TAHLILI //Новости образования: исследование в XXI веке. – 2023. – Т. 1. – №. 6. – С. 889-893.