MUHAMMAD AL-XORAZMIY
NOMIDAGI TATU FARG'ONA FILIALI

FERGANA BRANCH OF TUIT
NAMED AFTER MUHAMMAD AL-KHORAZMI

"AL-FARG'ONIY AVLODLARI"

ELEKTRON ILMIY JURNALI | ELECTRONIC SCIENTIFIC JOURNAL

TA'LIMDAGI ILMIY, OMMABOP VA ILMIY TADQIQOT ISHLARI

1-SON 1(5)
2024-YIL

TATU, FARG'ONA
O'ZBEKISTON

ISSN 2181-4252

O‘ZBEKISTON RESPUBLIKASI RAQAMLI TEXNOLOGIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI FARG‘ONA FILIALI

Muassis: Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg‘ona filiali.
Chop etish tili: O‘zbek, ingliz, rus.
Jurnal texnika fanlariga ixtisoslashgan bo‘lib, barcha shu sohadagi matematika, fizika, axborot texnologiyalari yo‘nalishida maqolalar chop etib boradi.

Учредитель: Ферганский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хоразми.
Язык издания: узбекский, английский, русский.
Журнал специализируется на технических науках и публикует статьи в области математики, физики и информационных технологий.

Founder: Fergana branch of the Tashkent University of Information Technologies named after Muhammad al-Khorazmi.
Language of publication: Uzbek, English, Russian.
The magazine specializes in technical sciences and publishes articles in the field of mathematics, physics, and information technology.

2024 yil, Tom 1, №1
Vol.1, Iss.1, 2024 y

ELEKTRON ILMIY JURNALI **ELECTRONIC SCIENTIFIC JOURNAL**

«Al-Farg‘oniy avlodlari» («The descendants of al-Fargani», «Potomki al-Fergani») O‘zbekiston Respublikasi Prezidenti administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligida 2022-yil 21 dekabrda 054493-son bilan ro‘yxatdan o‘tgan.

Jurnal OAK Rayosatining 2023-yil 30 sentabrdagi 343-sonli qarori bilan Texnika fanlari yo‘nalishida milliy nashrlar ro‘yxatiga kiritilgan.

Tahririyat manzili:
151100, Farg‘ona sh.,
Aeroport ko‘chasi 17-uy,
202A-xona
Tel: (+99899) 998-01-42
e-mail: info@al-fargoniy.uz

FARG’ONA - 2024 YIL

Jurnal quyidagi bazalarda indekslanadi:

Google Scholar · zenodo · ORCID · CYBERLENINKA · WORLD of JOURNALS · Directory of Research Journals Indexing

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

SHA oilasiga mansub xesh funksiyalar tahlili

Rahmatullayev Ilhom Rahmatullayevich,
texnika fanlari bo‘yicha falsafa doktori (PhD),
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalar universiteti Samarqand filiali “Axborot xavfsizli” kafedrasi o‘qituvchisi
Ilhom9001@gmail.com

Umurzakov Oybek,
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalar universiteti Samarqand filiali “Axborot xavfsizli” kafedrasi o‘qituvchisi

Annotatsiya. Bu algoritmlar, turli xil dasturlash va xavfsizlik talablarida keng qo‘llaniladi, jumladan, elektron raqamli imzolar, SSL sertifikatlari va boshqa ko‘plab xavfsizlik protokollari uchun asosiy qismlardir. SHA oilasiga mansub xesh funksiya algoritmlari va ularning qadamlari ketma-ketligi, shuningdek, SHA-3 algoritmi uchun o‘tkazilgan tanlov haqida ma’lumotlar, shuningdek, SHA-1, SHA-2, SHA-3 algoritmlariga nisbatan o‘tkazilgan kriptotahlil natijalari keltirilgan.

Kalit so‘zlar: Xesh funksiya, autentifikatsiya, kalitli va kalitsiz xesh funksiya, SHA-0, SHA-1, SHA-2, SHA-3, Keccak

Kirish. Xesh funksiya bu - ixtiyoriy uzunlikdagi kirish ma’lumotlar to‘plamini (M) fiksirlangan uzunlikdagi H(M) qiymatiga aks ettiruvchi bir tomonlama funksiyadir. Bu qiymat, odatda, xesh yoki xesh qiymati deb ataladi. Bu yerda fiksirlangan uzunlik sifatida 64 bit, 128 bit, 160 bit, 256 bit, 512 bit tushuniladi[2].

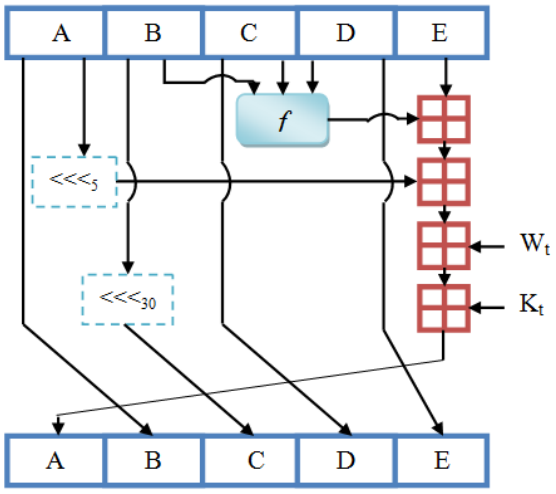
Xeshlash, kirish massividagi ma’lumotlarni maxsus algoritm yordamida bitlar ketma-ketligiga aylantirish jarayonidir. Bu jarayonda, har qanday hajmdagi kirish ma’lumoti qat’iy belgilangan uzunlikdagi xesh qiymatiga aylantiriladi. Xeshlashning asosiy maqsadi ma’lumotlarni xavfsiz, qisqartirilgan va boshqariladigan shaklga olib kelishdir.

Xesh funksiya algoritmlaridan amaliy foydalanishdan ko‘zlangan asosiy maqsad:

1. Ma’lumotni uzatishda va saqlashda uning to‘laligini nazorat qilish.
2. Ma’lumot manba’sini autentifikatsiya qilish.

Amerika Qo‘shma Shtatlarida 1993-yil NSA va NIST birgalikda FIPS PUB 180 standartiga binoan xesh-funksiya algoritmi SHA-0 ni yaratishdi. Oradan ko‘p o'tmay ushbu algoritm bir guruh kriptograflar tomonidan kolliziyaga uchratildi. Shuning uchun 1995-yilda FIPS PUB 180-1[5] standartga binoan SHA-0 algoritmining ma’lum bir qismi o‘zgartirilib SHA-1 algoritmini ishlab chiqildi[1].

Asosiy qism. SHA-1 algoritmda kiruvchi ma’lumotning uzunligi 2^{64} bitdan kichik bo‘lib, xesh qiymat uzunligi *160 bit* bo‘ladi. Kiritilayotgan ma’lumot *512* bitlik bloklarga ajratilib qayta ishlanadi.



1-rasm. SHA-0 va SHA-1 algoritmining blok sxemasi

Xesh qiymatni hisoblash jarayoni quyidagi bosqichlardan iborat:

1-bosqich. To‘ldirish bitlarini qo‘shish.

Berilgan ma’lumot uzunligi *512* modul bo‘yicha *448* bilan taqqoslanadigan (ma’lumot uzunligi $\equiv 448 \bmod 512$) qilib to‘ldiriladi.To‘ldirish hamma vaqt, hattoki ma’lumot uzunligi 512 modul bo‘yicha 448 bilan taqqoslanadigan bo‘lsa ham bajariladi.

To‘ldirish quyidagi tartibda amalga oshiriladi: ma’lumotga *1* ga teng bo‘lgan bitta bit qo‘shiladi, qolgan bitlar esa 0 lar bilan to‘ldiriladi. Shuning uchun qo‘shilgan bitlar soni 1 dan 512 tagacha bo‘ladi.

2- bosqich. Ma’lumotning uzunligini qo‘shish.

1-bosqichning natijasiga berilgan ma’lumot uzunligining *64* bitlik qiymati qo‘shiladi.

3- bosqich. Xesh qiymat uchun bufer initsializatsiya qilish.

Xesh funksiyaning oraliqva ohirgi natijalarini saqlash uchun *160* bitlik buferdan foydalaniladi. Bu buferni beshta *32* bitlik *A, B, C, D, E* registrlar ko‘rinishida tasvirlash mumkin. Bu registrlarga *16* lik sanoq sistemasida quyidagi boshlang‘ich qiymatlar beriladi:

A=0x67452301,
B=0xEFCDAB89,
C=0x98BADCFE,
D=0x10325476,
E=0xC3D2E1F0.

Keyinchalik bu o‘zgaruvchilar mos ravishda yangi *a, b, c, d* va *e* o'zgaruvchilarga yozib olinadi.

4- bosqich. Ma’lumotni *512* bitlik bloklarga ajratib qayta ishlash.

Bu xesh funksiyaning asosiy sikli quyidagicha bo‘ladi:

for (t = 0; t < 80; t++)
{temp = (a<<< 5) + f_t(b, c, d) +e+ W_t+ K_t;
e = d; d = c; c = b<<< 30; b = a; a = temp;
},

Bu yerda <<< - chapga siklik surish amali. K_t lar *16* lik sanoq sistemasida yozilgan quyidagi fiksirlangan sonlardan iborat:

$$\mathbf{K}_t = \begin{cases} \mathbf{5A827999}, & t = 0,...,19, \\ \mathbf{6ED9EBA1}, & t = 20,...,39, \\ \mathbf{8F1BBCDC}, & t = 40,...,59, \\ \mathbf{CA62C1D6}, & t = 60,...,79. \end{cases}$$

$f_t(x, y, z)$ funksiyalar esa quyidagi ifodalar bilan aniqlanadi:

$$f_t(\mathbf{x},\mathbf{y},\mathbf{z}) = \begin{cases} \mathbf{X} \wedge \mathbf{Y} \vee \neg\mathbf{X} \wedge \mathbf{Z}, & \mathbf{t} = 0,...,19, \\ \mathbf{X} \oplus \mathbf{Y} \oplus \mathbf{Z}, & \mathbf{t} = 20,...,39,\ 60,...,79, \\ \mathbf{X} \wedge \mathbf{Y} \vee \mathbf{X} \wedge \mathbf{Z} \vee \mathbf{Y} \wedge \mathbf{Z}, & \mathbf{t} = 40,...,59. \end{cases} \quad (1)$$

W_t lar kengaytirilgan ma’lumotning *512* bitlik blokining *32* bitlik qism bloklaridan quyidagi qoida bo‘yicha hosil qilinadi:

$$W_t = \begin{cases} M_t, & t = 0,...,15, \\ (W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16}) <<< 1, & t = 16,...,79. \end{cases}$$

SHA-1 uchun (2)

$$W_t = \begin{cases} M_t, & t = 0,...,15, \\ (W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16}), & t = 16,...,79. \end{cases}$$

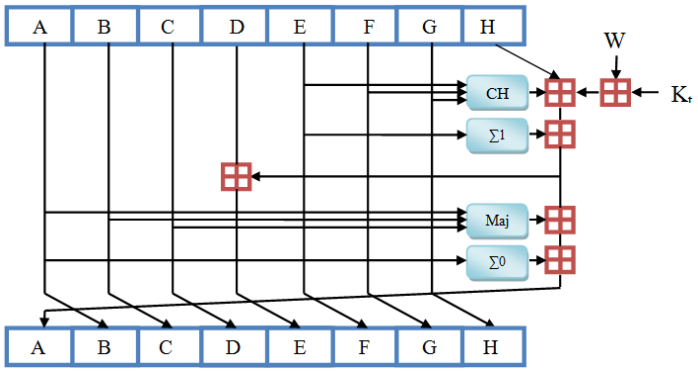
SHA-0 uchun (3)

Asosiy sikl tugagandan so‘ng *a, b, c, d* va *e* larning qiymatlari mos ravishda *A, B, C, D* va *E* registrlardagi qiymatlarga qo‘shiladi hamda shu registrlarga yozib qo'yiladi va kengaytirilgan ma’lumotning keyingi *512* bitlik blokini qayta ishlashga o‘tiladi.

5- bosqich. Natija.

Ma’lumotning xesh qiymati *A, B, C, D* va *E* registrlardagi qiymatlarni birlashtirish natijasida hosil qilinadi.

Keyinchalik AQSh da kalit uzunligi *128, 192* va *256* bit bo‘lgan yangi shifrlash standarti ishlab chiqilganligi hamda texnologiyaning yuqori sur’atda rivojlanganligi sababli shunday darajadagi bardoshlilikka ega bo‘lgan yangi xesh funksiyalar algoritmlarini yaratishga ehtiyoj paydo bo‘ldi. Shu sababli 2002-yilda AQSh ning yangi xesh funksiya standarti FIPS PUB 180-2[6] qabul qilindi. Bu standartda to‘rtta xesh funksiya - SHA-224, SHA-256, SHA-384 va SHA-512 algoritmlari keltirilgan[12].



2-rasm. SHA-2 algoritmining umumiy blok sxemasi.

Quyida **SHA-256** xesh funksiyasi algoritmini qarab chiqamiz. Bu algoritmda kiruvchi ma’lumotning uzunligi 2^{64} bitdan kichik bo‘lib, xesh qiymat uzunligi *256* bit bo‘ladi. Ushbu algoritmni ikki qismga: siqish funksiyasi va ma’lumotni qayta ishlash algoritmiga bo‘lish mumkin. Siqish funksiyasi uzunligi *256* bit bo‘ladigan oraliq xesh qiymatni matnning navbatdagi blokini kalit sifatida olib shifrlash algoritmidan iborat. Siqish funksiyasida oldingi belgilashlardan tashqari quyidagi belgilashlar ham ishlatiladi: R^n - so'zni *n* bit o'nga siklik surish, S^n - so'zni *n* bit o‘ngga arifmetik(logik) surish. So‘zning o‘lchami *32* bitga teng deb, qo‘shish esa $(a+b) mod\ 2^{32}$ bo'yicha olinadi. Boshlang‘ich xeshlash vektori 8 ta 32 razryadlik so'zlardan iborat bo‘lib, u quyidagi tub sonlardan olingan kvadrat ildizlarning kasr qismlariga teng qilib olinadi:

{6a09e667, bb67ae85, 3c6ef372, a54ff53a, 510e527f, 9b05688c, 1f83d9ab, 5be0cd19}

Keyingi hisoblashlar quyidagi bosqichda olib boriladi:

1-bosqich. Boshlang‘ich qayta ishlash. Xeshlanuvchi ma’lumot SHA-1 ga o‘xshab uzunligi 512 ga karrali bo‘lguncha to‘ldiriladi. To‘ldirishda ma’lumotdan keyin 1 yoziladi va qolgan bitlar 0 lar bilan to‘ldiriladi. Bunda ma’lumot uzunligi *512* modul bo'yicha *448* bilan taqqoslanadigan qilib to‘ldiriladi. Keyin berilgan ma’lumotning 64 bitlik uzunligi yoziladi.

2-bosqich. Ma’lumotni *512* bitlik bloklarga ajratish. Kengaytirilgan ma’lumot *512* bitlik bloklarga ajratiladi.

3-bosqich. Asosiy sikl. Bu siklda argumenti va qiymatlari *32* bit bo‘lgan oltita mantiqiy funksiyadan foydalaniladi:

$$Ch(x,y,z)=(x\wedge y)\oplus(\overline{x}\wedge z),$$
$$Maj(x,y,z)=(x\wedge y)\oplus(x\wedge z)\oplus(y\wedge z),$$
$$\Sigma_0(x)=S^2(x)\oplus S^{13}(x)\oplus S^{22}(x), \qquad (4)$$
$$\Sigma_1(x)=S^6(x)\oplus S^{11}(x)\oplus S^{25}(x),$$
$$\sigma_0(x)=S^7(x)\oplus S^{18}(x)\oplus R^3(x),$$
$$\sigma_1(x)=S^{17}(x)\oplus S^{19}(x)\oplus R^{10}(x).$$

$M^{(i)}$ blokni $M^{(i)}=M_0^{(i)}M_1^{(i)}...M_{15}^{(i)}$ 16 ta *32* bitlik so'zlargta ajratiladi va $W_0,...,W_{63}$ lar quyidagicha aniqlanadi:

$$W_j=M_j^{(i)}, \quad j=0,...,15$$

for j=16 to 63

{

$$W_j=\sigma_1(W_{j-2})+W_{j-7}+\sigma_0(W_{j-15})+W_{j-16} \quad \}$$

$K_0,...,K_{63}$ o'zgarmaslar sifatida esa quyidagi 64 ta *16* lik ko'rinishda tasvirlangan sonlardan chiqarilgan kub ildizlar kasr qismlarining birinchi *32* biti olinadi:

428a2f98	*71374491*	*b5c0fbcf*	*e9b5dba5*	*3956c25b*	*59f111f1*	*923f82a4*	*ab1c5ed5*
d807aa98	*12835b01*	*243185be*	*550c7dc3*	*72be5d74*	*80deb1fe*	*9bdc06a7*	*c19bf174*
e49b69c1	*efbe4786*	*0fc19dc6*	*240ca1cc*	*2de92c6f*	*4a7484aa*	*5cb0a9dc*	*76f988da*
983e5152	*a831c66d*	*b00327c8*	*bf597fc7*	*c6e00bf3*	*d5a79147*	*06ca6351*	*14292967*
27b70a85	*2e1b2138*	*4d2c6dfc*	*53380d13*	*650a7354*	*766a0abb*	*81c2c92e*	*92722c85*
a2bfe8a1	*a81a664b*	*c24b8b70*	*c76c51a3*	*d192e819*	*d6990624*	*f40e3585*	*106aa070*
19a4c116	*1e376c08*	*2748774c*	*34b0bcb5*	*391c0cb3*	*4ed8aa4a*	*5b9cca4f*	*682e6ff3*
748f82ee	*78a5636f*	*84c87814*	*8cc70208*	*90befffa*	*a4506ceb*	*bef9a3f7*	*c67178f2*

Asosiy sikl quyidagicha bo‘ladi:

for i=0 to N

{ // *N* - kengaytirilgan ma’lumotning bloklari soni.

// *a, b, c, d, e, f, g, h* registrlarni xesh funksiyaning *(i-1)* oraliq qiymati bilan

// qiymatlarni o’zlashtirish(initsializatsiyalash).

$a=H_1^{(i-1)};\ b=H_2^{(i-1)};\ c=H_3^{(i-1)};\ d=H_4^{(i-1)};\ e=H$

// *a, b, c, d, e, f, g, h* registrlarga siqish funksiyasini qo‘llash.

for i=0 to 63

{ // Ch (e,f,g), Maj (a,b,c), $\Sigma_0(a)$, $\Sigma_1(e)$ va W_j lar hisoblanadi.

$T_1 = h + \Sigma_1(e) + Ch(e, f, g) + K_j + W_j$

$T_2 = \Sigma_0(a) + Maj(a,b,c)$

$h = g$; $g = f$; $f = e$; $e = d + T_1$; $d = c$; $c = b$; $b = a$; $a = T_1 + T_2$

}

// i – oraliq xesh qiymat $H^{(i)}$ ni hisoblash.

$H_1^{(i)} = a + H_1^{(i-1)}$; $H_2^{(i)} = b + H_2^{(i-1)}$; $H_3^{(i)} = c + H_3^{(i-1)}$; $H_4^{(i)} = d + H_4^{(i-1)}$;

$H_5^{(i)} = e + H_5^{(i-1)}$; $H_6^{(i)} = f + H_6^{(i-1)}$; $H_7^{(i)} = g + H_7^{(i-1)}$; $H_8^{(i)} = h + H_7^{(i-1)}$

}

Natijada

$H^{(N)} = H_1^{(N)} \| H_2^{(N)} \| H_3^{(N)} \| H_4^{(N)} \| H_5^{(N)} \| H_6^{(N)} \| H_7^{(N)} \| H_8^{(N)}$

ifoda *M* ma’lumotning xesh qiymatini beradi.

SHA-224 xesh funksiyasi algoritmi SHA-256 algoritmidan faqat boshlang‘ich vektori ya’ni:

{c1059ed8, 367cd507, 3070dd17, f70e5939, ffc00b31, 0x68581511, 0x64f98fa7, 0xbefa4fa4} bilan farq qiladi. Bu algoritmda kiruvchi ma’lumotning uzunligi 2^{64} bitdan kichik bo‘lib, xesh qiymat uzunligi *224* bit bo‘ladi. Boshqa barcha hisoblashlar SHA-256 algoritmi bilan bir hil bo‘ladi. Natijada chiquvchi xesh qiymat sifatida

$H^{(N)} = H_1^{(N)} \| H_2^{(N)} \| H_3^{(N)} \| H_4^{(N)} \| H_5^{(N)} \| H_6^{(N)} \| H_7^{(N)} \| H_8^{(N)}$

ning chap tomonidan *256* biti, ya'ni

$H^{(N)} = H_1^{(N)} \| H_2^{(N)} \| H_3^{(N)} \| H_4^{(N)} \| H_5^{(N)} \| H_6^{(N)} \| H_7^{(N)}$

olinadi.

SHA-512 xesh funksiya o‘zining tuzilishiga ko‘ra SHA-256 xesh funksiyasiga o‘xshaydi, lekin unda uzunligi *64* bit bo‘lgan ma’lumotlar ustida amal bajariladi. Bu algoritmda kiruvchi ma’lumotning uzunligi 2^{128} bitdan kichik bo‘lib, xesh qiymat uzunligi *512* bit bo‘ladi. Ma’lumotning uzunligi *1024* ga karrali qilib to‘ldiriladi. To‘ldirishda ma’lumotning oxiriga *1* yozilib, qolgan qismi *0* lar bilan shunday to‘ldiriladiki, ma’lumotning uzunligi *1024* ga karrali sondan *128* bit kam bo‘lishi kerak. Oxiriga berilgan ma’lumotning *128* bit uzunligi qo‘shiladi. Shunday qilib, kengaytirilgan ma’lumot uzunligi *1024* ga karrali bo‘ladi. Boshlang‘ich vektor 8 ta *64* razryadlik so‘zlardan iborat bo‘lib, u quyidagi tub sonlardan olingan kvadrat ildizlarning kasr qismlariga teng bo‘ladi:

{6a09e667f3bcc908, bb67ae8584caa73b, 3c6ef372fe94f82b, a54ff53a5f1d36f1, 510e527fade682d1, 9b05688c2b3e6c1f, 1f83d9abfb41bd6b, be0cd19137e2179}

Asosiy sikl huddi SHA-256 algoritmidagidek bo‘lib, faqat SHA-512 algoritmidagi funksiyalar va bajariladigan amallar *64* bitlik ma’lumotlarda aniqlangan hamda qo‘shish mod 2^{64} bo'yicha olinadi. Siqish funksiyasi esa faqat sikldagi iteratsiyalar soni bilan farq qiladi:

for i=0 to 79

{ // Ch (e,f,g), Maj (a,b,c), $\Sigma_0(a)$, $\Sigma_1(e)$ va W_j larni hisoblanadi.

$T_1 = h + \Sigma_1(e) + Ch(e, f, g) + K_j + W_j$

$T_2 = \Sigma_0(a) + Maj(a,b,c)$

$h = g$; $g = f$; $f = e$; $e = d + T_1$; $d = c$; $c = b$; $b = a$; $a = T_1 + T_2$

}

Mantiqiy funksiylar esa SHA-256 algoritmdagi mantiqiy funksiyalardan quyidagicha farq qiladi:

$$\begin{aligned} &\Sigma_0(x)=S^{28}(x)\oplus S^{34}(x)\oplus S^{39}(x),\\ &\Sigma_1(x)=S^{14}(x)\oplus S^{18}(x)\oplus S^{41}(x),\\ &\sigma_0(x)=S^{1}(x)\oplus S^{8}(x)\oplus R^{7}(x),\\ &\sigma_1(x)=S^{19}(x)\oplus S^{61}(x)\oplus R^{6}(x). \end{aligned} \quad (5)$$

$M^{(i)}$ blokni $M^{(i)} = M_0^{(i)} M_1^{(i)} ... M_{15}^{(i)}$ 16 ta *64* bitlik qismlarga ajratiladi va $W_0,...,W_{79}$ lar quyidagicha aniqlanadi:

$W_j = M_j^{(i)}, \quad j = 0,...,15,$

for j=16 to 79

{

$W_j = \sigma_1(W_{j-2}) + W_{j-7} + \sigma_0(W_{j-15}) + W_{j-16}$ }

$K_0,...,K_{79}$ o‘zgarmaslar sifatida esa quyidagi *80* ta *16* lik ko'rinishda tasvirlangan tub sonlardan chiqarilgan kub ildizlar kasr qismining birinchi *64* biti olinadi:

428a2f98d728ae22	*7137449123ef65cd*	*b5c0fbcfec4d3b2f*	*e9b5dba58189dbbc*
3956c25bf348b538	*59f111f1b605d019*	*923f82a4af194f9b*	*ab1c5ed5da6d8118*
d807aa98a3030242	*12835b0145706fbe*	*243185be4ee4b28c*	*550c7dc3d5ffb4e2*
72be5d74f27b896f	*80deb1fe3b1696b1*	*9bdc06a725c71235*	*c19bf174cf692694*
e49b69c19ef14ad2	*efbe4786384f25e3*	*0fc19dc68b8cd5b5*	*240ca1cc77ac9c65*
2de92c6f592b0275	*4a7484aa6ea6e483*	*5cb0a9dcbd41fbd4*	*76f988da831153b5*
983e5152ee66dfab	*a831c66d2db43210*	*b00327c898fb213f*	*bf597fc7beef0ee4*
c6e00bf33da88fc2	*d5a79147930aa725*	*06ca6351e003826f*	*142929670a0e6e70*
27b70a8546d22ffc	*2e1b21385c26c926*	*4d2c6dfc5ac42aed*	*53380d139d95b3df*
650a73548baf63de	*766a0abb3c77b2a8*	*81c2c92e47edaee6*	*92722c851482353b*
a2bfe8a14cf10364	*a81a664bbc423001*	*c24b8b70d0f89791*	*c76c51a30654be30*
d192e819d6ef5218	*d69906245565a910*	*f40e35855771202a*	*106aa07032bbd1b8*
19a4c116b8d2d0c8	*1e376c085141ab53*	*2748774cdf8eeb99*	*34b0bcb5e19b48a8*
391c0cb3c5c95a63	*4ed8aa4ae3418acb*	*5b9cca4f7763e373*	*682e6ff3d6b2b8a3*
748f82ee5defb2fc	*78a5636f43172f60*	*84c87814a1f0ab72*	*8cc702081a6439ec*
90beffa23631e28	*a4506cebde82bde9*	*bef9a3f7b2c67915*	*c67178f2e372532b*
ca273eceea26619c	*d186b8c721c0c207*	*eada7dd6cde0eb1e*	*f57d4f7fee6ed178*
06f067aa72176fba	*0a637dc5a2c898a6*	*113f9804bef90dae*	*1b710b35131c471b*
28db77f523047d84	*32caab7b40c72493*	*3c9ebe0a15c9bebc*	*431d67c49c100d4c*
4cc5d4becb3e42b6	*597f299cfc657e2a*	*5fcb6fab3ad6faec*	*6c44198c4a475817.*

Natijada chiqqan *8* ta *64 bitlik* ma’lumotlar konketenatsiya amali yordamida birlashtirilib, hosil bo‘lgan *512 bit* ni M ma’lumotning xesh qiymati deb e’lon qilinadi. Ya’ni:

$$H^{(N)} = H_1^{(N)} \| H_2^{(N)} \| H_3^{(N)} \| H_4^{(N)} \| H_5^{(N)} \| H_6^{(N)} \| H_7^{(N)} \| H_8^{(N)}$$

SHA-384 xesh-funksiya algoritmi SHA-512 algoritmidan faqat boshlang‘ich vektori $H^{(0)}$ = *{cbbb9d5dc1059ed8, 629a292a367cd507, 9159015a3070dd17, 152fecd8f70e5939, 67332667ffc00b31, eb44a8768581511, db0c2e0d64f98fa7, 47b5481dbefa4fa4}* bilan farq qiladi. Bu algoritmda kiruvchi ma’lumotning uzunligi 2^{128} bitdan kichik bo‘lib, xesh qiymat uzunligi *384* bit bo‘ladi. Qolgan barcha hisoblashlar SHA-512 algoritmi bilan bir hil bo‘ladi. Natijada chiquvchi xesh qiymat sifatida $H^{(N)} = H_1^{(N)} \| H_2^{(N)} \| H_3^{(N)} \| H_4^{(N)} \| H_5^{(N)} \| H_6^{(N)} \| H_7^{(N)} \| H_8^{(N)}$ ning chap tomonidan *384* biti, ya'ni $H^{(N)} = H_1^{(N)} \| H_2^{(N)} \| H_3^{(N)} \| H_4^{(N)} \| H_5^{(N)} \| H_6^{(N)}$ olinadi.

1-jadval. SHA oilasiga mansub algoritmlarning umumiy parametrlari[2].

Xesh funksiya algoritm nomi	Xeshlan adigan matn uzunligi	Kirish blok uzunligi	Xesh qiymat uzunligi	Har bir blokning xeshlash qadamlar soni
SHA-1	$<2^{64}$	512	160	80
SHA-224	$<2^{64}$	512	224	64
SHA-256	$<2^{64}$	512	256	64
SHA-384	$<2^{128}$	1024	384	80
SHA-512	$<2^{128}$	1024	512	80

SHA-3 algoritmini qabul qilish bo‘yicha o‘tkazilayotgan tanlov

Bugungi kunda dunyoning bir qator rivojlangan mamlakatlari hukumatining bank va boshqa tizimlarida elektron hujjatlardan foydalanish, ularni qabul qilish, uzatish va qayta ishlashda tezligi hamda ishonchliligiga nisbatan yangi talablar yuzaga kelmoqda. Buning asosiy sababi axborot hajmi kundan-kunga keskin ortib borishi ta’kidlanadi. Lekin vazifa faqatgina axborotni uzatish emas, balki uzatish bilan bir qatorda uning xavfsizligini ham ta'minlashdan iborat. Ushbu masalani hal etish uchun bevosita elektron raqamli imzo algoritmlaridan foydalaniladi. So‘ngi yillarda himoyalangan elektron raqamli imzo algoritmlari standart tizimlaridan foydalanish ustida olib borilgan tadqiqotlar shuni ko'rsatadiki, Amerika Qo‘shma Shtatlarida eng ko'p tarqalgan FIPS PUB 180-1 algoritniga kolliziyaning topilganligi va FIPS PUB 180-2 standartlariga kiruvchi algoritmlarning ham umumiy strukturasi SHA-1 algoritmiga asoslanganligi, ular uchun ham kolliziya topilish ehtimolligini keltirib chiqaradi. Bu omillar esa o‘z navbatida yangi kriptobardoshligi yuqori bo‘lgan algoritmlar ustida tadqiqot olib borishni talab etadi.

2007-yil iyun oyida aynan mana shu g‘oya asosida SHA-3 deb nomlangan yangi xesh funksiya algoritmini qabul qilish bo‘yicha tanlov e’lon qilindi[9]. Tanlovda qatnashuvchi ishtirokchilarning arizalari 2008 yilning dekabr oyigacha qabul qilinib, unda jami 64 ta arizalardan 51 tasi tanlovga qatnashish

imkoniyatiga ega bo‘ldi. Tanlov uch bosqichdan iborat bo‘lib, 2012-yilning dekabr oyida tugatish rejalashtirilgan.

Amerikaning Milliy Standartlar va Texnologiyalar Instituti(NIST) tomonidan tanlovga qo‘yilgan asosiy talab SHA-2 oilasiga mansub xesh-algoritmlarga nisbatan ma’lumotni xeshlash samaradorligi yuqori va barcha kriptotahlil usullariga nisbatan bardoshli bo‘lgan yangi xesh-funksiya algoritmlar sinfini yaratishdan iborat.

SHA-3 tanlovining g‘olib algoritmi *224, 256, 384* va *512* bit chiqish bloklariga mo‘ljallangan bo‘lishi kerak.

Tanlovda xesh-funksiya algoritmlariga qo'yilgan umumiy talablar:

- katta o‘lchamdagi axborotni xeshlash imkonining mavjudligi;
- algoritmning ishlash tezligining yuqoriligi(>10 CPB(cycles per byte-bir bayt axborotni qayta ishlash uchun zarur bo‘lgan sikllar soni) Intel Core2);
- bir qancha zamonaviy platformalarda realizatsiya qilishning osonligi;

Bundan tashqari algoritmda turli blok o‘lchamidagi hisoblashni amalga oshirishda funksiya qadamlar ketma-ketligining deyarli bir xil(farqi juda kam) bo‘lishi kerak. Bu talab bir rejimdan boshqasiga tez o'tib hisoblash imkonini yaratib beradi.

Tanlovning birinchi bosqichi 2009-yilning dekabr oyida yakunlandi. Natijada 51 ta xesh funksiya algoritmi tanlovga kelib tushgan. Ular bardoshligi, foydalanish platformasi (8,16, 32, 64) va tezligi tahlili haqida qisqa ma’lumot [8,12,14] adabiyotlarda keltirilgan.

Mazkur tanlovning o’tkazilishida tanlov rahbariyati algoritmlarning ikkinchi bosqichga o'tishi uchun uning turli xil kriptotahlil usullariga nisbatan bardoshli yoki bardoshsiz ekanligiga ham katta e'tibor qaratishgan. Shundan kelib chiqib ikkinchi bosqichga ishtirokchilardan 14 tasi (BLAKE, Blue Midnight WISH, CubeHash, ECHO, Fugue, Grost l, Hamsi, JH, Keccak, Luffa, Shabal, SHAvite-3, SIMD, Skein) loyiq deb topildi. Ushbu xesh algortimlarning qurilish tamoyillari bo’yicha qisqacha ma’lumot keltirilgan[9].

2010-yilda ikkinchi bosqich yakunlanib 14 ta algoritmdan quyidagi 5 tasi tanlov finaliga qatnashish imkoniyatini qo‘lga kiritdi:

1. BLAKE (Jean-Philippe Aumasson);
2. Grostl (Lars Ramkilde Knudsen);
3. JH (Hongjun Wu);
4. Keccak (Joan Daemen);
5. Skein (Bryus Shnayer).

2012-yilning noyabr oyida yuqoridagi beshta algotimdan “Keccak” xesh funksiya algoritmi tanlov g‘olibi deb e’lon qilinib, SHA-3 xesh funksiya algoritm standarti sifatida qabul qilindi.

Kriptotahlil natijalari. SHA-1 (SHA – Secure Hash Algorithm) – xesh-funksiya AQSH Milliy xavfsizlik agentligi tomonidan Standartlar va texnologiyalar milliy instituti (NIST) bilan hamkorlikda ishlab chiqilgan va 1995-yilda FIPS PUB 180-1 standarti orqali e’lon qilingan. 2005-yil yanvarda V.Rijmen va E.Oswald tomonidan kam raundli (53 ta) SHA-1 xesh-funksiya algoritmi uchun kolliziya topish qiyinchiligi maksimum 280 ta hisoblash amalini talab etuvchi hujum mavjudligi e’lon qilindi. 2005-yil fevral oyiga kelib esa, X.Wang, L.Yin va H.Yu tomonidan to‘liq raundli (80 ta) SHA-1 xesh-funksiya algoritmi uchun kolliziya topish qiyinchiligi maksimum 269 ta hisoblash amalini talab etuvchi differensial kriptotahlil usuliga asoslangan hujum taklif etildi. 2005-yil avgust oyida bo‘lib o‘tgan CRYPTO-2005 konferensiyasida yuqoridagi mualliflar tomonidan ushbu hujum yanada mukammallashtirib (263 ta amal talab etuvchi) taqdim etiladi. ASIACRYPT-2006 konferensiyasida K.Kanyer va K.Rexberg tomonidan 64 raundli SHA-1 xesh-funksiya algoritmiga ikkita blok uchun kolliziya topish qiyinchiligi o‘rtacha 235 ta hisoblash amalini talab etuvchi hujum taklif etildi.

SHA-2 (SHA-256, SHA-384, SHA-512) – xesh-funksiyasi FIPS PUB 180-2 standarti orqali 2002-yilda e’lon qilingan. 2007-yilda xind mutaxassislari S.Kumar va P.Sarkar tomonidan SHA-2 xesh-funksiya algoritmining dastlabki hujum natijalari e’lon qilindi. Ushbu hujumning to‘liq bayoni keltirilmagan va u orqali kolliziya topish ehtimolligi 2-5, 2-9 bo‘lib, 22 raundli SHA-256 va SHA-512 xesh-funksiyalarga

qaratilgan. 2008-yilga kelib Y.Sasaki, L.Wang va K.Aoki tomonidan 41 raundli SHA-256 va 46 raundli SHA-512 xesh-funksiya algoritmlariga mos ravishda 2249 va 2497 ta amal talab etuvchi namunaviy matn topishga (Preimage Attacks) asoslangan yangi hujum taklif etildi. Shuningdek, M.Lamberger va F.Mendel tomonidan ham 46 raundli SHA-512 xesh-funksiya algoritmi uchun 246 ta hisoblash amalini talab etuvchi differensial kriptotahlil usuliga asoslangan sohta-kolliziya topish (pseudo-collision attack) hujumi taklif etildi.

Shu tariqa SHA-1 va SHA-2 xesh-funksiya algoritmlarining nazariy bardoshligi keskin tushgan. Mazkur algoritmlarga qo‘llanilgan ko‘plab hujum usullari to‘liq ochilmaganligiga va ularning nazariy ahamiyat kasb etishiga qaramay, 2007-yil noyabr oyiga kelib NIST yangi SHA-3 (FIPS PUB 180-3) standart xesh-funksiya avlodini tanlash va qabul qilishga qaratilgan loyiha (tanlov) boshlanganini e’lon qiladi. Shuningdek, 2010-yildan so‘ng SHA-1 algoritmi ERI va kolliziyaga bardoshliligi talab etilgan boshqa turli ilovalar tarkibida foydalanish mumkin emasligi ham ma’lum qilinadi. Mazkur tanlov 2007-2012-yillar davomida uch bosqichda olib borildi. Tanlovda qatnashuvchi ishtirokchilarning arizalari 2008-yilning dekabr oyiga qadar qabul qilinib, taqdim etilgan 64 ta arizadan 51 tasi tanlovda qatnashish imkoniyatiga ega bo‘lgan. 2009-yil iyulda yakunlangan birinchi bosqich natijalariga ko‘ra, quyidagi 14 ta nomzod algoritm tanlab olindi: BLAKE, Blue Midnight Wish, CubeHash, ECHO, Fugue, Grøstl, Hamsi, JH, Keccak, Luffa, Shabal, SHAvite-3, SIMD, Skein. 2010-yil 9-dekabrda yakunlangan ikkinchi bosqich natijalariga ko‘ra esa, quyidagi 5 ta nomzod algoritm final bosqichi uchun tanlab olindi: Blake, Grostl, JH, Keccak va Skein. 2012-yil yakuniga qadar davom etgan final bosqichi natijasida GUBKA (Sponge) iterativ-prinsipiga asoslangan Keccak xesh-funksiya algoritmi tanlov g‘olibi sifatida e’lon qilindi. Keccak algoritmi g‘olib bo‘lishiga qaramay, final bosqichining barcha ishtirokchi xesh-funksiyalari yetarlicha kriptobardoshlikka ega va turli talablarni qanoatlantirishi bo‘yicha bir-biridan kam bo‘lmagan algoritmlar ekanligi aniqlangan. Keccak algoritmi esa, qolgan nomzodlar orasida asosan apparat realizatsiyasi eng yaxshi bo‘lgan algoritm hisoblanadi.

SHA-3 – xesh-funksiyasi Italiya va Belgiya mutaxassislari Guido Bertoni, Joan Daemen, Gilles Van Assche, Michaël Peeters tomonidan ishlab chiqilgan Keccak algoritmiga asoslangan. Mazkur xesh-funksiya “SHA-3 tanlovi” doirasida turli mutaxassislar tomonidan chuqur tahlil qilingan, biroq samarador bo‘lgan hujum turi taklif etilmagan. Jumladan, 8 raundli algoritm uchun 2511,5 ta amalni talab etuvchi ikkinchi namunaviy matnni topish (second preimage attack) hujum turi, ishda 8 raundli algoritm uchun 2491,47 ta amalni talab etuvchi farqlash hujum turi (distinguishing attack), to‘liq raundli (24 ta) algoritm uchun 21579 ta amalni talab etuvchi farqlash hujum turi taklif etilgan. Kam raundli Keccak algoritmining turli versiyalariga qarshi kolliziya aniqlash uchun ichki differensial kriptotahlilga (internal differential attack) asoslangan hujum taklif etilgan. Ushbu hujum uch raundli Keccak-384 va Keccak-512, to‘rt raundli Keccak-384 va besh raundli Keccak-256 algoritmlari uchun ishlab chiqilib, to‘rt raund uchun hujumni amalga oshirish qiyinchiligi tug‘ilgan kunlar paradoksi hujumi qiyinchiligidan 245 martaga kam bo‘lgan. 3, 4, 6, 7 va 8 raundli Keccak-512 algoritmiga qarshi namunaviy matn topishga qaratilgan va mos ravishda 2505,2, 2505,3, 2506, 2507 va 2511,5 ta hisoblash amalini talab etuvchi hujum taklif etilgan. Shuningdek, 3 va 4 raundli Keccak-512 algoritmiga qarshi 2506 ta hisoblash amalini talab etuvchi hujum, 2 raundli Keccak-512 algoritmiga qarshi differensial kriptotahlil usuliga asoslangan va 2503,7 ta hisoblash amalini talab etuvchi namunaviy matn topish va 4 raundli Keccak-512 algoritmiga qisman namunaviy matn topish hujum turlari taklif etilgan.

O’tkazilgan tahlillar natijalari shuni ko‘rsatadiki, to‘liq raundli SHA-3 algoritmga nisbatan taklif etilgan hujumning 21600 (maksimal nazariy bardoshlilik qiyinchiligi) ta hisoblash amalidan kam bo‘lishiga qaramay, uni ma’lum bir vaqt davomida amalga oshirish imkoni umuman mavjud emas.

Xulosa. Mazkur maqolada SHA (Secure Hash Algorithm) oilasi, Amerika Qo‘shma Shtatlari Milliy

Standartlar va Texnologiyalar Instituti (NIST) tomonidan ishlab chiqilgan va keng qo‘llaniladigan bir qator kriptografik hash funksiyalari to‘plamlari haqida, shuningdek ushbu oilaga mansub xesh funksiya algoritmlari va ularning qadamlari ketma-ketligi, shuningdek, SHA-3 algoritmi uchun o‘tkazilgan tanlov haqida ma’lumotlar, shuningdek, SHA-1, SHA-2, SHA-3 algoritmlariga nisbatan o‘tkazilgan kriptotahlil matijalari keltirilgan. Har bir algoritmning maqsadi, ixtiyoriy uzunlikdagi ma’lumotlarni qisqa, fiksirlangan uzunlikdagi xesh qiymatiga aylantirish kabi asosiy natijalari tahlil qilingan.

Keyingi tadqiqotlarda kriptotahlil usullarining xesh funksiyalarga nisbatan qo‘llanilishi bo’yicha tahlillar natijalarini keltirish ko’zda tutilgan.

Foydalanilgan adabiyotlar

1. Raxmatullayevich R. I. OQIMLI SHIFRLASH ALGORITMLARI TAHLILI //Новости образования: исследование в XXI веке. – 2023. – Т. 1. – №. 6. – С. 889-893.
2. 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.
3. 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.
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. 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.
6. Rakhmatullaev I. Self-synchronizing (asynchronous) Stream Encryption Algorithms //Scientific Collection «InterConf». – 2023. – №. 164. – С. 249-254.
7. 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.
8. Boyquziyev I., Saydullayev E., Rahmatullayev I. ELLIPTIK EGRI CHIZIQLARNING KRIPTOGRAFIYADA QO ‘LLANILISHI //DIGITAL TRANSFORMATION AND ARTIFICIAL INTELLIGENCE. – 2024. – Т. 2. – №. 1. – С. 71-76.
9. Rakhmatullaev I. Evaluation of new NSA stream encryption algorithm by integrated cryptanalysis method //Scientific Collection «InterConf». – 2023. – №. 164. – С. 242-248.
10. 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.