HASH ALGORITMLARINI TAHLIL QILISH (MD5, SHA-1, BCRYPT)
АНАЛИЗ ХЭШ-АЛГОРИТМОВ (MD5, SHA-1, BCRYPT)
ANALYSIS OF HASH ALGORITHMS (MD5, SHA-1, BCRYPT)

Sobirjonov Behzod Qahramon o‘g‘li
Farg‘ona davlat universiteti
Axborot texnologiyalari kafedrasi o‘qituvchi
behzodbekqahramonovich@gmail.com
Rayimberdiyeva Dilnavoz Alisher qizi
Qosimjonova Sadoqat Elmurod qizi
Farg‘ona davlat universiteti
Axborot tizimlari va texnologiyalar yo‘nalishi
2-kurs talabalari
dilnavozrayimberdiyeva@gmail.com
sadoqatqosimjonova4@gmail.com

Annotatsiya: *Ushbu maqolada hash algoritmlarining ishlash prinsiplari va ularning axborot xavfsizligidagi ahamiyati tahlil qilinadi. Xususan, MD5, SHA-1 va bcrypt algoritmlarining tuzilishi, ishlash mexanizmi hamda ularning kuchli va zaif tomonlari ko‘rib chiqiladi. Shuningdek, ushbu algoritmlarning ma’lumotlarni himoyalash, parollarni saqlash va autentifikatsiya jarayonlaridagi qo‘llanilishi yoritiladi. Maqolada turli hash algoritmlarining xavfsizlik darajasi taqqoslanib, zamonaviy axborot tizimlarida ularni qo‘llash bo‘yicha tavsiyalar ham keltiriladi.*

Аннотация: *В данной статье анализируются принципы работы хэш-алгоритмов и их значение в области информационной безопасности. В частности рассматриваются алгоритмы MD5, SHA-1 и bcrypt, их структура, механизм работы, а также сильные и слабые стороны. Кроме того, освещается применение данных алгоритмов для защиты данных, хранения паролей и процессов аутентификации. В статье также проводится сравнение уровня безопасности различных хэш-алгоритмов и приводятся рекомендации по их использованию в современных информационных системах.*

Abstract: *This article analyzes the working principles of hash algorithms and their importance in information security. In particular, the algorithms MD5, SHA-1, and bcrypt are examined, including their structure, operating mechanisms, strengths, and weaknesses. The paper also discusses the application of these algorithms in data protection, password storage, and authentication processes. Additionally, the security levels of different hash algorithms are compared, and recommendations for their use in modern information systems are provided.*

Kalit so‘zlar: *Hash algoritmlari, MD5, SHA-1, bcrypt, kriptografiya, axborot xavfsizligi, parolni himoyalash, autentifikatsiya, ma’lumotlarni himoyalash*

Ключевые слова: *Hash algorithms, MD5, SHA-1, bcrypt, криптография, информационная безопасность, защита паролей, аутентификация, защита данных.*

Keywords: *Hash algorithms, MD5, SHA-1, bcrypt, cryptography, information security, password protection, authentication, data protection.*

Zamonaviy axborot texnologiyalari va dasturlash sohasida ma’lumotlar xavfsizligini ta’minlash muhim masalalardan biri hisoblanadi. Internet orqali ma’lumot almashinuvi kengayib borayotgan bir davrda foydalanuvchi ma’lumotlarini, ayniqsa parollarni himoyalash alohida ahamiyat kasb etadi. Shu sababli axborotni xavfsiz saqlash va uzatishda kriptografik usullar keng qo‘llaniladi. Bunday usullardan biri hash algoritmlaridir.

Hash algoritmlari ma’lumotlarni ma’lum uzunlikdagi maxsus kod — hash qiymatiga aylantiradi. Ushbu jarayon bir tomonlama bo‘lib, hosil bo‘lgan qiymatdan asl ma’lumotni qayta tiklash deyarli imkonsiz hisoblanadi. Shu xususiyati sababli hash algoritmlari parollarni saqlash, ma’lumotlar yaxlitligini tekshirish hamda autentifikatsiya jarayonlarida keng qo‘llaniladi.

Mazkur maqolada hash algoritmlarining ishlash prinsiplari hamda keng tarqalgan **MD5**, **SHA-1** va **bcrypt** algoritmlarining imkoniyatlari, afzalliklari va kamchiliklari tahlil qilinadi. Shuningdek, ularning axborot xavfsizligidagi o‘rni va amaliy qo‘llanilishi misollar orqali yoritiladi.

HASH ALGORITMLARINING VAZIFALARI VA AHAMIYATI

Hash algoritmlari — bu ma’lumotlarni ma’lum uzunlikdagi maxsus kodga aylantiruvchi matematik funksiyalardir. Har qanday hajmdagi ma’lumot kiritilgan taqdirda ham natijada doimiy uzunlikdagi hash qiymati hosil bo‘ladi. Bu algoritmlar axborot xavfsizligini ta’minlashda muhim rol o‘ynaydi.

Hash funksiyalarining asosiy vazifalaridan biri ma’lumotlarning yaxlitligini tekshirishdir. Agar ma’lumotlar uzatish jarayonida o‘zgarsa, u holda hosil bo‘lgan hash qiymati ham o‘zgaradi. Shu orqali tizim ma’lumotlarning buzilgan yoki o‘zgartirilganligini aniqlay oladi.

Hash algoritmlaridan yana bir muhim foydalanish sohasi foydalanuvchi parollarini saqlashdir. Zamonaviy tizimlarda parollar oddiy matn ko‘rinishida saqlanmaydi. Buning o‘rniga parol hash algoritmi orqali kodlanadi va ma’lumotlar bazasida faqat hash qiymati saqlanadi. Bu esa tizim xavfsizligini oshiradi va foydalanuvchi ma’lumotlarini himoya qiladi.

MD5 ALGORITMI: MD5 (Message Digest Algorithm 5) eng mashhur hash algoritmlaridan biri hisoblanadi. Ushbu algoritm 128 bitli hash qiymatini hosil qiladi va bir vaqtlar ma’lumotlar yaxlitligini tekshirish uchun keng qo‘llanilgan. MD5 algoritmi kiruvchi ma’lumotlarni bir nechta bloklarga ajratadi va matematik amallar orqali qayta ishlaydi. Natijada 32 belgidan iborat hexadecimal hash qiymati hosil bo‘ladi.

- **Afzalliklari:**

1. Juda tez ishlaydi.
2. Amalga oshirish oson.
3. Kichik hajmdagi ma’lumotlarni tekshirishda samarali.

- **Kamchiliklari:**

1. Kolliziya hujumlariga nisbatan zaif.
2. Zamonaviy xavfsizlik talablariga to‘liq javob bermaydi.
3. Parol saqlash uchun tavsiya etilmaydi.

SHA-1 ALGORITMI: SHA-1 (Secure Hash Algorithm 1) 160 bitli hash qiymatini hosil qiluvchi algoritm bo‘lib, u MD5 algoritmiga qaraganda xavfsizroq hisoblangan. SHA-1 algoritmi ma’lumotlarni 512 bitli bloklarga ajratadi va ularni bir necha bosqichli matematik funksiyalar orqali qayta ishlaydi. Natijada 40 belgidan iborat hash qiymati hosil bo‘ladi.

- **Afzalliklari:**

1.MD5 ga nisbatan xavfsizroq.
2.Ma’lumotlar yaxlitligini tekshirishda samarali.
3.Kriptografik tizimlarda uzoq vaqt foydalanilgan.

- **Kamchiliklari:**

1. Kolliziya hujumlariga nisbatan zaifligi aniqlangan.
2. Zamonaviy xavfsizlik standartlariga to‘liq mos kelmaydi.
3. Ko‘plab tizimlarda foydalanishdan chiqarilmoqda.

BCRYPT ALGORITMI: bcrypt — bu parollarni xavfsiz saqlash uchun ishlab chiqilgan zamonaviy hash algoritmidir. U Blowfish shifrlash algoritmiga asoslangan bo‘lib, parollarni himoyalashda yuqori xavfsizlik darajasini ta’minlaydi. Bcrypt algoritmi parolni hash qilish jarayonida salt deb ataladigan tasodifiy qiymatdan foydalanadi. Bu esa bir xil parollar uchun ham turli hash qiymatlar hosil bo‘lishini ta’minlaydi va hujumlarni qiyinlashtiradi.

- **Afzalliklari:**

1. Juda yuqori xavfsizlik darajasiga ega.
2. Salt mexanizmidan foydalanadi.
3. Brute-force hujumlariga qarshi samarali.
4.Zamonaviy tizimlarda keng qo‘llaniladi.

- **Kamchiliklari:**

1. Hisoblash jarayoni nisbatan sekinroq.
2. Katta hajmdagi ma’lumotlarni qayta ishlash uchun mo‘ljallanmagan.
3. Asosan parollarni himoyalashda qo‘llaniladi.

Amaliy qo‘llanilishi: Hash algoritmlari dasturchilar, axborot xavfsizligi mutaxassislari va tizim administratorlari tomonidan keng qo‘llaniladi. Ular bank tizimlari, internet xizmatlari, elektron pochta tizimlari hamda turli onlayn platformalarda foydalanuvchi ma’lumotlarini himoyalash uchun ishlatiladi.Oddiy hash misoli:

Parol:123456
MD5 hash: e10adc3949ba59abbe56e057f20f883e

Bu misolda foydalanuvchi paroli hash algoritmi orqali kodlangan va natijada maxsus hash qiymati hosil bo‘lgan.

Xulosa qilib aytganda, hash algoritmlari axborot xavfsizligini ta’minlashda muhim vosita hisoblanadi. Ular ma’lumotlarni himoyalash, parollarni saqlash va autentifikatsiya jarayonlarida keng qo‘llaniladi. MD5 va SHA-1 algoritmlari tarixan muhim bo‘lsa-da, hozirgi kunda xavfsizlik nuqtai nazaridan yetarli darajada ishonchli emas. Zamonaviy tizimlarda esa bcrypt kabi kuchli algoritmlardan foydalanish tavsiya etiladi. Shu sababli hash algoritmlarini to‘g‘ri tanlash va ulardan samarali foydalanish zamonaviy axborot tizimlarining xavfsizligini ta’minlashda muhim ahamiyatga ega.

FOYDALANILGAN ADABIYOTLAR

1. William Stallings. *Cryptography and Network Security: Principles and Practice*. Pearson Education, 2017.
2. Bruce Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, 1996.
3. National Institute of Standards and Technology. *Secure Hash Standard (SHS)* — FIPS PUB 180-4, 2015.
4. Ronald Rivest. *The MD5 Message-Digest Algorithm*. Internet Engineering Task Force (RFC 1321), 1992.
5. Niels Provos va David Mazières. *A Future-Adaptable Password Scheme (bcrypt)*. USENIX, 1999.
6. Internet Engineering Task Force. *RFC 3174: US Secure Hash Algorithm 1 (SHA-1)*. 2001.
7. Understanding Cryptography. Springer, 2010.
8. Axborot xavfsizligi va kriptografiya bo‘yicha zamonaviy ilmiy maqolalar hamda internet manbalari.