TOSHKENT AMALIY FANLAR UNIVERSITETI

Ma’lumotlar tuzilmasi va algoritmlar fani

“Kompyuter injiniring” kafedrasi
Katta o’qituvchi Kendjayeva Dildora Xudayberganovna

14 - Ma’ruza

Xesh funksiya. Xesh funksiyalar turlari, Xesh funksiyalar qo‘llanilishi va axborot xavfsizligidagi o‘rni

Asosiy adabiyotlar:

1. Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2022). Introduction to algorithms. MIT press.
2. O. R. Yusupov, I. Q. Ximmatov, E. Sh. Eshonqulov. Algoritmlar va berilganlar strukturalari. Oliy o‘quv yurtlari uchun o‘quv qo‘llanma. – Samarqand: SamDU nashri. 2021-yil, 204 bet.
3. Xayitmatov O’.T., Inogomjonov E.E., Sharipov B.A., Ruzmetova N., Ma'lumotlar tuzilmasi va algoritmlari fanidan o’quv qo’llanma
4. Rahimboboeva D. "Ma'lumotlar tuzilmasi va algoritmlari" fanidan o’quv qo’llanma – T.: TDIU, 2011.-135 bet.

MA’RUZA REJASI

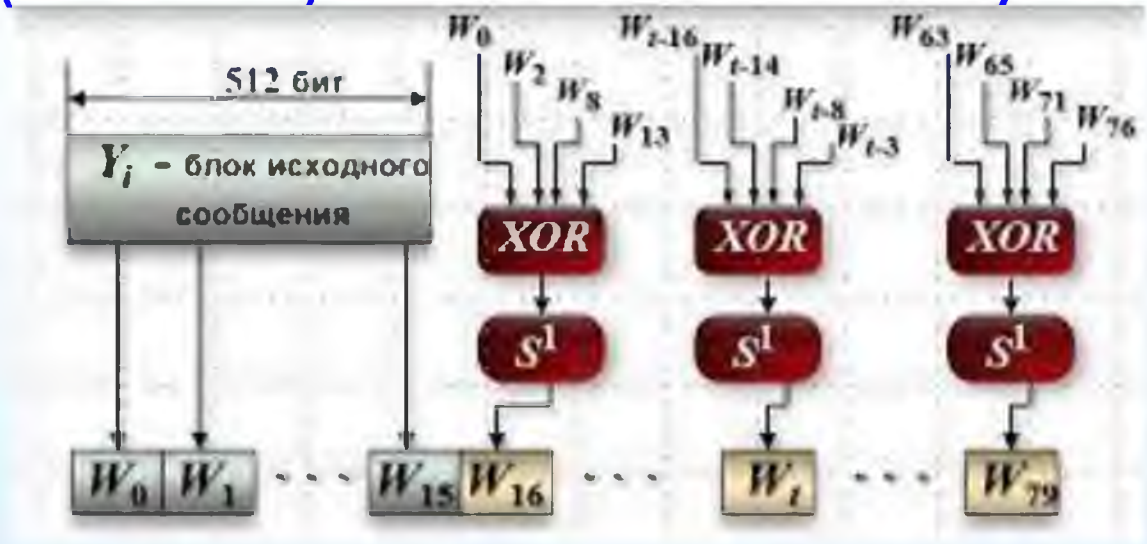
Xesh funksiya

Xesh funksiyalar turlari

Xesh funksiyalar qo'llanilishi va axborot xavfsizligidagi o‘rni

Xesh funksiya

- ***Xesh funksiyalar*** - ixtiyoriy uzunlikdagi kirish ma’lumotini chiqishda belgilangan uzunlikdagi xesh qiymatga aylantirib beruvchi bir tomonlama funksiyalarga aytiladi.
- ***Xesh funksiya*** - ixtiyoriy uzunlikdagi M-ma‘lumotni fiksirlangan uzunlikga siqish yoki ikkilik sanoq sistemasi ifodalangan ma‘lumotlarni fiksirlangan uzunlikdagi bitlar ko‘rinishidagi qandaydir kombinatsiyasi (svertkasi) deb ataluvchi funksiya.



Ta’rif

Xesh-funksiya deb, har qanday

$$h: X \to Y$$

oson hisoblanuvchi va $\forall M$ -ma’lumot uchun h(M) = H fiksirlangan uzunlikga ega bo‘lgan funksiyaga aytiladi.

Berilgan M-ma‘lumotning h(M) -xesh qiymatini topish uchun avvalo ma‘lumot biror «m» -uzunlikdagi bloklarga ajratilib chiqiladi. Agar M-ma’lumot uzunligi «m» -ga karrali bo‘lmasa, u holda oxirgi to‘lmay qolgan blok «m»- uzunlikga olindan kelishib olingan maxsus usulda biror simvol yoki belgi (masalan —”0” yoki —”1”) bilan to‘ldirilib chiqiladi. Natijada hosil qilingan M-ma‘lumot bloklariga:

$$M= \{ M_1, M_2 , \ldots, M_n\}$$

quyidagicha siqishni (svertkani) hisoblash protsedurasi qo‘llaniladi:

$$H_0 = v ,$$

$$H_i = f (M_i , H_{i-1}) , i =1,2,..., n.$$

$h(M)= H_n$;

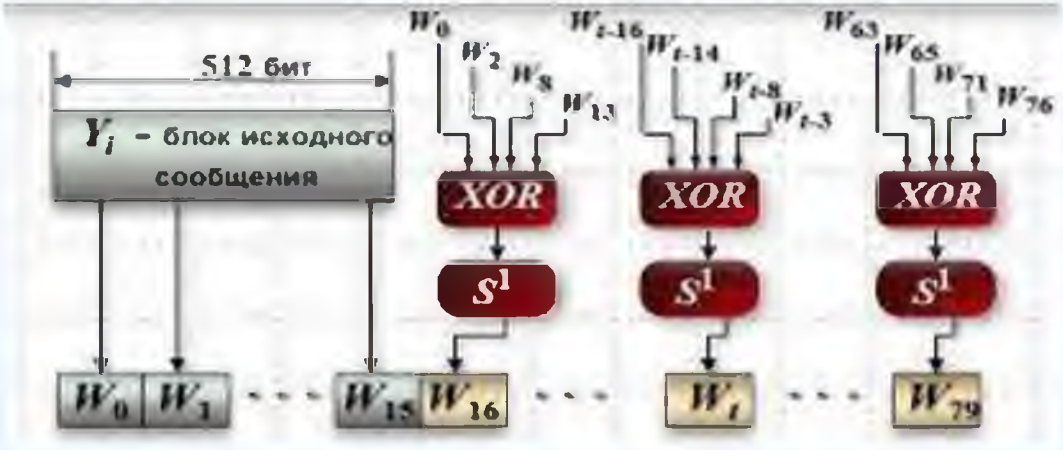
bu yerda v -qandaydir fiksirlangan boshlang‘ich vektor.

Xesh funksiyalar turlari

Oddiy xesh funksiyalar: Adler-32, CRC, FNV, Murmur2, PJW- 32, TTH, Jenkins hash.

Kriptografik xesh funksiyalar: CubeHash, BLAKE, BMW, ECHO, FSB, Fugue, Grostl, JH, Hamsi, HAVAL, Keccak (SHA-3), Kupyna, LM-хеш, Luffa, MD2, MD4, MD5, MD6, N-Hash, RIPEMD- 128, RIPEMD-160, RIPEMD-256, RIPEMD-320, SHA-1, SHA-2, SHABAL, SHAvite-3, SIMD, Skein, Snefru, SWIFFT, Tiger, Whirlpool, ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012.

Kalit hosil qiluvchi xesh funksiyalar: bcrypt, PBKDF2, scrypt.

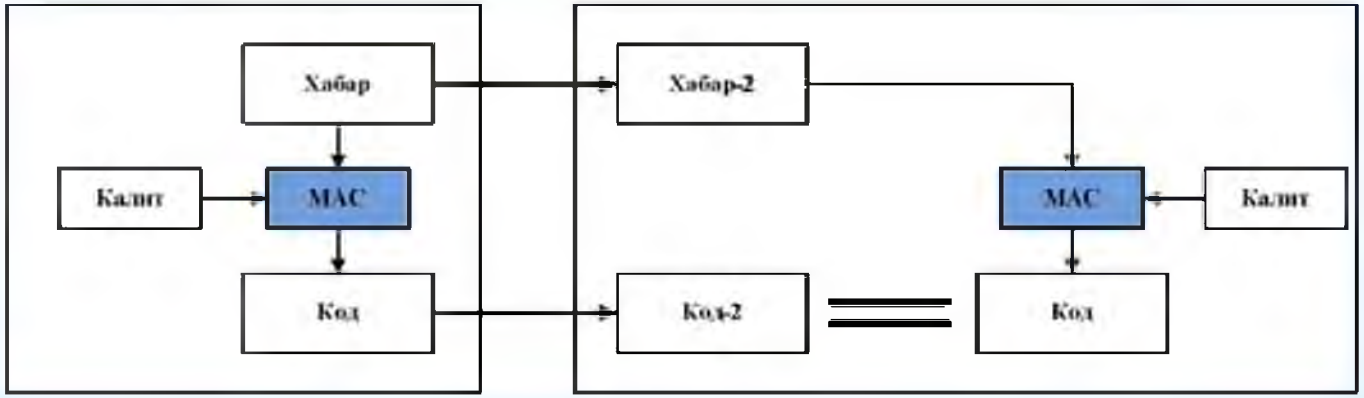


Xesh funksiyalar turlari

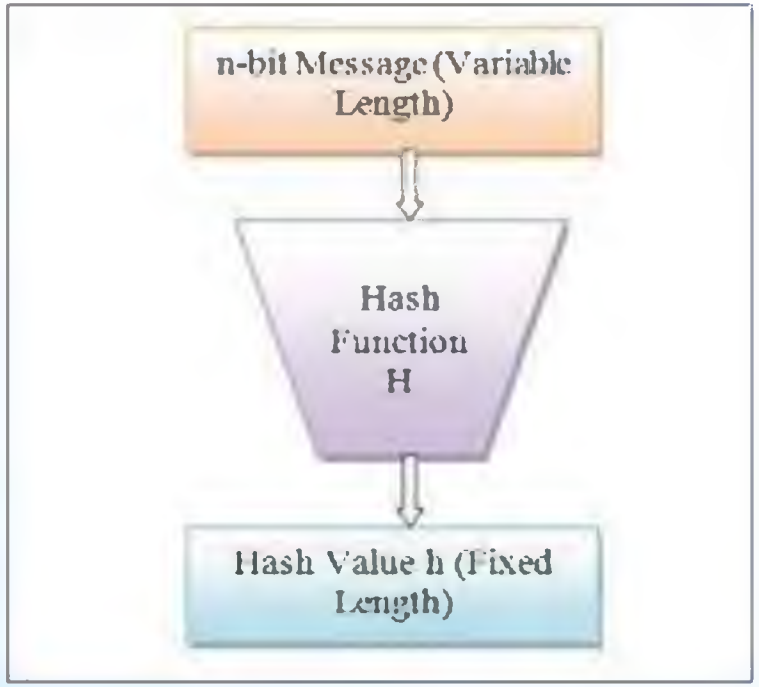
Kriptografik xesh funksiyalarning esa quyidagi turlari mavjud:

1) kalitli xesh funksiya; 2) kalitsiz xesh funksiya.

Kalitli xesh funksiyalar simmetrik shifrlash algoritmi tizimlarida qo‘llaniladi. Kalitli xesh funksiyalar ***berilgan ma’lumot autentifikatsiyasi kodi*** (message authentication code(***MAC***)) deb ham yuritiladi.



Xesh funksiyalar turlari



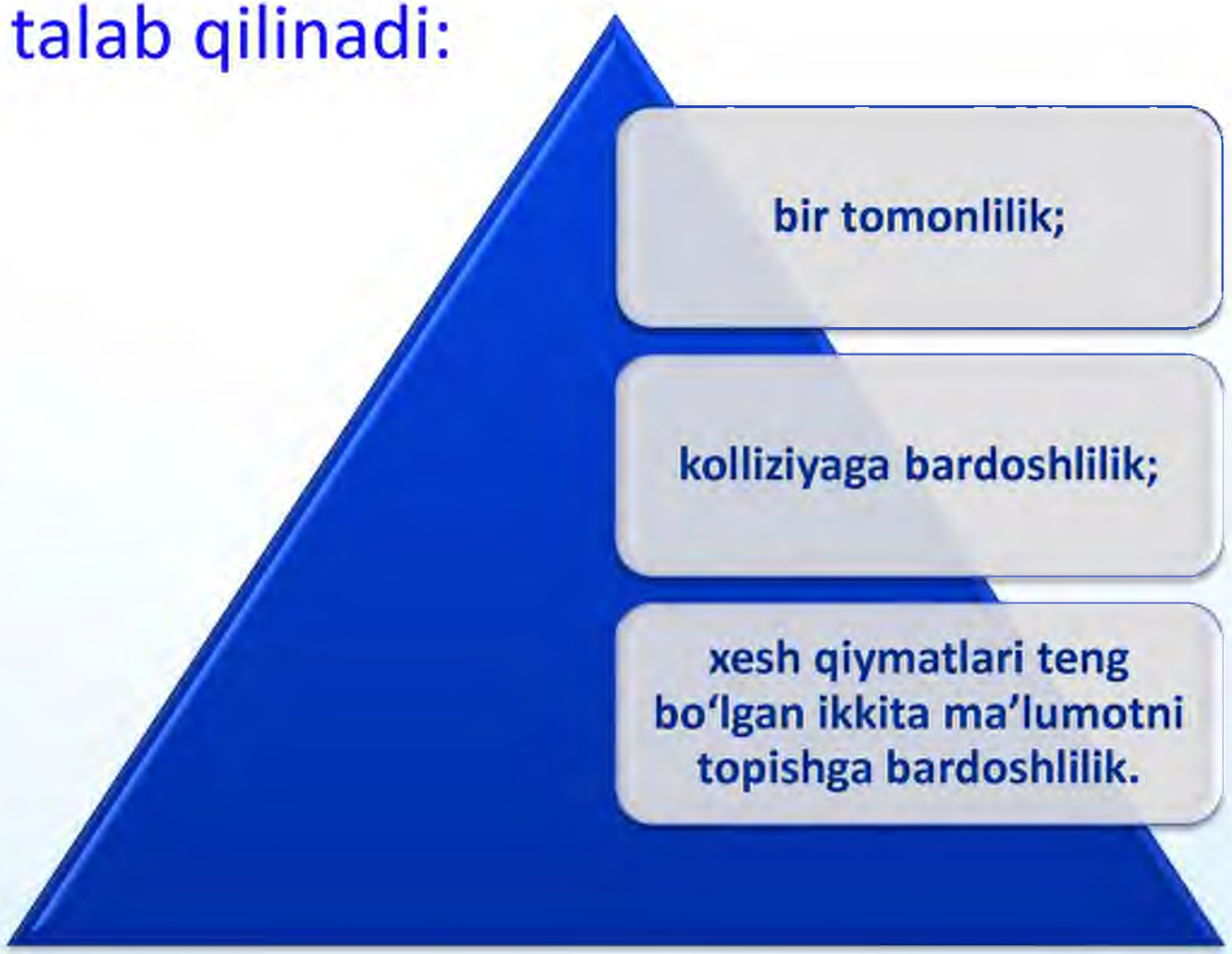
Kalitsiz xesh funksiyalar ***xatolarni topish kodi*** (modification detection code(***MDC***) yoki manipulation detection code, massage integrrity code(***MIC***) deb ataladi.

Ushbu kod qo‘shimcha vositalar (masalan: himoyalangan aloqa tarmog‘i, shifrlash yoki ERI algoritmlari) yordamida berilgan ma’lumot to‘laligini kafolatlaydi.

Bu turdagi xesh funksiyalardan bir-biriga ishonch bildiruvchi va ishonchi bo‘lmagan tomonlar foydalanishlari mumkin.

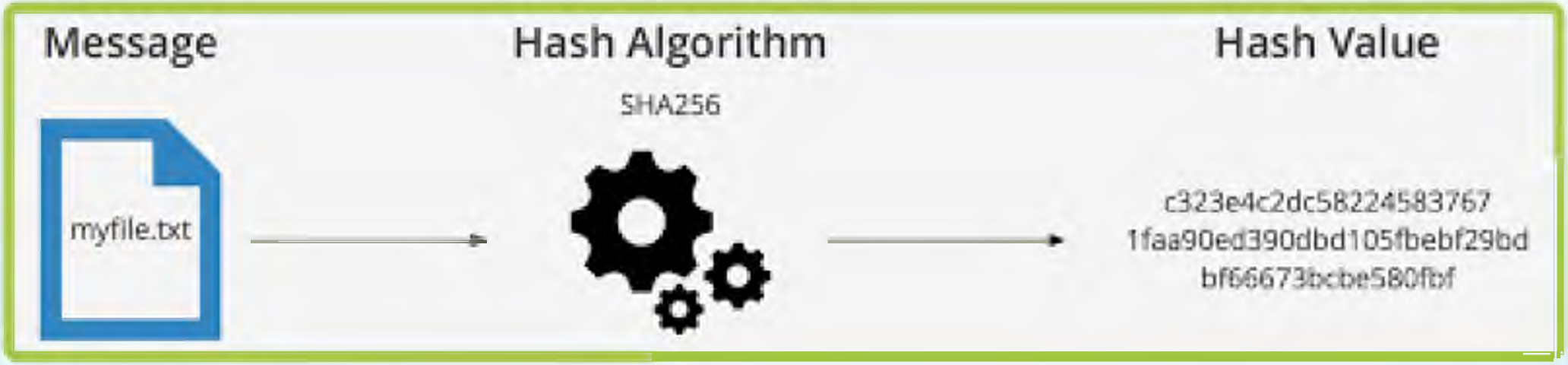
Xesh funksiyalar turlari

Odatda kalitsiz xesh funksiyalardan quyidagi xossalarni qanoatlantirishi talab qilinadi:

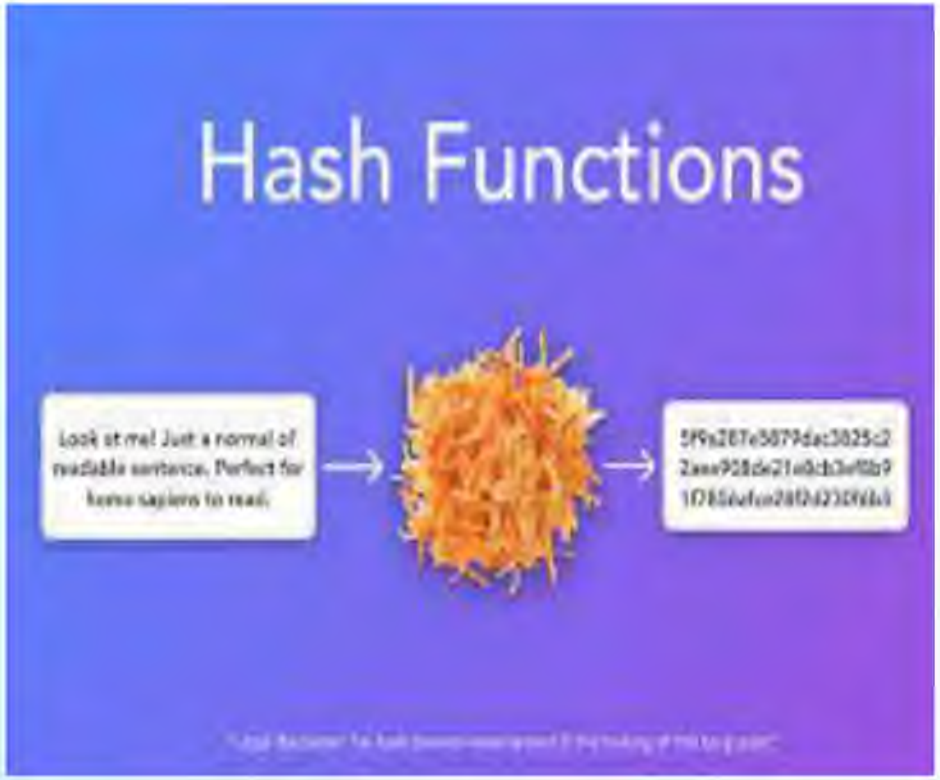


Xesh funksiyalar turlari

Ma’lumotlarni uzatishda yoki saqlashda ularning to‘laligini nazoratlashda har bir ma’lumotning xesh qiymati (bu xesh qiymat ma’lumotni autentifikatsiya qilish kodi yoki “imitoqo‘yish”-ma’lumot bloklari bilan bog‘liq bo‘lgan qo‘shimcha kiritilgan belgi deyiladi) hisoblaniladi va bu qiymat ma’lumot bilan birga saqlaniladi yoki uzatiladi.



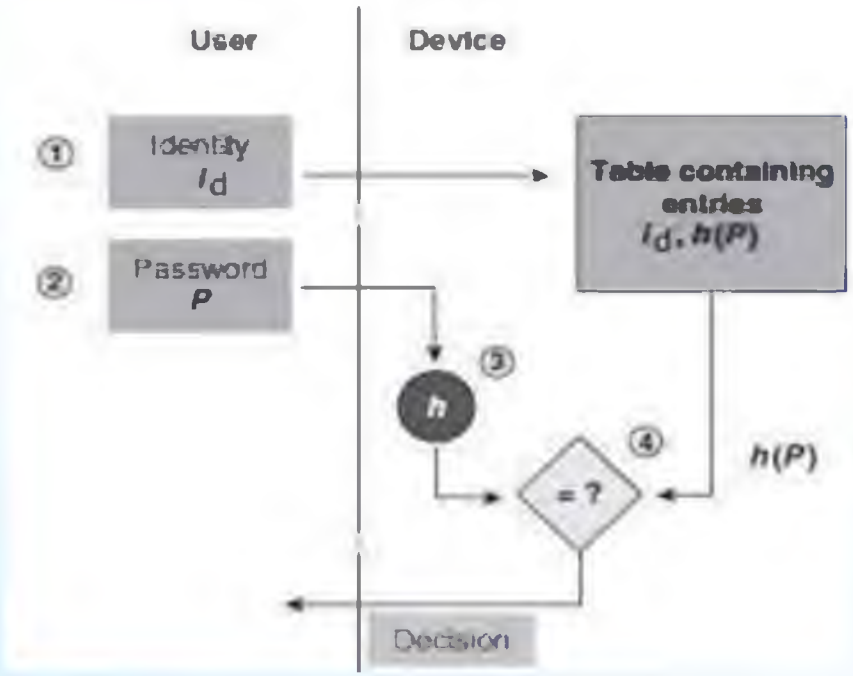
Xesh funksiyalar turlari



“Imitoqo‘yish”lar hosil qilish uchun foydalaniladigan xesh funksiyalar nazorat yig‘indisidan farqli ravishda ma’lumotni saqlash va uzatishda ro‘y beradigan tasodifiy xatolarni aniqlabgina qolmasdan, raqib tomonidan qilingan aktiv hujumlar to‘g‘risida ham ogohlantiradi.

Buzg‘unchi xesh qiymatni osonlik bilan o‘zi hisoblab topa olmasligi va muvaffaqiyatli imitatsiya qilishi yoki ma’lumotni o‘zgartira olmasligi uchun xesh funksiya 70 buzg‘unchiga ma’lum bo‘lmagan maxfiy kalitga ega bo‘lishi kerak.

Xesh funksiyalar turlari



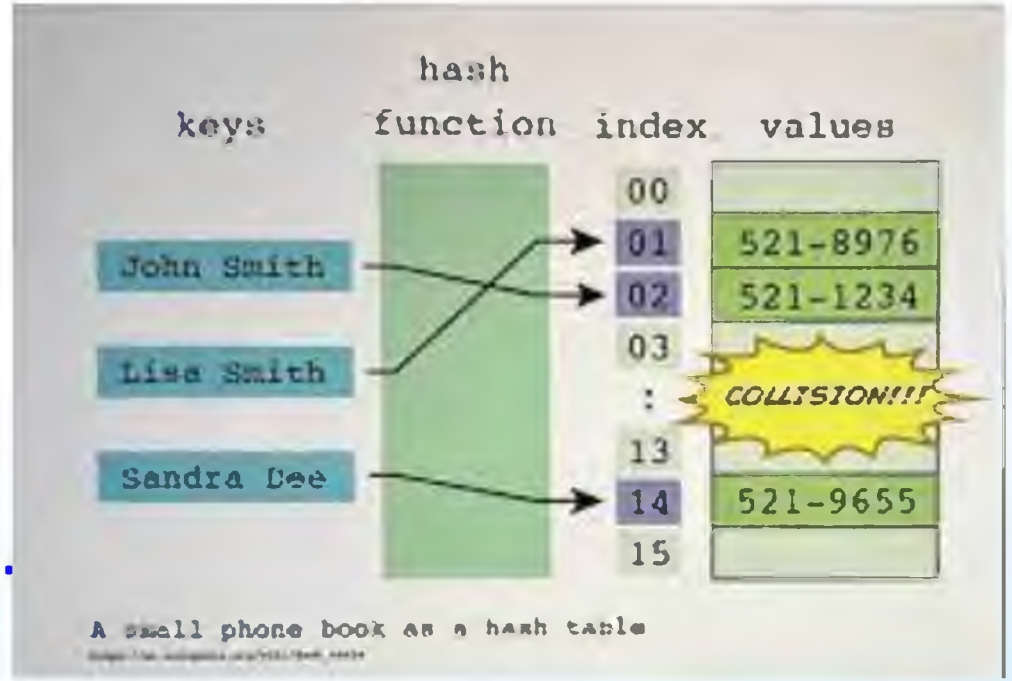
Ma’lumot manbaining autentifikatsiyalash masalasi axborot-kommunikatsiya tizimlarining bir-biriga ishonmaydigan ikki tomoni orasida ma’lumot almashinuvida yuzaga keladi.

Bu masalani hal qilishda ikkala tomon ham biladigan maxfiy kalitdan foydalanib bo‘lmaydi.

Bu holatda ma’lumotning manbaini autentifikatsiya qilishga imkon beradigan elektron raqamli imzo sxemasi qo‘llaniladi.

Xesh funksiyalar turlari

- Agar bir xil xesh qiymatga ega bo‘lgan ikkita har xil ma’lumot mavjud bo‘lsa, bu ma’lumotlar jufti kolliziya hosil qiladi deyiladi.
- ***Xesh funksiyalarda kolliziya*** - ikkita har xil ma’lumotdan bir xil xesh qiymat hosil bo‘lib qolishi. Kolliziyaning oldini olish yo‘llaridan biri bu xesh jadval hisoblanadi. Xeshlash algoritmlarining bardoshliligi xa xavfsizliligi kolliziyaga chidamliligi bilan aniqlanadi.



Xesh funksiyalar qo'llanilishi va axborot xavfsizligidagi o‘rni

Xeshlash algoritmlarining zamonaviy kriptografiyadagi tutgan o‘rni juda muhimdir va undan hozirda keng ko‘lamda foydalaniladi.

Yangi xesh algoritmlar xam yaratilmoqda. Yangi xesh algoritmlar kolliziyaga bardoshli, xesh qiymatning tez hisob-kitob qila olishi va.h.k xususiyatlarga ega bo‘ladi.

Xesh funksiyalar asosan, Elektron raqamli imzo (ERI)da, Torrent, DC Hub, Operatsion sistemalarda va fayllarning butunliligini yoki o‘zgartirilganligini nazorat qilish uchun foydalaniladi.

Components of Hashing

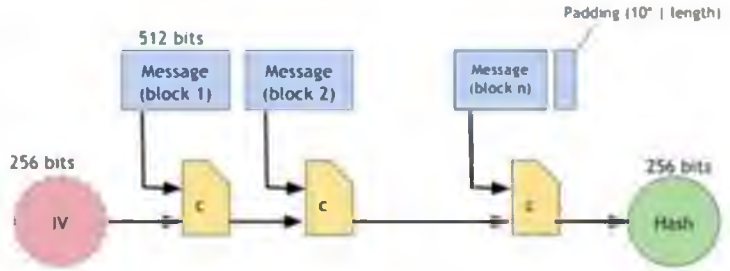
Xesh funksiyalar tahlili

	Xeshlanadigan matn uzunligi	Kirish blokining uzunligi	Xesh qiymat uzunligi	Har bir blokni xeshlash qadamlari soni
GOST R 34.11-94	Ixtiyoriy	256	256	19
MD 2	Ixtiyoriy	512	128	1598
MD 4	Ixtiyoriy	512	128	72
MD 5	Ixtiyoriy	512	128	88
SHA-1	$<2^{64}$	512	160	80

- **CRC32** (Cyclic redundancy check - Davriy kamchilikni tekshiruvchi kod) kompyuter qurilmalarida, ya‘ni tarmoq qurilmalari va doimiy xotiradagi ma‘lumotlarni xavfsizligini ta‘minlashda ya‘ni o‘zgartirilmaganligini doimiy ravishda tekshirib boradigan oddiy xesh funksiya hisoblanadi. CRC32 xalqaro standarti CRC32-IEEE 802.
- **MD4** xeshlash algoritmi RSA Data Security, Inc. Ronald L. Rivest tomonidan ishlab chiqilgan. MD4 aralashgan algoritm hisoblanadi, Endi ishonchsiz hisoblanadi.
- **MD5** xesh funksiyasi algoritmi Massachusets texnologiya instituti professori Ronald Rivest tomonidan 1992 yilda ishlab chiqilgan.

SHA-1 xesh funksiyasi algoritmi.

SHA-256	$<2^M$	512	256	64
SHA-384	$<2^{128}$	1024	384	80
SHA-512	$<2^{128}$	1024	512	80
STB 1176.1 - 99	Ixtiyoriy	256	142<L<256	77
O'z DSt 1106 : 2006	Ixtiyoriy	128,256	128, 256	16b+74, 16b+46, Bu erda b-bloklar soni



SHA-256 hash function

Kafolatlangan bardoshlilikka ega bo'lgan xeshlash algoritmi **SHA (Secure Hash Algorithm)** AQShning standartlar va texnologiyalar Milliy instituti (NIST) tomonidan ishlab chiqilgan bo'lib, 1992 yilda axborotni qayta ishlash federal standarti (RUB FIPS 180) ko'rinishida nashr qilindi.

Xesh qiymatni hisoblash jarayoni quyidagi bosqichlardan iborat:

1. 1-bosqich. To‘ldirish bitlarini qo‘shish.
2. 2-bosqich. Ma'lumotning uzunligini qo‘shish.
3. 3-bosqich. Xesh qiymat uchun bufer initsializatsiya qilish.
4. 4-bosqich. Ma'lumotni 512 bitlik bloklarga ajratib qayta ishlash.
5. 5- bosqich. Natija.

Mavzu yuzasidan savollar:

1. Xesh funksiya tushunchasiga ta‘rif bering.
2. Kriptografik xesh funksiyalarga misol keltiring
3. Xesh funksiyalarning yana qanday turlarini bilasiz
4. Kalit hosil qiluvchi xesh funksiyalarni keltiring

Do you have any questions?