OQIMLI SHIFRLASH UCHUN DASTURIY YECHIMLAR

Rahmatullayev Ilhom Raxmatullayevich[1], Boyquziyev Ilhom Mardonqulovich[2], Omonov Alisher Axmad o‘g‘li[3]

[1]Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Samarqand filiali Ilhom9001@mail.com
[2]Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti.
[3]Sharof Rashidov nomidagi Samarqand davlat universiteti alisher41077@gmail.com

K E Y W O R D S

Oqimli shifrlash algoritmlari, RC4, VMPC, SPRITZ, ISAAC, NIST, Psevdo-tasodifiy raqamlar generatori (PRNG), SSL/TLS, WEP protokoli, Salsa20, ChaCha,Shifrlash tezligi, Statistik testlar, Kriptografiya, Kalit massiv, Almashtirish jadvali (S-box).

A B S T R A C T

Ushbu ishda, dasturiy amalga oshirish uchun qulay bo‘lgan va baytlar massivini aralashtirish tamoyiliga asoslangan yangi oqimli shifrlash algoritmi taklif etildi. Taklif qilingan algoritmning tasodifiylik darajasini baholash maqsadida NIST (Milliy Standartlar va Texnologiyalar Instituti) tomonidan ishlab chiqilgan statistik testlar qo‘llanildi va natijalar olingan hamda tahlil qilindi. Natijalar asosida algoritmning tasodifiy raqamlar generatsiya qilishdagi sifat ko‘rsatkichlari aniqlangan. Shuningdek, generatsiya qilish tezligi bo‘yicha olingan parametrlar boshqa mavjud usullar bilan solishtirilib, algoritmning samaradorligi va ishlash tezligi haqida xulosalar chiqarildi.

Kirish

Oqimli, baytga yo‘naltirilgan 1987-yilda R. Rivest tomonidan ishlab chiqilgan RC4 shifri oqimli va baytga yo‘naltirilgan shifr sifatida kriptografiya sohasida muhim o‘rin egalladi. Dastlab, ushbu algoritm tijorat siri sifatida maxfiy saqlangan edi. Biroq, oradan yetti yil o‘tgach, algoritm anonim ravishda tarqatilib, Internetda ommaga e'lon qilindi [1].

Bu voqeadan so‘ng, RC4 shifri kriptografik hamjamiyat tomonidan intensiv tarzda o‘rganila boshlandi va ko‘plab amaliy dasturlarda keng qo‘llanila boshlandi. Masalan, SSL/TLS protokollari, WEP simsiz tarmoqlar xavfsizligi, Oracle ma’lumotlar bazasi tizimlari va boshqa ko‘plab sohalarda RC4 shifri qo‘llanildi[2].

RC4 muallifining asosiy g'oyasi juda aniq va oddiy bo‘lib, shifrning har bir elementi osongina tushuntirilishi va tushunilishi mumkin edi. Uning sodda dizayni va dasturiy hamda apparat ta’minotida samarali amalga oshirilishi tufayli shifr tez orada keng ommalashdi.

Shu sababli, RC4 hanuzgacha eng mashhur oqimli shifrlardan biri hisoblanadi va kriptografiya sohasida muhim ahamiyatga ega bo‘lib kelmoqda.

Algoritmning afzalliklari quyidagilardan iborat:

1. Ichki holatning katta hajmi: Algoritmning birinchi va asosiy afzalliklaridan biri uning ichki holatining yetarlicha katta hajmga ega ekanligidir. Bu ichki holat 8-bitli almashtirish jadvali S va ikkita 8-bitli hisoblagich Q1 va Q2 dan iborat bo‘lib, umumiy hajmi 8 x 256 + 16 bitni tashkil etadi. Katta ichki holat shifrning xavfsizligini oshiradi, chunki bu tajovuzkorlar uchun barcha mumkin bo‘lgan holatlarni tekshirishni deyarli imkonsiz qiladi[3].

2. Tezkor funktsiyalar orqali ichki holatni yangilash va chiqish qiymatini olish: Algoritm ichki holatni yangilash va chiqish qiymatlarini hosil qilish uchun juda samarali va tez ishlaydigan funktsiyalardan foydalanadi. Bu shifrning yuqori tezlikda ishlashini ta’minlaydi, shuningdek, real vaqt rejimida qo‘llanilishini imkonini beradi. Tezkor funktsiyalar hisob-kitoblarni soddalashtiradi va resurslarni tejaydi, bu esa dasturiy ta’minot va apparat tizimlarida muhim ahamiyatga ega.

3. Keng qamrovli foydalanish chegarasi: Algoritm nafaqat $n = 8$ bit uzunligi uchun emas, balki har qanday $n > 2$ bit uzunligi uchun ham samarali ishlaydi. Bu uning moslashuvchanligini

© Rahmatullayev I.R., Boyquziyev I.M., Omonov A.A.

oshiradi va turli xil ilovalarda, turli xavfsizlik darajalarida qo‘llash imkonini beradi. Shuning uchun, algoritmni turli bit uzunliklarida ishlaydigan tizimlarda osongina integratsiya qilish mumkin.

4. Kalit uzunligining moslashuvchanligi: Algoritmda foydalaniladigan kalit n-bitli elementlarning ixtiyoriy sonidan tashkil topishi mumkin va uning uzunligi 2^n gacha bo‘lishi mumkin. Bu shuni anglatadiki, kalit uzunligini xavfsizlik talablariga mos ravishda oshirish yoki kamaytirish mumkin. Kalit uzunligining moslashuvchanligi shifrni turli xavfsizlik darajalarida qo‘llash imkonini beradi va tajovuzkorlar uchun kalitni taxmin qilishni qiyinlashtiradi.

5. Almashtirish jadvalini yaratish uchun universal va o‘zini o‘zi ta’minlaydigan algoritm: Shifr almashtirish jadvalini yaratishda qo‘shimcha tashqi resurslarga muhtoj emas. U universal va o‘zini o‘zi ta’minlaydigan algoritmdan foydalanadi, bu esa shifrning soddaligini va mustaqilligini oshiradi. Bu yondashuv shifrning implementatsiyasini osonlashtiradi va uning turli platformalarda ishlashini ta’minlaydi.

6. Shifr holatining dinamik o‘zgarishi: Kriptoalgoritm ishlashi davomida shifrning ichki holati doimiy ravishda o‘zgarib boradi. Aynan 2^n qadamdan so‘ng almashtirish jadvali to‘liq o‘zgarishi kafolatlanadi. Bu shifrning dinamikligini va xavfsizligini oshiradi, chunki u tajovuzkorlar uchun statistik tahlil va bashorat qilishni qiyinlashtiradi. Shifr holatining muntazam o‘zgarishi ma’lumotlarning yaxlitligi va maxfiyligini ta’minlashga yordam beradi[5].

Ushbu afzalliklar algoritmning yuqori samaradorlikka ega ekanligini, keng ko‘lamda qo‘llanilishi va yuqori xavfsizlik darajasini ta’minlashini ko‘rsatadi. Algoritmning moslashuvchanligi va samaradorligi uni turli kriptografik ilovalarda muvaffaqiyatli qo‘llash imkonini beradi.

Kriptografiya sohasining rivojlanish tarixi shuni ko‘rsatadiki, vaqt o‘tishi bilan yangi turdagi hujum usullari paydo bo‘lishi va yangi zaifliklarning aniqlanishi sababli, dastlab xavfsiz deb hisoblangan kriptoalgoritmlar ham zaiflashishi mumkin. Bu holat kriptoalgoritmlarni muntazam ravishda yangilab borish va ularning xavfsizligini ta’minlash uchun doimiy ravishda tahlil qilish zaruratini keltirib chiqaradi.

Masalan, RC4 algoritmi ham vaqt o‘tishi bilan zaifliklari aniqlangan va amalga oshirish jarayonida muvaffaqiyatsizliklarga duch kelgan. Xususan, WEP (Wired Equivalent Privacy) protokolida RC4 algoritmini qo‘llash natijasida xavfsizlik muammolari paydo bo‘lgan [6]. Bu protokolning xavfsizligi tajovuzkorlar tomonidan osongina buzilishi mumkinligi sababli, simsiz tarmoqlar uchun ishonchsiz deb topilgan.

Bundan tashqari, vaqt o‘tishi bilan RC4 algoritmining statistik zaifliklari aniqlangan. Ushbu zaifliklar nafaqat S-box (almashtirish jadvali) ni yaratish algoritmida, balki psevdo-tasodifiy raqamlar (PRN) generatori funksiyasida ham mavjud ekanligi isbotlangan. Bu esa shifrlangan ma’lumotlarning xavfsizligini jiddiy ravishda pasaytiradi, chunki tajovuzkorlar ushbu zaifliklardan foydalanib, shifrni buzishlari yoki ma’lumotlarni o‘qishlari mumkin.

Shu sababli, kriptografiyada yangi va xavfsizroq algoritmlarni ishlab chiqish, mavjud algoritmlarni tahlil qilish va ularning zaifliklarini bartaraf etish muhim ahamiyat kasb etadi. Kriptografiya sohasida ilmiy izlanishlar va tadqiqotlar davom etmoqda, chunki ma’lumotlarning maxfiyligi va yaxlitligini ta’minlash zamonaviy axborot texnologiyalari uchun juda muhimdir.

Kriptografik tadqiqotlar va tahlillar natijasida RC4 algoritmining bir qator zaif tomonlari aniqlangan, ular quyidagicha tavsiflanadi [7]:

1. S-box ni ishga tushirish algoritmining zaifligi: S-box (almashtirish jadvali) ni ishga tushirish uchun ishlatiladigan algoritm ba’zi hollarda tajovuzkorga shifrning ichki holatidan foydalangan holda kalitni tiklash imkonini beradi. Bu shifrning xavfsizligini jiddiy ravishda pasaytiradi, chunki kalitni tiklash orqali tajovuzkor shifrlangan ma’lumotlarga to‘liq kirish imkoniyatiga ega bo‘ladi.

2. S-box boshlang'ich qiymatlarining kalitga bog'liqligi: S-box almashtirish jadvalidagi boshlang'ich qiymatlar kalitga kuchli bog'liq

(cc) BY © Rahmatullayev I.R., Boyquziyev I.M., Omonov A.A.

bo‘lib, bu bog'liqlik tajovuzkorlar tomonidan tahlil qilinishi va kalit haqidagi ma’lumotlarni oshkor qilish uchun ishlatilishi mumkin. Bu esa shifrning buzilishiga olib kelishi ehtimolini oshiradi.

3. Kalitlarning to‘qnashuvi (kolliziyasi): RC4 algoritmida turli kalitlar shifrni bir xil ichki holatga o‘tkazishi mumkin, ya’ni kalitlarning to‘qnashuvi sodir bo‘ladi. Bu holat kalitlarning noyobligini pasaytiradi va shifrning umumiy xavfsizligiga salbiy ta’sir ko‘rsatadi, chunki tajovuzkorlar bir xil shifr oqimini qayta tiklash uchun turli kalitlardan foydalanishlari mumkin.

4. Psevdo-tasodifiy chiqish ketma-ketligi orqali shifr holatini aniqlash: Ba’zi hollarda, shifrning chiqishidagi psevdo-tasodifiy ketma-ketliklarni tahlil qilish orqali shifrning joriy ichki holatini aniqlash mumkin. Bu tajovuzkorlarga shifrni teskari muhandislik qilish va shifrlangan ma’lumotlarni ochish imkonini beradi.

5. PRNG chiqishidagi birinchi baytlarning tasodifiy emasligi: Psevdo-tasodifiy sonlar generatori (PRNG) chiqishidan olingan kalit oqimining birinchi baytlari har doim ham to‘liq tasodifiy bo‘lmaydi. Bu holat tajovuzkorlarga ushbu baytlardan foydalanib, ishlatilayotgan kalit haqida taxminlar qilish imkonini beradi. Natijada, uzoq muddatli kalitni ushbu kalit yordamida shifrlangan katta hajmdagi xabarlarni tahlil qilish orqali aniqlash mumkin bo‘ladi[8].

Ushbu aniqlangan zaifliklarga qaramay, RC4 algoritmi hanuzgacha ayrim tizimlarda qo‘llanilmoqda. Biroq, aniqlangan zaifliklarga bo‘lgan e'tibor oshgani sari, kriptografiya sohasida RC4 ning o‘rnini bosadigan yangi, yanada ishonchli va chidamli muqobil algoritmlar izlanmoqda va ishlab chiqilmoqda. Bu yangi algoritmlar RC4 da aniqlangan kamchiliklarni bartaraf etish va yuqori xavfsizlik darajasini ta’minlashga qaratilgan. Shuningdek, ular zamonaviy xavfsizlik talablariga mos keladigan kuchliroq kriptografik mexanizmlarni taklif etadi, bu esa ma’lumotlarning maxfiyligi va yaxlitligini yanada ishonchli tarzda ta’minlashga xizmat qiladi[9].

Asosiy qism.

Bugungi kunga kelib, RC4 algoritmining bir qator takomillashtirilgan variantlari, jumladan RC4A, RC4+, VMPC va SPRITZ taklif qilingan. Ushbu algoritmlarning barchasi dastlab maxfiy kalit yordamida almashtirish jadvali (S-box) ni hosil qilish orqali ishga tushadi. Bu jarayon shifrning xavfsizligi va samaradorligi uchun muhim ahamiyatga ega.

RC4 algoritmida almashtirish jadvali (S-box) ni yaratish:

RC4 algoritmi S-box ni initsializatsiya qilish va kalit bilan aralashtirish jarayonlaridan foydalanadi.

1. Initsializatsiya:
S-box *S[0]* dan *S[255]* gacha bo‘lgan 256 ta elementdan iborat.

Dastlab S-box quyidagicha to‘ldiriladi:

S[i]=I bu yerda *i=0,1,2,…,255*

Kalit massivini tayyorlash: agar kalit uzunligi kalit_uzunligi bo‘lsa, K[] massiviga kalit baytlari joylashtiriladi.

2. Kalit bilan aralashtirish:

$$J = 0$$

$$For\ i = 0\ to\ 255\ do$$

$$J = (J + S[i] + K\ [i \bmod kalit_uzunligi] \bmod 256\ ]$$

S[i] va S[J] ni almashtirish:

$$swap(S[i],S[J])$$

Ushbu jarayon natijasida kalitga bog'liq bo‘lgan almashtirish jadvali hosil qilinadi, bu jadval keyinchalik psevdo-tasodifiy raqamlar generatori sifatida ishlatiladi.

RC4A algoritmi:

RC4A algoritmi RC4 ning zaifliklarini kamaytirish maqsadida Samarjit L. Paul va Bart Preneel tomonidan taklif qilingan. RC4A ikki xil S-box dan foydalanadi va oqim hosil qilish jarayonini quyidagicha o‘zgartiradi:

1. Initsializatsiya:

Ikkita S-box: S1 va S2, har biri 256 ta elementdan iborat, RC4 dagi usul bilan initsializatsiya qilinadi.

(cc) BY © Rahmatullayev I.R., Boyquziyev I.M., Omonov A.A.

2. Oqim hosil qilish:

Har bir qadamda ikkita chiqish bayti hosil qilinadi, bu jarayon S1 va S2 ga asoslanadi va aralashtirish jarayonini yaxshilaydi.

RC4+ algoritmi:

RC4+ algoritmi sekulyar almashtirish va XOR operatsiyalarini qo‘shish orqali RC4 ni yaxshilaydi.

1. Initsializatsiya:
RC4 dagi kabi S-box ni yaratadi.
2. Oqim hosil qilish:

Qo‘shimcha aralashtirish funksiyalari va XOR operatsiyalari bilan psevdo-tasodifiy oqimni hosil qiladi, bu esa statistik zaifliklarni kamaytiradi.

VMPC (Variably Modified Permutation Composition):

VMPC algoritmi RC4 ning ichki tuzilishini o‘zgartirish orqali uning zaifliklarini bartaraf etishga harakat qiladi.

1. Initsializatsiya:
P[0] dan P[255] gacha bo‘lgan almashtirish jadvali yaratiladi.
Dastlab $P[i] = i$.
2. Kalit bilan aralashtirish:

$$N = 256$$
$$For\ m = 0\ to\ 767\ do$$
$$J = (J + P[m \bmod N] + K[m \bmod kalit_uzunligi]) \bmod N\ ]$$
$$P[m \bmod N]\ va\ P[J]\ ni\ almashtirish$$

3. Oqim hosil qilish:
VMPC funksiyasi orqali psevdo-tasodifiy oqim yaratiladi:

$$Q = P[(P[(P[J] + 1) \bmod N])]\ ]$$

Chiqish bayti: Q

SPRITZ algoritmi:

SPRITZ RC4 ning muallifi Ronald Rivest va Jacob Schuldt tomonidan taklif qilingan va RC4 ning butun tuzilishini qayta ko‘rib chiqadi.

1. Initsializatsiya:

$$N = 256$$
$$S[0...N-1] = 0...N-1$$
$$I, J, K = 0$$

2. Kalitni qabul qilish (Absorb):
Kalit baytlari S-box ga Absorb funktsiyasi orqali kiritiladi.
3. Aralashtirish (Shuffle):

S-box ni yaxshilab aralashtirish uchun Shuffle funksiyasi qo‘llaniladi.

4. Oqim hosil qilish (Drip):

Har bir qadamda ichki holatni yangilash va chiqish baytini hosil qilish amalga oshiriladi:

$$I = I + W \bmod N$$
$$J = K + S[(J + S[I]) \bmod N] \bmod N$$
$$K = I + K + S[J] \bmod N$$
$$S[I]\ va\ S[J]\ ni\ almashtirish$$

Chiqish bayti:

$$Z = S[(J + S[(I + S[(Z + K) \bmod N]) \bmod N]) \bmod N]$$

SPRITZ algoritmi RC4 ga nisbatan xavfsizlikni oshirish uchun mo‘ljallangan bir qator qo‘shimcha funksiyalardan foydalanadi, bu esa uni murakkabroq va bardoshlilik darajasini yuqori qiladi.

RC4 algoritmi va uning takomillashtirilgan variantlarida S-box ni hosil qilish jarayoni shifrning xavfsizligi uchun hal qiluvchi ahamiyatga ega. Har bir variant RC4 ning aniqlangan zaifliklarini bartaraf etish va xavfsizlikni oshirish maqsadida o‘ziga xos initsializatsiya va aralashtirish mexanizmlarini qo‘llaydi. Bu o‘zgarishlar shifrlarning statistik zaifliklarini kamaytirishga va tajovuzkorlar uchun hujumlarni qiyinlashtirishga xizmat qiladi.

Keyin esa mazkur jadval yordamida chiqish baytlari shakllantiriladi hamda shifr holati o‘zgartiriladi. Quyidagi 1-jadvalda RC4 ning yuqorida keltirilgan modifikatsiya variantlarining mazkur jarayonda qanday o‘zgartirishlardan foydalanishi keltirilgan.

1-jadval.

RC4 va uning takomillashtirilgan variantlarining Chiqish baytini shakllantirish va shifr holatini o‘zgartirish jarayoni

© Rahmatullayev I.R., Boyquziyev I.M., Omonov A.A.

ISSN: 3030-3346

Algoritm	Iteratsiya	Chiqish baytini shakllantirish va shifr holatini o‘zgartirish
RC4	*1.i=(i+1)mod 256* *2. j=(j+S[i])mod 256* *3.* ***swap(S[i],S[j]***	*1. t=(S[i]+S[j])mod* *2. Chiqish bayti: K=S[t]*
RC4A	*1.* ***i=(i+1)mod*** *2.* ***j1=(j1+S1[i])mod 256*** *3.* ***swap(S1[i],S1[j1])*** *4.* ***j2=(j2+S2[i])mod 256*** *5.* ***swap(S2[i],S2[j2])***	*1. Chiqish bayti 1:* ***K1=S2[(S1[i]+S1[j1])mod 256*** *2. Chiqish bayti 2:* ***K2=S1[(S2[i]+S2[j2])mod 256]***
RC4+	*1.* ***i=(i+1)mod 256*** *2.* ***a=S[i]*** *3.* ***j=(j+a+C)mod 256*** *4.* ***swap(S[i],S[j])***	*1.* ***b=S[(S[i]+S[j])mod 256]*** *2. Chiqish bayti:* ***K=b⊕a***
VMPC	*1.* ***i=(i+1)mod 256*** *3.* ***j=(j+a)mod 256*** *4.* ***swap(S[i],S[j])***	*1. Chiqish bayti:* ***K=S[S[S[j]]]***
SPRITZ	*1.* ***i=(i+w)mod N*** *2.* ***j=(k+S[(j+S[i])mod N])mod N*** *3.* ***k=(k+i+S[j])mod N*** *4.* ***swap(S[i],S[j])***	***j:=k+S[j+S[i]]*** ***k:=k+i+S[j]***

Yuqorida keltirilgan va boshqa oqimli shifrlash algoritmlarini chuqur tahlil qilish natijasida, tezkorlik, bardoshlilik va psevdotasodifiylik talablariga to‘liq javob beradigan yangi dasturiy oqimli shifrlash algoritmi ishlab chiqildi. Ushbu algoritm zamonaviy kriptografiya talablariga mos ravishda yaratilgan bo‘lib, uning asosiy maqsadi yuqori samaradorlik bilan birga ma’lumotlarning xavfsizligini ta’minlashdir.

Ishlab chiqilgan algoritm tizimli-nazariy yondashuv asosida qurilgan. Bu yondashuv nazariy bilimlarni amaliyot bilan uyg'unlashtirish orqali optimal yechim topishga qaratilgan. Algoritmning asosini elementlari 256 ta baytdan iborat bo‘lgan bir o‘lchamli massiv tashkil etadi. Ushbu massiv shifrning ichki holatini ifodalaydi va u orqali psevdo-tasodifiy raqamlar oqimi generatsiya qilinadi.

256 ta baytdan iborat massivdan foydalanish bir necha afzalliklarni ta’minlaydi:

- Katta ichki holat maydoni: 256 baytli massiv shifrning ichki holatini 2048 bitgacha kengaytiradi, bu esa tajovuzkorlar uchun barcha mumkin bo‘lgan holatlarni tekshirishni amalda imkonsiz qiladi.

- Yuqori tezkorlik: Algoritmda ichki holatni yangilash va chiqish qiymatlarini hosil qilish uchun samarali matematik operatsiyalar qo‘llaniladi. Bu shifrning yuqori tezlikda ishlashini ta’minlaydi va real vaqt rejimida qo‘llash imkonini beradi.

- Yaxshi psevdotasodifiylik xususiyatlari: Algoritm tomonidan generatsiya qilinadigan raqamlar ketma-ketligi NIST (Milliy Standartlar va Texnologiyalar Instituti) statistik testlari yordamida sinovdan o‘tkazilgan va tasodifiylik bo‘yicha yuqori natijalarga erishilgan.

Shuningdek, algoritmning parametrlari va generatsiya qilish tezligi boshqa mavjud usullar bilan solishtirilib, uning samaradorligi va xavfsizlik darajasi yuqori ekanligi aniqlangan. Bu esa uni turli kriptografik ilovalarda, jumladan, ma’lumotlarni shifrlash, autentifikatsiya va xavfsiz aloqa kanallarini tashkil etishda muvaffaqiyatli qo‘llash imkonini beradi.

Kirish parametrlari:

k[]: Uzunligi kamida 16 bayt (128 bit) bo‘lgan bir o‘lchamli kalit massivi. Kalit dastlab 256 baytgacha to‘ldiriladi.

(cc) BY © Rahmatullayev I.R., Boyquziyev I.M., Omonov A.A.

***s[]*:** Har biri bir baytdan iborat bo‘lgan, 256 bayt uzunlikdagi bir o‘lchamli massiv. Bu massiv almashtirish jadvali sifatida ishlatiladi.

- ***m[]:*** Ochiq matn (plaintext) massivi, shifrlanishi kerak bo‘lgan ma’lumotlar.

Algoritmda foydalanilgan akslantirishlar:

⊕: Ikki modul bo‘yicha qo‘shish (bitwise XOR operatsiyasi).

⇔: Qiymatlarni almashtirish (swap).

&: Bit bo‘yicha "va" (AND) operatsiyasi.

%: Qoldiqni olish amali (modulus operatsiyasi).

Algoritmning bosqichlari:

1. Kalit massivi k[] ni tayyorlash:

Kalitni kengaytirish: Agar ***k[]*** massivining dastlabki uzunligi 256 baytdan kichik bo‘lsa, u birinchi elementidan boshlab o‘zini takrorlab, umumiy uzunligi 256 bayt bo‘lgunga qadar to‘ldiriladi. Bu shuni anglatadiki, kalit massivi tsiklik ravishda o‘zini qayta takrorlaydi:

Agar ***k[]*** uzunligi c bo‘lsa (c < 256), unda: ***k[i] = k[i % c]***, bu yerda i = 0 dan 255 gacha.

2. Almashtirish jadvali ***s[]*** ni initsializatsiya qilish:

- Dastlabki qiymatlar: ***s[]*** massivining indekslari 0 dan 255 gacha bo‘lib, har bir element o‘z indeksiga teng qiymat bilan to‘ldiriladi:

s[i] = i, bu yerda i = 0 dan 255 gacha.

3. ***s[]*** massivini ***k[]*** kalit yordamida aralashtirish:

Dastlabki o‘zgaruvchilar:

- r = 0;
- rr = 0;

- c: ***k[]*** massivining to‘ldirishdan oldingi (asl) uzunligi.

Aralashtirish jarayoni:

i ning 0 dan 255 gacha bo‘lgan barcha qiymatlari uchun quyidagi amallar bajariladi:

1. ***r*** ni yangilash:
r=s[(r+s[i]+k[i%c]+s[rr]) & 255]

Izoh: Bu yerda r qiymati ***s[]*** massivining hozirgi holati, kalit elementi va ***s[rr]*** yordamida yangilanadi. Bit bo‘yicha AND operatsiyasi bilan 255 ga cheklangan (mod 256).

2. rr ni yangilash:

$$rr=s[(r+i+i)\ \&\ 255] \oplus rr$$

- Izoh: rr qiymati ***s[]*** massividan olingan qiymat bilan XOR qilinadi, bu esa aralashtirish jarayoniga qo‘shimcha tasodifiylik qo‘shadi.

3. ***s[i]*** va ***s[r]*** ni almashtirish:

$$s[i] \Leftrightarrow s[r]$$

- Izoh: ***s[]*** massivining i va r indeksli elementlari o‘rin almashtiriladi, bu almashtirish jadvalini aralashtiradi.

4. Shifr oqimini generatsiya qilish va ***s[]*** holatini yangilash:

Dastlabki o‘zgaruvchilar:

- t = 0;

- j = 0;

- bayt: Dastlabki qiymati aniqlanmagan, lekin jarayon davomida yangilanadi.

Shifr oqimini generatsiya qilish jarayoni:

i ning 0 dan ***L*** gacha bo‘lgan barcha qiymatlari uchun (bu yerda ***L*** — ochiq matn ***m[]*** uzunligi), quyidagi qadamlar bajariladi:

1. bayt ni yangilash:
bayt=s[(bayt+s[(t+j) & 255]) & 255]
- Izoh: bayt qiymati massivining elementlari orqali yangilanadi, bu yerda t va j indekslari ishlatiladi.
2. ***v[i]*** ni hisoblash:
v[i]=s[(s[s[bayt]]+1) & 255]

© Rahmatullayev I.R., Boyquziyev I.M., Omonov A.A.

- Izoh: v[i] qiymati s[] massiviga uch bosqichli indeksatsiya orqali olinadi, bu shifr oqimini hosil qilish uchun ishlatiladi.

3. j ni yangilash:

$$j=v[i] \oplus j$$

- Izoh: j qiymati v[i] bilan XOR qilinadi, bu shifr holatini yanada aralashtiradi.

4. ***s[t]*** va ***s[bayt]*** ni almashtirish:

$$s[t] \Leftrightarrow s[bayt]$$

- Izoh: ***s[]*** massivining t va bayt indeksli elementlari o‘rin almashtiriladi.

5. t ni yangilash:

$$t=(t+1)\ \&\ 255$$

- Izoh: t qiymati 1 ga oshiriladi va 255 ga bit bo‘yicha AND operatsiyasi bilan cheklangan (mod 256).

5. Ochiq matnni shifrlash:

- Shifrlangan matnni olish:

- Har bir i uchun shifrlangan matn ***c[i]*** quyidagicha hisoblanadi:

$$c[i]=m[i] \oplus v[i]$$

- Izoh: Ochiq matn ***m[i]*** shifr oqimi ***v[i]*** bilan XOR qilinadi.

Algoritmning tahlili:
Afzalliklari:

- Katta ichki holat maydoni: 256 baytli ***s[]*** massivi shifrning ichki holatini tashkil etadi, bu esa 256! ta mumkin bo‘lgan almashtirishlarni anglatadi. Bu tajovuzkorlar uchun barcha mumkin bo‘lgan holatlarni tekshirishni amalda imkonsiz qiladi.

- Kalitning moslashuvchanligi: Kalit uzunligining minimal chegarasi 16 bayt bo‘lib, u 256 baytgacha kengaytiriladi. Bu kalit uzunligini xavfsizlik talablariga mos ravishda oshirish imkonini beradi.

- Yuqori tasodifiylik: Shifr oqimi ***v[i]*** ni hosil qilishda uch bosqichli indeksatsiya va XOR operatsiyalaridan foydalanish tasodifiylikni oshiradi va statistik zaifliklarni kamaytiradi.

- Tezkor ishlash: Algoritm faqat oddiy arifmetik va bit bo‘yicha operatsiyalardan foydalanadi, bu esa uni dasturiy ta’minotda samarali amalga oshirishga imkon beradi.

Xavfsizlik xususiyatlari:

- Zaifliklarni kamaytirish: RC4 da aniqlangan zaifliklarni bartaraf etish uchun qo‘shimcha o‘zgaruvchilar (r, rr, j, bayt) va murakkabroq aralashtirish funksiyalari qo‘shilgan.

- Dinamik holat o‘zgarishi: Shifrning ichki holati har bir iteratsiyada o‘zgarib boradi, bu tajovuzkorlar uchun shifr holatini bashorat qilishni qiyinlashtiradi.

- Tasodifiylik testlari: Algoritm tomonidan generatsiya qilingan shifr oqimi NIST statistik testlari yordamida sinovdan o‘tkazilishi mumkin, bu tasodifiylik darajasini baholashga imkon beradi.

E'tiborga olish kerak bo‘lgan jihatlar:

- Kalit va ichki holat bog'liqligi: Kalitning to‘g'ri aralashtirilishi va ichki holatdan kalitni tiklash imkoniyatining oldini olish uchun algoritmning KSA (Key Scheduling Algorithm) qismi puxta tahlil qilinishi kerak.

- Statistik tahlil: Shifr oqimining statistik xususiyatlarini chuqur tahlil qilish zarur, chunki RC4 ning ayrim zaifliklari aynan shifr oqimining statistik nomuvofiqliklari tufayli yuzaga kelgan.

Kriptoanaliz: Algoritmni differential va boshqa kriptoanaliz usullari yordamida tahlil qilib, uning bardoshliligini tekshirish muhimdir.

Natijalar

Tasodifiy yoki psevdotasodifiy sonlar generatorlari tomonidan hosil qilingan ketma-ketliklarning tasodifiylik darajasini tekshirish juda muhim hisoblanadi. Bugungi kunda tadqiqotchilar qurilmalar yoki dasturiy ta’minotga asoslangan yangi tasodifiy sonlar generatorlarini ishlab chiqmoqdalar. Biroq, ulardan hosil bo‘lgan tasodifiy qiymatlarni tegishli baholashlarsiz amaliyotda qo‘llash tavsiya etilmaydi.

(cc) BY © Rahmatullayev I.R., Boyquziyev I.M., Omonov A.A.

Tasodifiy sonlar generatorlarining sifatini baholash 2-jadvalda keltirib o‘tilgan bo‘lib, ayniqsa kriptografiyada, juda katta ahamiyatga ega. Chunki uzluksiz shifrlash algoritmlari tasodifiy sonlar generatorlariga tayanadi. Agar generatorning chiqishlari yetarli darajada tasodifiy bo‘lmasa, shifrlarning xavfsizligi jiddiy xavf ostida qolishi mumkin. Shu sababli, statistik testlash usullari asosida generatorlarni sinovdan o‘tkazish amaliyotda keng qo‘llaniladi.

2-jadval

Statistik testlar to‘plami va ularning xususiyatlari

№	***Muallif***	***Nomi***	***To‘plamdagi testlar soni***
1.	*Donald Knuth/ Stanford University*	*The Art Of Computer Programming Vol. 2 Seminumerical Algorithms*	*11 ma*
2.	*George Marsaglia/Florida State University*	*DIEHARD*	*15 ma*
3.	*Helen Gustafson, et. al./ Queensland University of Technology*	*Crypt-XS*	*6 ma*
5.	*Pierre L’Ecuyer, Richard Simard/ Université de Montréal*	*TestU01’s test batteries*	*SmallCrush (10) Crush (96) BigCrush (106)*
6.	*Andrew Rukhin, et. al./NIST ITL*	*NIST Statistical Test Suite*	*15 ma*

Taklif etilgan algoritm yordamida generatsiya qilingan ketma-ketliklar NIST statistik testlar to‘plami yordamida baholandi. NIST statistik testlar to‘plami (NIST Statistical Test Suite) NIST institutining Kompyuter xavfsizligi va Statistik injeneriya bo‘limlari tomonidan ishlab chiqilgan bo‘lib, 15 ta statistik testni o‘z ichiga oladi. Har bir test ma’lum bir statistik zaiflik tomonini baholashga qaratilgan va shu bo‘yicha natija beradi. Shuningdek, har bir test uchun baholash jarayonida talab etiladigan uzunlikdagi tasodifiy qiymatlar kiritilishi kerak. NIST tarkibidagi har bir test uchun kiritiladigan tasodifiy qiymatlarga minimal uzunlik talabi qo‘yilgan.

Quyidagi **3-jadvalda** NIST testlarining maqsadi (baho beruvchi asosiy zaiflik tomoni), testlash uchun zarur bo‘lgan minimal kirish qiymati uzunligi va taklif etilgan algoritmni baholash natijalari keltirilgan

3-jadval

NIST statistik testlar to‘plami va undan olingan natijalar

№	**Test nomi**	**Test maqsadi**	**Minimal kirish uzunligi (bit)**	**Algoritmni baholash natijalari**
1.	Monobit testi	Ketma-ketlikdagi 0 va 1 lar sonining tengligini tekshiradi	≥ 100	Testdan o‘tdi
2.	Blok ichidagi chastota testi	Bloklardagi 0 va 1 lar sonining tengligini tekshiradi	≥ 100	Testdan o‘tdi
3.	Yugurishlar testi	Yugurishlar soni va uzunligini tekshiradi	≥ 100	Testdan o‘tdi
4.	Eng uzun birlar yugurishi testi	Bloklardagi eng uzun birlar yugurishini tekshiradi	≥ 128	Testdan o‘tdi
5.	Ikkilik matritsa rank testi	Ketma-ketlikdagi matritsalar rangini tekshiradi	≥ 38,912	Testdan o‘tdi

© Rahmatullayev I.R., Boyquziyev I.M., Omonov A.A.

6.	Diskret Furye transformasi testi	Ketma-ketlikdagi davriyliklarni aniqlaydi	≥ 1,000	Testdan o‘tdi
7.	Qoplashsiz shablon moslashtirish testi	Ketma-ketlikda berilgan shablonlarning qoplashsiz takrorlanishini tekshiradi	≥ 1,000,000	Testdan o‘tdi
8.	Qoplanadigan shablon moslashtirish testi	Ketma-ketlikda berilgan shablonlarning qoplanadigan takrorlanishini tekshiradi	≥ 1,000,000	Testdan o‘tdi
9.	Maurerning universal statistik testi	Ketma-ketlikning siqilish darajasini baholaydi	≥ 387,840	Testdan o‘tdi
10.	Chiziqli murakkablik testi	Ketma-ketlikning chiziqli murakkabligini baholaydi	≥ 1,000,000	Testdan o‘tdi
11.	Serial testi	Ketma-ketlikdagi ketma-ket simvollar kombinatsiyalarining chastotasini tekshiradi	≥ 1,000,000	Testdan o‘tdi
12.	Taxminiy entropiya testi	Ketma-ketlikning entropiyasini baholaydi	≥ 1,000,000	Testdan o‘tdi
13.	Kumulativ yig'indilar testi	Kumulativ summalarni tekshiradi	≥ 100	Testdan o‘tdi
14.	Random Excursions testi	Ketma-ketlikdagi Markov zanjiri xususiyatlarini tekshiradi	≥ 1,000,000	Testdan o‘tdi
15.	Random Excursions Variant testi	Random Excursions testining kengaytirilgan varianti	≥ 1,000,000	Testdan o‘tdi

Natijalar tahlili

Taklif etilgan oqimli shifrlash algoritmining samaradorligini baholash maqsadida, maxsus ishlab chiqilgan dasturiy ta’minot yordamida turli oqimli shifrlash algoritmlarining shifrlash tezligi o‘lchandi. Ushbu sinovda 100,000,000 bayt hajmdagi ma’lumotlar shifrlanib, jarayonga sarflangan vaqt millisekundlarda hisoblandi. Olingan natijalar 4-jadvalda keltirilgan.

Quyida ishlab chiqilgan yangi algoritm va mavjud oqimli shifrlash algoritmlarining xavfsizlik va tezkorlik jihatlari bo‘yicha tahlil natijalari keltirilgan. Jadvalda har bir algoritm NIST Statistical Test Suite (15 ta test) asosida baholangan va shifrlash tezligi megabit/sekund (Mbit/sek) da ko‘rsatilgan.

Ishlab chiqilgan va mavjud algoritmlarning xavfsizlik va tezkorlik bo‘yicha tahlili

№	Algoritm nomi	NIST Special testlar to’plami asosida tahlil natijasi (15 testdan)	Tezligi (Mbit/sek)
1.	SalSa20	15	254.89
2.	XSalSa20	15	216.61
3.	ChaCha	15	227.36
4.	ISAAC	14	550.15
5.	RC4	15	395.02
6.	RC4+	15	302.45
7.	VMPC	15	305.61
8.	SPRITZ	15	281.36
9.	HC128	12	229.51
10.	HC256	15	353.29
11.	AES CTR 128	13	131.08
12.	Taklif etilgan algoritm	15	322.50

NIST testlari natijalari bo‘yicha tahlil:

© Rahmatullayev I.R., Boyquziyev I.M., Omonov A.A.

15 ta testdan muvaffaqiyatli o‘tgan algoritmlar:

- Salsa20, XSalsa20, ChaCha, RC4, RC4+, VMPC, SPRITZ, HC-256 va taklif etilgan algoritm.

Ushbu algoritmlar tasodifiylik va statistik xususiyatlari bo‘yicha yuqori ko‘rsatkichlarga ega ekanligini ko‘rsatadi.

- 14 ta testdan o‘tgan algoritm:
  - ISAAC.
  - Bu algoritm bir testda yetarli natijaga erishmagan bo‘lsa-da, umuman olganda yaxshi ko‘rsatkichlarga ega.
- **12 va 13 ta testdan o‘tgan algoritmlar:**
  - HC-128 (12 ta test), AES CTR 128 (13 ta test).
  - Ushbu algoritmlar ayrim statistik testlarda yetarli tasodifiylikni ta’minlamagan bo‘lishi mumkin.
- **Tezlik bo‘yicha tahlil:**
  - Eng tezkor algoritmlar:
  - ISAAC – 550.15 Mbit/sek.
  - RC4 – 395.02 Mbit/sek.
  - HC-256 – 353.29 Mbit/sek.
  - Taklif etilgan algoritm – 322.50 Mbit/sek.
- **O‘rtacha tezlikka ega algoritmlar:**
  - RC4+, VMPC, SPRITZ – taxminan 280–305 Mbit/sek oralig‘ida.
  - Salsa20, XSalsa20, ChaCha – 216.61–254.89 Mbit/sek.
- **Nisbatan sekinroq algoritmlar:**
  - AES CTR 128 – 131.08 Mbit/sek.
  - Bu algoritm blokli shifrlash usuliga asoslanganligi sababli tezligi oqimli shifrlash algoritmlariga nisbatan pastroq.

Taklif etilgan algoritm NISTning 15 ta statistik testidan muvaffaqiyatli o‘tib, yuqori xavfsizlik darajasini namoyon etdi. Bu uning tasodifiylik va kriptografik mustahkamlik bo‘yicha zamonaviy talablarni qondirishini ko‘rsatadi.

- **Tezlik bo‘yicha**, taklif etilgan algoritm **322.50 Mbit/sek** ko‘rsatkich bilan yuqori samaradorlikka ega. Bu uni boshqa mashhur oqimli shifrlash algoritmlari bilan raqobatbardosh qiladi.

- **ISAAC** algoritmi eng yuqori tezlikka ega bo‘lsa-da, NIST testlaridan faqat 14 tasidan o‘tganligi uning xavfsizlik darajasi bo‘yicha ba’zi savollarni keltirib chiqarishi mumkin.

- **RC4** va uning variantlari (**RC4+**, **VMPC**, **SPRITZ**) ham yuqori tezlik va xavfsizlik ko‘rsatkichlariga ega. Biroq, RC4 algoritmining ma’lum zaifliklari mavjudligi sababli, uning xavfsizligi bo‘yicha ehtiyotkorlik talab etiladi.

- **AES CTR 128** algoritmi nisbatan sekinroq bo‘lsa-da, blokli shifrlash algoritmi sifatida yuqori xavfsizlikka ega va turli kriptografik ilovalarda keng qo‘llaniladi.

Xulosa

Yuqoridagi tahlil natijalariga asoslanib, taklif qilingan yangi oqimli shifrlash algoritmi o‘zining samaradorligi va xavfsizlik xususiyatlari bilan ajralib turishini ko‘rishimiz mumkin. Algoritm NIST statistik testlar to‘plamidagi barcha 15 ta testdan muvaffaqiyatli o‘tdi, bu esa uning yuqori tasodifiylik darajasiga ega ekanligini va kriptografik talablarni to‘liq qondirayotganini tasdiqlaydi. Tasodifiylik testlaridan muvaffaqiyatli o‘tish shifr oqimining statistik zaifliklardan xoli ekanligini va potensial kriptoanalitik hujumlarga qarshi bardoshli ekanligini bildiradi.

Bundan tashqari, shifrlash tezligi bo‘yicha o‘tkazilgan sinovlarda algoritm yuqori natijalarni ko‘rsatdi. 100 million bayt hajmdagi ma’lumotlarni shifrlashda taklif etilgan algoritm boshqa mashhur oqimli shifrlash algoritmlari bilan raqobatbardosh, ba’zi hollarda esa ulardan ustun ekanligini namoyish etdi. Bu uning nafaqat xavfsiz, balki samarali ekanligini ham ko‘rsatadi, bu esa real vaqt rejimidagi ilovalar va katta hajmdagi ma’lumotlarni qayta ishlashda muhim ahamiyatga ega.

Kelajakdagi tadqiqotlar doirasida taklif qilingan algoritmni kriptoanalitik usullar yordamida chuqurroq baholash rejalashtirilgan. Bu uning potensial zaifliklarini aniqlash va xavfsizlik darajasini yanada oshirish imkonini beradi. Kriptoanaliz algoritmning mustahkamligini sinab ko‘rish va uni tajovuzkorlar tomonidan amalga oshirilishi

(cc) BY © Rahmatullayev I.R., Boyquziyev I.M., Omonov A.A.

mumkin bo‘lgan hujumlardan himoya qilish uchun zarurdir.

Shuningdek, boshqa yondashuvlar asosida yangi oqimli shifrlash algoritmlarini ishlab chiqish ham maqsad qilingan. Bu kriptografiya sohasida innovatsiyalarni davom ettirish, xavfsizlik va samaradorlikni yanada oshirish uchun muhimdir. Turli matematik modellar va arxitekturalarni qo‘llash orqali yangi algoritmlar yaratilishi va ular mavjud yechimlar bilan solishtirilishi mumkin.

Umumiy xulosa sifatida, taklif etilgan yangi oqimli shifrlash algoritmi zamonaviy kriptografik talablarni qondiradi, yuqori xavfsizlik va samaradorlikni ta’minlaydi. Uning NIST statistik testlaridan muvaffaqiyatli o‘tishi va yuqori shifrlash tezligi uni turli sohalarda, jumladan, axborot xavfsizligi, tarmoq kommunikatsiyalari va ma’lumotlarni saqlash tizimlarida qo‘llash imkonini beradi. Boshqa algoritmlarni tanlashda ularning xavfsizlik va tezlik ko‘rsatkichlarini muvozanatlash zarur, chunki har bir ilova uchun optimal yechim xavfsizlik va samaradorlik talablari asosida aniqlanadi.

Foydalanilgan adabiyotlar:

1. Абдурахимов Б., Болтаев Ф. Тасодифий кетма-кетликлар энтропиясини ўлчаш усуллари. “Ахборот технологиялари ва коммуникациялари соҳасида ахборот хавфсизлиги муаммолари” мавзусидаги Республика илмий-техник конференцияси материаллари. «UNICON.UZ» ДУК – Фан-техника ва маркетинг тадқиқотлари маркази. Тошкент, 2019 йил 26 ноябрь. –С.74-75.
2. Абдурахимов Б., Болтаев Ф. Узлуксиз шифрлаш алгоритмларининг тасодифий даражасини тестлаш усуллари. “Ахборот технологиялари ва коммуникациялари соҳасида ахборот хавфсизлиги муаммолари” мавзусидаги Республика илмий-техник конференцияси материаллари. «UNICON.UZ» ДУК – Фан-техника ва маркетинг тадқиқотлари маркази. Тошкент, 2019 йил 26 ноябрь. –С.79-82.
3. Rahmatullayev I. et al. OQIMLI SHIFRLASH ALGORITMLARINING LOYIHALASH USULLARI //Talqin va tadqiqotlar. – 2024. – Т. 1. – №. 27.
4. 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.
5. 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.
6. Xudoykulov Z. T., Rahmatullayev I. R. Yangi oqimli shifrlash algoritmlari va uning kriptotahlili //Milliy standart Ilmiy-texnik jurnali. – 2023. – С. 42-47.
7. Rahmatullayev I. SIMMETRIK UZLUKSIZ SHIFRLASH ALGORITMLARI KRIPTOBARDOSHLILIGINI BAHOLASH MEZONLARI //DIGITAL TRANSFORMATION AND ARTIFICIAL INTELLIGENCE. – 2024. – Т. 2. – №. 3. – С. 94-100.
8. Raxmatullayevich R. I., Nizomovich M. O. MASSIV ELEMENTLARINI UZLUKSIZ ALMASHTIRISHGA ASOSLANGAN UZLUKSIZ SHIFRLASH ALGORITMI //PEDAGOGS. – 2024. – Т. 55. – №. 1. – С. 145-151.
9. Ergash o‘g‘li M. H., Tohir ogli S. D., Baxodir ogli X. A. OQIMLI SHIFRLARNING QURILISH PRINSIPLARI //Journal of new century innovations. – 2023. – Т. 41. – №. 2. – С. 90-94.
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

© Rahmatullayev I.R., Boyquziyev I.M., Omonov A.A.