HESH FUNKSIYALAR

Qurbonmurodov Diyorbek Ulug'bek o'g'li
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti talabasi

Annotatsiya: Ushbu maqolada hesh funksiyalarga ehtiyoj tug'ilishining sabablari, hesh funksiyalarning xususiyatlariva hesh funksiyalarga qo'yiladigan talablarga to'xtalib o'tildi.

Kalit so'zlar: hesh funksiya, bir tomonlama funksiya, fiksirlangan qiymat, sha1, md5.

Hammamizga ma'lumki, biz ma'lumotlarni simmetrik kriptotizimlar orqali shifrlab qabul qiluvchiga jo'natamiz. Bunga sabab simmetrik kriptotizimlarni amalga oshirish vaqt jihatidan tez va unumdordir. Lekin bu yerda asosiy muammo bu o'rtada kalitni xavfsiz almashish muammosidir. Bu muammoni esa assimmetrik, ya'ni ochiq kalitli kriptotizimlar orqali hal qilamiz. Bunda o'rtada almashiniladigan simmetrik kalitni ochiq kalitli kriptotizimlar orqali shifrlab jo'natamiz. Chunki assimmetrik kriptotizimlarda kalit almashinish muammosi yo'q va bu tizimlar ancha bardoshli hisoblanadi. Lekin bu yerda buzg'unchi ma'lumotga o'zgaritirish kirita oladi, shunchaki ma'lumotni o'zgartirib qo'yadi va ma'lumot ahamiyatini yo'qotadi. Qabul qiluvchi ma'lumotdagi o'zgarishni sezmaydi. Aynan shu muammoning oldini olish uchun biz hesh funksiyalarga murojaat qilamiz.

Kriptografiyadagi xesh funksiyasi xabarlar yoki ma'lumotlar kabi turli xil ma'lumotlarni qabul qiluvchi va ularni belgilangan uzunlikdagi belgilar qatoriga aylantiruvchi matematik funktsiyaga o'xshaydi. Xesh funksiyasiga kirish har qanday uzunlikda, lekin chiqish har doim belgilangan uzunlikda ekanligini bildiradi[1].

Xesh funksiya deb, ixtiyoriy uzunlikdagi M ma'lumotni fiksirlangan uzunlikdagi h(M)=H qiymatga akslantib beruvchi, oson hisoblanadigan bir tomonli funksiyaga aytiladi. Xesh qiymat: "xesh qiymat", "svertka", "daydjest", "barmoq izlari" deb ham ataladi. Xesh funksiyaga nisbatan quyidagi talablar qo'yiladi[2]:

- Ixtiyoriy uzunlikdagi matn uchun qo'llab bo'lishlik.
- Chiqishda belgilangan uzunlikdagi qiymatni berishlik.
- Ixtiyoriy berilgan x bo'yicha h(x) oson hisoblanishlik.
- Ixtiyoriy berilgan H bo'yicha h (x)= N tenglikdan x ni hisoblab topib bo'lmaslik. (Bir tomonlilik xususiyati).
- Olingan x va y≠x matnlar uchun h(x)≠ h(y) munosabat o'rinli bo'lishi. (Kolliziyaga bardoshlilik xususiyati).

Shunday qilib hesh funksiyalar ixtiyoriy o'lchamdagi ma'lumotni algoritmga xos bo'lgan bir xil fiksirlangan qiymatga aylantirib beradi. Bu fiksirlangan qiymat o'lchami algoritmda beriladi. Biz hozirda md5, sha1, sha2 va boshqa turdagi hesh funksiyalarni

ishlatamiz. Agar misol uchun md5 algoritmini olib qaraydigan bo'lsak bunda ixtiyoriy uzunlikdagi kiruvchi ma'lumot bir xil 128 bit o'lchamdagi hesh qiymatga o'giriladi.

Hesh funskiyalar bizga yuqorida keltirib o'tgan muammomizni hal etishga yordam beradi, ya'ni ma'lumotimizning butunligini tekshirib beradi. Bu quyidagicha kechadi. Dastlab yuboruvchi ma'lumotni ma'lum bir algoritm yordamida ma'lumotni heshlaydi va hesh qiymatni ma'lumotga qo'shib jo'natadi. Qabul qiluvchi ma'lumotni qabul qiladi va uni heshlab, hosil qilgan hesh qiymatini yuboruvchidan kelgan hesh qiymat bilan solishtirib ko'radi. Agar bu ikkisi teng chiqsa, demak ma'lumot o'zgarishga uchramagan bo'ladi.

Hesh funksiyalar ma'lumotlar yaxlitligini tekshirishdan tashqari quyidagi holatlarda ham qo'l keladi:

Parolni tekshirish. Oddiy matn faylida parollarni saqlash xavfli, shuning uchun deyarli barcha saytlar parollarni xesh sifatida saqlaydi. Foydalanuvchi o'z parolini kiritganda, u xeshlanadi va natija kompaniya serverlarida saqlangan xeshlangan qiymatlar ro'yxati bilan taqqoslanadi. Biroq, bu aql bovar qilmaydigan amaliyot emas - xakerlar kamalak jadvallari deb ataladigan umumiy parollar va ularning xeshlari ma'lumotlar bazalarini yaratdilar, bu esa ularga hisoblarga kirishni osonlashtiradi.

Imzo yaratish va tekshirish. Imzolarni tekshirish raqamli hujjatlar yoki xabarlarning haqiqiyligini tekshirish uchun ishlatiladigan matematik jarayondir. Kerakli shartlar qondirilgan haqiqiy raqamli imzo qabul qiluvchiga xabarni ma'lum jo'natuvchi tomonidan yaratilganligi va u tranzit paytida o'zgartirilmaganligi haqida ishonchli dalil beradi[3].

Xulosa.

Shunday qilib hesh funksiyalar kriptografiyaning asosiy elementlaridan biri hisoblanib, ko'p jihatdan bizga qo'l keladi. Bizning parollarimiz ma'lumotlar bazalarida heshlangan holda saqlanadi. Shuningdek biz hesh funksiyalar orqali ma'lumotlardagi ruxsatsiz o'zgaritirishlarni aniqlashimiz mumkin. Shuningdek biz katta hajmli ma'lumotlar bilan ishlaganimizda ishimizni osonlashtirish uchun avval ularni heshlab keyin shifrlash kabi boshqa maqsadlar uchun ishlatamiz.

Foydalanilgan adabiyotlar.

1. https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm
2. S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari: O'quv qo'llanma. – T.: «Aloqachi», 2020, 221 bet.
3. https://www.investopedia.com/news/cryptographic-hash-functions/