XESH FUNKSIYASIYALAR VA ULARNING KRIPTOGRAFIYADA QO‘LLASH

Muqumov Dadaxon Maqsudovich
Anvarov Sharofidin Sobitali o‘g‘li
Mudofaa vazirligi MA

Annotatsiya: Xesh funksiyalari kriptologiyaga yetmishinchi yillarning oxirida kiritilgan. Ular ma’lumotlar yaxlitligini himoya qilishda vosita sifatida ishlatiladi. Tez orada ular kompyuter tarmoqlari va telekommunikatsiyalardagi boshqa xavfsizlik masalalarini hal qilish uchun juda foydali ekanligi ayon bo‘ldi. Kriptografik xesh funktsiyasi matematik tushuncha bo‘lib, asosan raqamli imzo sxemalarining bir qismi sifatida ishlatiladi.

Abstract: Hash functions were introduced to cryptology in the late seventies. They are used as a tool to protect data integrity. It soon became clear that they were very useful for solving other security problems in computer networks and telecommunications. A cryptographic hash function is a mathematical concept mainly used as part of digital signature schemes.

Tayanch so‘zlar: xesh qiymat, imzoni shakllantirish, imzoni tekshirish, rad etish, yaxlitlilik, blokli shifrlash, kalitli xesh, kalitlisiz xesh.

Kirish

Ushbu maqolada biz xesh funksiyalari, ularning turlari, afzalliklari va kamchiliklari shuningdek, blokli shifrlardan tuzilgan xesh funktsiyalari, ularga qo‘yilgan talablar, ularning xususiyatlari, siqish funksiyalari, kriptografiya, kriptografik xesh funktsiyalari hamda ularni ERI *(elektron raqamli imzo tizimlarida)* tizimlarida qo‘llash usullari haqida umumiy ma’lumot beramiz.

Xesh funksiyalari deb – ixtiyoriy uzunlikdagi ma’lumotlarni fiksirlangan uzunlikdagi H(M) qiymatga akslantiruvchi, bir tomonli funksiyaga aytiladi. Kirish qancha belgidan iborat bo‘lishidan qat’iy nazar, chiqish har doim o‘n oltilik (harflar va raqamlar) belgilar soni bo‘yicha bir xil bo‘ladi. Xeshlash funksiyasidan ma’lumotlar qismining haqiqiyligini ta’minlashda foydalaniladi, chunki xabardagi har qanday kichik o‘zgarish butunlay boshqa xesh qiymat qaytaradi.

Fiksirlangan qiymat deb – H(M) = {64,128,160,256,512} qiymatlardan biriga aytiladi. Xesh - funksiyalar zamonaviy kriptografiyaning asosiy vositalari bo‘lib, ular axborot xavfsizligida tranzaktsiyalar, xabarlar va raqamli imzolarni autentifikatsiya qilish uchun foydalaniladi. Xabarlar xeshlaganda, fayl yoki istalgan hajmdagi xabarni oladi, uni matematik algoritm orqali boshqaradi va belgilangan uzunlikdagi chiqish qiymatini qaytaradi.

Kirish xabari	Xesh funksiya	Natija (Xesh
CFI	MD5 (128-bit, 16-byte) 32 characters	3A10 0B15 B943 0B17 11F2 E38F 0593 9A9A
CFI	SHA-1 (160-bit, 20-byte) 40 characters	569D C9F0 7B48 7F58 9241 AD4C 5C28 7DA0 A448 8D08
CFI	SHA-256 (256-bit, 32-byte) 64 characters	F3ED 0867 48FF 3641 3091 0BB6 6293 7080 2958 B5A2 52AF F364 1FC5 07FD E80D 9929

1-rasm - Xesh funksiyalari orqali ma’lumotni xeshlashdan olingan natijalar.

Xesh funksiyalar yaratilishiga ko‘ra ikkiga bo‘linadi:

1) Kalitli;

2) Kalitsiz

Kalitli xesh funksiya - simmetrik kalitli tizimlarda ishlatiladi. Simmetrik kalitli tizim, kriptografiyada ishlatiladigan bir tizim bo‘lib. Bu tizimda, shifrlash va shifrni ochish uchun bir xil kalitdan foydalaniladi. Bu tizimning o‘ziga yarasha afzalliklari va kamchiliklari mavjud.

Simmetrik kalitli tizimning asosiy xususiyatlari quyidagilardir:

- Shifrlash va shifrni ochish uchun bir xil kalit ishlatiladi;
- Simmetrik kalitli tizimlar, asimmetrik kalitli tizimlarga nisbatan ancha tez ishlaydi;
- Kalit maxfiy saqlanishi kerak, ushbu kalit bilan shifrlangan ma’lumotlarni ochishda ishlatiladi.

Simmetrik kalitli tizimning kamchiliklari quyidagilardir:

- Kalitni maxfiy saqlash va uni to‘g‘ri shaklda tarqatish juda muhimdir;
- Har bir foydalanuvchi uchun alohida kalit yaratish va uni maxfiy saqlash kerak bo‘ladi;

Simmetrik kalitli tizimlar, maxfiy yozishmalarni saqlash, bank tranzaktsiyalarining xavfsizligini ta’minlash, internet xizmatlarini himoyalash va boshqa maqsadlar uchun ishlatiladi.

Kalitsiz xesh funksiyalar – bu qo‘shimcha vositalar (elektron raqamli imzo va h.k) yordamida ma’lumotlarning to‘laligini kafolatlaydi.

Kalitsiz xesh funksiyalar, ma’lumotlarning to’liq va o’zgarmasligini kafolatlash uchun qo‘llaniladi. Elektron raqamli imzolar, blok zanjiri (blockchain) va boshqa axborot xavfsizligi sohalarida juda muhimdir. Elektron raqamli imzo, ma’lumotlarni elektron shaklda imzolash uchun ishlatiladi. Bu imzolar, ma’lumotlarning o’zgarmasligini va imzo egasi tomonidan tasdiqlanganligini kafolatlaydi. Zamonaviy kriptografiya sohasida xesh-funksiyalar raqamli aloqani ta’minlash, ma’lumotlar yaxlitligini ta’minlash va raqamli imzolarni yaratishda hal qiluvchi rol o‘ynaydi.

Har bir ishlab chiqilgan elektron hujjatni ishlab chiquvchi o‘z imzosi bilan imzolashi hamda ikkinchi tomon ushbu hujjatning ishlab chiquvchi tomonidan imzolanganini tekshirish quyidagi ikki jarayondan iborat (10.1, 10.2 - rasmlar):

- ERIni shakllantirish;
- ERI haqiqiyligini tekshirish.

Imzoni shakllantirish jarayoni. Boshlang‘ich ma’lumotlar sifatida: M imzolanuvchi ma’lumot, foydalanilgan elliptik chiziq parametrlari va imzo uchun maxfiy kaliti. Ushbu algoritm uchun elliptik egri chiziq tenglamasi $p > 2^{255}$ shartni qanoatlantiruvchi tub xarakteristikali Fp maydonda deb olinishi shart. Qo‘yilgan imzo (r,s) ga teng bo‘ladi.

Imzoni hosil qilish bosqichlari

a. $1< k< n-1$ oraliqdagi ixtiyoriy k soni tanlanadi (bu erda n soni G nuqta tartibi va $2^{254} < n < 2^{256}$ shartni qanoatlantiruvchi butunison).

b. (x1,y1) = [k]G hisoblanadi.

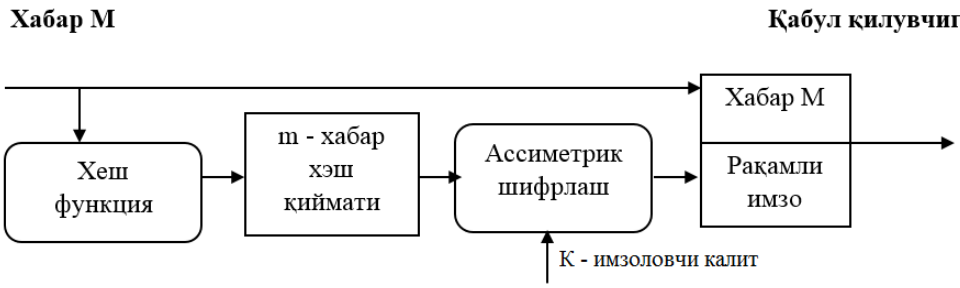
c. $r=x_1 \bmod n$ hisoblanadi. Agar r=0 ga teng bo‘lsa, 1-qadamga qaytib, k soni qaytadan tanlanadi.

d. Imzolanuvchi M ma’lumotning xesh xesh qiymatini hisoblanadi, ya’ni e=H(M). Agar H(M) mod n=0 ga teng bo‘lsa, H(M) mod n=1 shart olinadi.

e. $0< d <n$ oraliqdan tanlangan d maxfiy kalit asosida $s=(dr+ke) \bmod n$ kattalik hisoblanadi.

f. Agar s=0 ga teng bo‘lsa, 1-qadamga qaytiladi va boshqa k soni tanlanadi.

g. Hosil qilingan (r,s) sonlar jufti M ma’lumot uchun elektron raqamli imzo hisoblanadi.



10.1- rasm. Elektron raqamli imzoni shakllantirish jarayoni

Imzoni tekshirish jarayoni. Imzoni tekshirish qabul qilingan M’ ochiq malumot va imzo (r’, s’) asosida amalga oshiriladi.

a. Agar $1 < r’, s’ < n-1$ shart bajarilmasa, imzo qalbaki deb topiladi va tekshirish to‘xtatiladi.

b. e= H(M’) ma’lumotning xesh qiymati hisoblanadi.

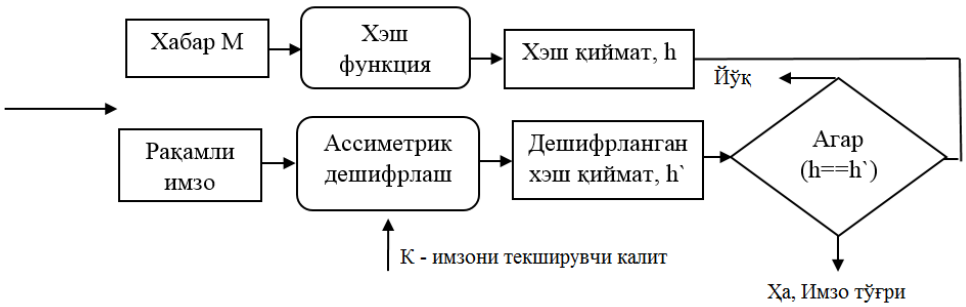
c. w= $H(M')^{(n-2)}$mod n kattalik hisoblanadi.

d. u_1 = s’ w mod q kattalik hisoblanadi.

e. u_2 = (n-r’) w mod n kattalik hisoblanadi.

f. X=[u_1] G+[u_2] Q=(x_1,y_1) kattalik hisobalanadi.

g. Agar x1 mod n = r’ ga teng bo‘lsa, qo‘yilgan imzo haqiqiy, aks holda qalbaki deb topiladi



10.2 - rasm. Elektron raqamli imzoni tekshirish jarayoni

Xesh funksiyalar bundan tashqari blok zanjirida ham keng qo‘llaniladi. Blok zanjiri, ma’lumotlarni o’zgarmas va o‘zaro bog‘liq bloklarda saqlaydi. Har bir blok, oldingi blokning xesh qiymatini saqlaydi, bu esa ma’lumotlarning o‘zgarmasligini kafolatlaydi. Shunday qilib, kalitsiz xesh funksiyalar, ma’lumotlarning to‘liq va o‘zgarmasligini kafolatlashda muhim ahamiyatga ega.

Siqish funksiyalari

Kriptografik xesh funktsiyasi blokli shifrdan iborat. Blok shifrlash xesh funksiyalari Message Digest(MD) va Secure Hash Algoritms(SHA) algoritmlari hisoblanadi.

Message Digest(MD) algoritmi - barcha MD xesh algoritmlari Ron Rivest tomonidan ishlab chiqilgan. MD xesh algoritmlarining MD2, MD4 va MD5 oilalari mavjud.

Secure Hash Algoritms(SHA) algoritmi - xavfsiz xesh algoritmlari Secure Hash Standard (SHS) deb nomlanadi. U Milliy Standartlar va Texnologiyalar Instituti (NIST) tomonidan ishlab chiqilgan. SHA-0 algoritmi xabarni oladi va uni 160 bitli blokga ajratadi. Bu kuchli to‘qnashuvga chidamli emas deb topilgan. SHA-1 160 bitli xesh funksiyasi bo‘lib, MD5 algoritmiga o‘xshaydi. SHA-256 algoritmi berilgan xabarni 512 bitli bloklarga ajratadi va 256 bitli xabar dayjestini yaratadi. SHA-512 algoritmida xabar 1024 bitli bloklarga bo‘linadi va 256 bitli xabarlar dayjestini yaratadi. MD5 va SHA algoritmlarni blok o‘lchami, kalit uzunligi, kriptoanaliz, iteratsiyalar va jami qadamlar kabi ba’zi asosiy parametrlar yordamida solishtirish mumkin.

SHA algoritmi MD5 ga qaraganda ancha xavfsizroq hisoblanadi, chunki u asl xabarni topish uchun 2 ^ 160 bit operatsiyalarni talab qiladi, MD5 esa 2 ^ 128 bit operatsiyalarni talab qiladi. SHA-da xabarlar digestining uzunligi 160 bit, MD5-da bo‘lgani kabi 128 bit. MD5 SHA algoritmiga nisbatan tezroq, chunki u atigi 64 iteratsiyani talab qiladi, SHA esa 80 iteratsiyani talab qiladi. Ikkala algoritm ham to‘ldirishga, barmoq iziga muhtoj va deyarli bir xil miqdordagi resurslardan foydalaniladi. Siqish funksiyasi blokli shifrdan foydalanishga asoslangan.

Blok shifr - bu shifrlangan matnni ishlab chiqarish uchun ma’lumotlarni shifrlash usuli bo‘lib, unda kriptografik kalit va algoritm ma’lumotlar blokiga bir vaqtning o‘zida bir bitga emas, balki bir vaqtning o‘zida guruh sifatida qo‘llaniladi. SHA xabarni oladi va uni 512 bitli bloklarga ajratadi va 512 bitli xabar dayjestini yaratadi. Bu boshqa algoritmlarga qaraganda, uning xabarlar biti nisbatan ko‘proq bo‘lganligi sababli, to‘qnashuvning yuzaga kelishi qiyin. Bu odatiy hujumlarga nisbatan ancha chidamli va ko‘proq xavfsizlikni ta’minlaydi.

Xesh funksiyalarga qo‘yiladigan umumiy talablar:

1) Ixtiyoriy uzunlikdagi matnga qo‘llay olishlik;

2) Chiqishda belgilangan uzunlikdagi qiymatni qaytarishi;

3) Ixtiyoriy berilgan X bo‘yicha H(X) hisoblanadi;

4) Ixtiyoriy berilgan h(xesh) bo‘yicha H(X) = h tenglikdan X (ma’lumot)ni topib bo‘lmaydi*(bir tomonlama xossasi)*;

5) X = Y ma’lumotlardan olingan xesh funksiyalar H(X) = x va H(Y) = y uchun x = y bo‘ladi. *(kolliziya bardoshlilik xossasi)*

Xesh-funksiya quyidagi xossalarga ega bo‘ladi:

1) Teskari funksiyaning mavjud emasligi;
2) Kollizia holatining yo‘qligi;
3) Determinanlanganlik;
4) Natijaning tasodifligi.

Kriptografiya - shaxsiy ma’lumotlarni xavfsiz uzatish va saqlash uchun ishlatiladigan usullarni o‘rganish sohasi. U shifrlash, xeshlash va steganografiya kabi jarayonlarni o‘z ichiga oladi. Kriptografiya bugungi kunda odamlar o‘zlarining shaxsiy hayotini himoya qilish uchun kriptografiyadan har kuni o‘zlari bilmagan holda (masalan, bank operatsiyalari, veb-saytga kirish va h.k.) foydalanadilar. Ilgari kriptografiya faqat xabarning maxfiyligi, ya’ni shifrlash bilan bog‘liq edi. Shifrlash - oddiy matnni (o‘qilishi mumkin bo‘lgan shakl) shifrlangan matnga (o‘qilmaydigan shakl) aylantirish jarayoni. Shifrni ochish shifrlangan matnni yana oddiy matnga aylantirish jarayonidir. Bir nechta kriptografik algoritmlar mavjud. Ammo shifrlash va shifrni ochish uchun ishlatiladigan kalitlar soniga asoslanib, kriptografik algoritmlar quyidagicha tasniflanadi:

Maxfiy kalit kriptografiyasi: shifrlash va shifrni ochish uchun bitta kalitdan foydalanganligi sababli simmetrik shifrlash deb ham ataladi. Asosan maxfiylik uchun ishlatiladi.

Ochiq kalitli kriptografiya: shifrlash uchun bitta kalitdan va shifrni ochish uchun boshqa kalitdan foydalanadi.

Foydalanilgan adabiyotlar:

1. Florian Mendel, Tomislav Nad, Martin Schlaffer (2013-05-28). Improving Local Collisions: New Attacks on Reduced SHA-256

2. Somitra Kumar Sanadhya; Palash Sarkar (2008-11-25). New Collision attacks against Up to 24-Step SHA-2. Indocrypt 2008

3. Информационная технология. Методы защиты информации. Хэш-функции. Часть 1.Общие положения {Information technology — Security techniques — Hash-functions —Part 1: General)

4. Информационные технологии. Методы защиты информации. Хэш-функции. Часть 4.

5. Kaliski B. RFC-1319 The MD2 Message-Digest Algorithm, 1992. http://www.ietf.org/rfc/rfc1319.txt.

6. Jones Eastlake. US Secure Hash Algorithm 1 (SHA1), 2001. http://www.ietf.org/rfc/rfc3174.txt.

7. https://allgosts.ru/35/040/gost_34.10-2018

8. Хэш-функции с применением арифметических операций над абсолютными значе1ниями чисел (Information technology — Security techniques — Hash-functions — Pari 4: Hash-functions using modular arithmetic)