AXBOROTLARNI HIMOYALASHDA QO’LLANILADIGAN HESHLASH ALGORITMINING TAHLILI

Seytniyazov Davronbek Bayramovich
tayanch doktorant
Atamuratova Shaxsanem Turdimuratovna
talaba
Dauletmuratova Juldiz Ayapbergenovna
talaba
Jumaniyazova Ulbosin Polatbay qizi
talaba

Heshlash axborot xavfsizligi sohasida juda muhim texnologiya bo’lib hisoblanadi. Hesh funktsiyalari o’zgaruvchan uzunlikdagi ma’lumotlarni hesh qiymati yoki nazorat summasi deb ataladigan qat’iy uzunlikka ega bo’lgan satrga aylantirish uchun ishlatiladi. Bu bizga ma’lumotlarning yaxlitligini tezda tekshirish imkonini beradi, chunki dastlabki ma’lumotlarning kichik o’zgarishi ham hesh qiymatining sezilarli o’zgarishiga olib keladi.

Eng keng tarqalgan hesh algoritmlaridan biri bu SHA (Secure Hash Algoritm). SHA - bu AQSh Milliy standartlar va texnologiyalar instituti (NIST) tomonidan ishlab chiqilgan kriptografik hesh-funksiyalar oilasi bo’lib hisoblanadi. SHA-ning SHA-1, SHA-2 va SHA-3 kabi bir nechta versiyalari mavjud bo’lib, ularning har biri o’ziga hos hesh qiymati uzunligini ta’minlaydi.

SHA-1 1995 yilda ishlab chiqilgan va 160 bit hesh qiymatiga ega. Biroq, 2005 yilda SHA-1da soxta ma’lumotlar uchun ishlatilishi mumkin bo’lgan jiddiy zaifliklar aniqlandi. Hozirgi vaqtda SHA-2 yoki SHA-3 kabi xavfsizroq algoritmlardan foydalanish tavsiya etiladi.

SHA-2 - bu 2001 yilda ishlab chiqilgan kriptografik hesh-funktsiyalar oilasi. SHA-2 SHA-224, SHA-256, SHA-384 va SHA-512 kabi bir nechta hesh uzunlikdagi algoritmlarni o’z ichiga oladi. Eng keng tarqalgan SHA-256 va SHA 512 algoritmlari bo’lib hisoblanadi.

SHA-256 32 bitli so’zlardan foydalanadi va 256 bit hesh qiymatiga ega. SHA 512 64 bitli so’zlardan foydalanadi va 512 bit hesh qiymatiga ega. Ikkala algoritm ham hujumlarga, jumladan, kunduzgi hujumlarga va to’qnashuvni tanlash hujumlariga yuqori qarshilik ko’rsatadi.

SHA-3 kriptografik heshlash funksiyalarining SHA oilasining so’nggi versiyasidir. U 2015 yilda NIST standarti sifatida tanlangan va hesh uzunligi 224, 256, 384 yoki 512 bitga ega. SHA-3 yangi heshlash standartini tanlash uchun NIST tomonidan o’tkazilgan tanlovdan so’ng tanlangan Keccak algoritmidan foydalanadi.

Heshlash turli sohalarda, jumladan, axborot xavfsizligi, raqamli imzo, autentifikatsiya va ma’lumotlar yaxlitligida keng qo’llaniladi. Misol uchun, ma’lumotlar

bazasida foydalanuvchi parollarini saqlashda parol odatda aniq saqlanmaydi, lekin tegishli foydalanuvchi identifikatori bilan birga heshlanadi va saqlanadi. Foydalanuvchi o’z parolini kiritganda, kiritilgan parolning haqiqiyligini tekshirish uchun uning hesh qiymati saqlangan hesh qiymati bilan taqqoslanadi.

Hesh funksiyalari kriptografiyada raqamli imzolarni yaratish uchun ham qo’llaniladi. Raqamli imzo - bu xabarning autentifikatsiyasi, yaxlitligi va rad etilmasligini ta’minlaydigan matematik konstruktsiyadir. Raqamli imzo yaratishda asl xabar heshlanadi, so’ngra jo’natuvchining shaxsiy kaliti yordamida imzo yaratiladi. Qabul qiluvchi xabar o’zgartirilmaganligini va jo’natuvchi o’zi da’vo qilgan shaxs ekanligini tekshirish uchun jo’natuvchining ochiq kaliti yordamida imzoni tekshirishi mumkin.

Hesh funksiyalari fayllarning yaxlitligini tekshirish uchun ham ishlatilishi mumkin. Misol uchun, Internetdan faylni yuklab olayotganda, uning hesh qiymatini ishonchli manbadan yuklab olishingiz va keyin yuklab olingan faylning hesh qiymati saqlangan qiymatga mos kelishini tekshirishingiz mumkin. Agar hesh qiymatlari mos kelmasa, bu ma’lumotlarni uzatishda xatolar borligini yoki fayl tajovuzkor tomonidan o’zgartirilganligini ko’rsatishi mumkin.

Biroq, barcha hesh-funksiyalar teng yaratilmagan va ba’zi hesh-funksiyalar boshqalarga qaraganda hujumga nisbatan zaifroq bo’lishi mumkin. Hesh-funksiyalarga bo’lgan ba’zi hujumlar kunduzgi to’ldirish hujumlari, to’qnashuv hujumlari, bit imzo hujumlari va boshqalarni o’z ichiga oladi. Ushbu hujumlar ma’lumotlar yaxlitligini buzish, axborot xavfsizligini buzish va boshqa muammolarga olib kelishi mumkin.

Hesh-funksiyalarga hujum qilish xavfini kamaytirish uchun ularning ko’pchiligi tuz bilan birgalikda ishlatiladi, bu xashingdan oldin asl ma’lumotlarga tasodifiy qo’shilgan qiymatdir. Bu to’qnashuv hujumlarini amalga oshirishni qiyinlashtiradi, chunki tajovuzkor faqat dastlabki ma’lumotlar uchun emas, balki barcha mumkin bo’lgan tuz qiymatlari uchun hesh qiymatini hisoblashi kerak bo’ladi.

Ba’zi heshlash funktsiyalari ham muayyan ilovalar uchun mo’ljallangan. Masalan, SHA-3 funksiyasi kriptografik protokollarda hesh funksiyasi sifatida foydalanish uchun maxsus ishlab chiqilgan. U 2015 yilda SHA-2 o’rniga tanlovda tanlanganidan so’ng NISTning yangi heshlash standarti sifatida tanlangan.

Shuni ham hisobga olish kerakki, xash-funksiyalar panatseya emas va mutlaq xavfsizlikni kafolatlay olmaydi. Lug’at hujumlari va qo’pol kuch hujumlari kabi heshlangan ma’lumotlarga hujumlar mumkin. Shuning uchun, hesh funksiyalarini ma’lumotlarni shifrlash va foydalanuvchi autentifikatsiyasi kabi boshqa xavfsizlik choralari bilan birgalikda ishlatish muhimdir.

Bundan tashqari, hesh-funksiyalarning ishlashini hisobga olish kerak, chunki ular dastur ishlashiga sezilarli ta’sir ko’rsatishi mumkin. Ba’zi heshlash funktsiyalari boshqalarga qaraganda tezroq bo’lishi mumkin, ammo xavfsizroq bo’lishi mumkin. Shuning uchun, hash funktsiyasini tanlash xavfsizlik va ishlash o’rtasidagi muvozanatga asoslangan bo’lishi kerak.

Ba’zi keng tarqalgan hesh funktsiyalariga MD5, SHA-1, SHA-2 va SHA-3 kiradi. MD5 va SHA-1 90-yillarda ishlab chiqilgan va shundan beri jiddiy hujumlarga uchragan. SHA-2 2001 yilda ishlab chiqilgan va bugungi kunda keng tarqalgan bo’lib qo’llanilmoqda, ammo uning xavfsizligi ham tanqid qilindi. SHA-3 ushbu muammolarga javob sifatida ishlab chiqilgan va yangi, xavfsizroq heshlash funktsiyasidir.

Xulosa qilib aytganda, hesh funktsiyalari ma’lumotlarni himoya qilish va fayl yaxlitligini ta’minlash uchun ishlatiladigan muhim axborot xavfsizligi vositasidan biri bo’lib hisoblanadi. Biroq, xavfsizlik va ishonchlilikni ta’minlash uchun hesh funktsiyalari ularning xavfsizligi, ishlashi va ma’lum bir dastur uchun mosligi asosida tanlanishi kerak.

FOYDALANILGAN ADABIYOTLAR:

1. Винокуров, С.Ф. Избранные вопросы теории булевых функций / С.Ф. Винокуров. - М.: [не указано], 2012. - 564 с.
2. Рассел, Джесси Tiger (хэш-функция) / Джесси Рассел. - М.: VSD, 2012. - 833 с.
3. Мещанов С. В. Хеширование //Аллея науки. - 2018. - Т. 7. - N°. 6. - С.
4. Григорьев Д. Ю., Кондратьев В. Ю. Хеширование //Цифровизация экономики: направления, методы, инструменты. - 2019. - С. 102-104.