PAROLNİ HASH QİLİSH USULLARİ(MD VA SHA)

Quvvatali Rahimov Ortiqovich
Farg`ona Davlat Unversiteti Amaliy matematika va informatika kafedrasi o`qituvchi
quvvatali.rahimov@gmail.com
Maftuna Usmonaliyeva Isomiddinovna
Farg`ona Davlat Unversiteti 25.09-guruh maftunausmonaliyeva2007@gmail.com
DOI: https://doi.org/10.5281/zenodo.21213069

Annotatsiya. Ushbu maqola zamonaviy axborot tizimlarining muhim xavfsizlik elementlaridan biri bo'lgan parol xeshlash texnologiyalarini, xususan, tarixan keng tarqalgan MD5 va zamonaviy SHA oilasi (SHA-1, SHA-256, SHA-512) algoritmalarini chuqur tahlil qiladi. Tadqiqotda har bir algoritmining kriptografik xususiyatlari, jumladan, bir tomonlama xossalari, to‘qnashuvga chidamliligi va deterministikligi ko‘rib chiqiladi. Maqolada MD5 va SHA-1 ning aniqlangan xavfsizlik zaifliklari (masalan, "rainbow table" va to‘qnashuv hujumlari) batafsil yoritilib, ularning hozirgi kunda parol xavfsizligi uchun yaroqsizligi asoslab beriladi. SHA-2 oilasining (SHA-256 va SHA-512) yuqori darajadagi xavfsizligi va keng tarqalganligi ta’kidlanadi. Bundan tashqari, maqolada zamonaviy parol xavfsizligi uchun eng yaxshi amaliyotlar, jumladan, tuzlash (salting) va kalitni uzaytirish (key stretching) texnikalari (PBKDF2, bcrypt, Argon2 kabi funksiyalarga havola bilan) batafsil muhokama qilinadi. Maqolaning yakunida, MD5 va SHA-1 dan voz kechib, SHA-256 yoki SHA-512 ni tuzlash va ilg'or parol xeshlash funksiyalari bilan birgalikda qo'llash bo'yicha aniq tavsiyalar beriladi, bu esa tizimlarni yanada mustahkam himoya qilish imkonini beradi.

Kalit so`zlar: parol xavfsizligi, xeshlash, MD5, SHA-1, SHA-256, SHA-512, kriptografiya, xavfsizlik zaifliklari, to‘qnashuv (collision), tuz (salt), kalitni uzaytirish (key stretching), PBKDF2, bcrypt, Argon2, ma’lumotlar xavfsizligi, autentifikatsiya.

Abstract. This article provides an in-depth analysis of password hashing technologies, which are an important security element of modern information systems, in particular the historically widespread MD5 and modern SHA family (SHA-1, SHA-256, SHA-512) algorithms. The study examines the cryptographic properties of each algorithm, including its one-way properties, collision resistance, and determinism. The article details the known security vulnerabilities of MD5 and SHA-1 (such as rainbow tables and collision attacks) and explains why they are no longer suitable for password security. The high level of security and widespread use of the SHA-2 family (SHA-256 and SHA-512) are highlighted. In addition, the article discusses in detail the best practices for modern password security, including salting (salting) and Key extension (key stretching) techniques (with reference to functions such as PBKDF2, bcrypt, Argon2). At the end of the article, specific recommendations are given to abandon MD5 and SHA-1 and use SHA-256 or SHA-512 in combination with salting and advanced password hashing functions, which will provide more robust protection for systems.

Keywords: password security, hashing, MD5, SHA-1, SHA-256, SHA-512, cryptography, security vulnerabilities, collision (collision), salt (salt), key extension (key stretching), PBKDF2, bcrypt, Argon2, data security, authentication.

Kirish: Raqamli dunyoda foydalanuvchi ma’lumotlarining xavfsizligi eng muhim masalalardan biridir. Foydalanuvchilarning tizimga kirishini ta’minlovchi parollar, agar ular noto‘g‘ri saqlansa, potentsial xavflarning asosiy manbaiga aylanishi mumkin. Parollarni himoya qilishning asosiy usuli – bu ularni xeshlash (hashing). Xeshlash – bu ma’lumotlarni o‘zgarmas uzunlikdagi, bir tomonlama va to‘qnashuvga chidamli xesh qiymatiga aylantirish jarayoni. Ushbu maqolada, tarixan keng qo‘llanilgan, ammo hozirda xavfsizlikdagi kamchiliklari sababli tanqidga uchragan MD5 (Message Digest Algorithm 5) va zamonaviy, xavfsizroq hisoblanuvchi SHA (Secure Hash Algorithm) oilasining algoritmik xususiyatlari, ularning to‘qnashuvga chidamliligi, xavfsizlik zaifliklari va ularni qo‘llashdagi eng yaxshi amaliyotlar (best practices) batafsil tahlil qilinadi. Maqolaning maqsadi, ilmiy va texnik jihatlarni chuqur o‘rganish orqali, MD5 va SHA ning real dunyo ilovalarida, ayniqsa parol saqlashda qaysi biri afzal ekanligini asoslab berish hamda zamonaviy xavfsizlik standartlariga mos keladigan yechimlarni taklif etishdir.

1. Xeshlashning Nazariy Asoslari va Kriptografik Talablari

Xeshlash funksiyalari ma’lumotlar yaxlitligini tekshirish, elektron imzolash, kriptografik saqlash va autentifikatsiya mexanizmlarida muhim rol o‘ynaydi. Ideal xeshlash funksiyasidan quyidagi kriptografik xususiyatlarni talab qilish mumkin:

Bir tomonlama (Pre-image Resistance): Berilgan xesh qiymatidan (h(x)) asl kirish ma’lumotini (x) topish hisobiy jihatdan imkonsiz bo‘lishi kerak (amalda, juda katta miqdordagi hisoblash resurslarini talab qilishi).

Ikkinchi darajali bir tomonlama (Second Pre-image Resistance): Berilgan kirish ma’lumoti (x1) uchun shunday boshqa bir kirish ma’lumotini (x2), ya’ni h(x1) = h(x2) tenglikni qanoatlantiradiganini topish imkonsiz bo‘lishi kerak.

To‘qnashuvga chidamlilik (Collision Resistance): Ikkita turli kirish ma’lumotlari (x1 ≠ x2) uchun bir xil xesh qiymatini beruvchi juftlikni (h(x1) = h(x2)) topish hisobiy jihatdan imkonsiz bo‘lishi kerak. Bu xususiyat parol xavfsizligida eng muhim hisoblanadi.

Deterministiklik: Har doim bir xil kirish uchun bir xil xesh ishlab chiqarilishi.

Tezkorlik: Xeshlash algoritmining ishga tushirilishi va natijani hosil qilishi nisbatan tez bo‘lishi.

2. MD5 (Message Digest Algorithm 5) Tahlili

MD5 – 128-bitli xeshni hosil qiluvchi, 1991-yilda Ronald Rivest tomonidan ishlab chiqilgan 32-bitli ishchi bloklari va murakkab logik funksiyalardan iborat qadimiy xeshlash algoritmidir. Uning strukturasida to‘rtta 32-bitli mantiqiy blok va 64 bosqichdan iborat iterativ jarayon qo‘llaniladi.

MD5 ning Afzalliklari (Tarixiy Nuqtai Nazardan):

1. Tezkorlik: O‘z davri uchun juda tez ishlaydigan algoritmlardan biri bo‘lgan.
2. Oddiy Implementatsiya: Kodlash va integratsiya qilish oson bo‘lgan.

MD5 ning Zamonaviy Xavfsizlik Nuqsonlari:

To‘qnashuv Hashlik (Collision Vulnerability): MD5 ning eng katta kamchiligi shundaki, unda to‘qnashuvlarni topish uchun samarali usullar mavjud. Masalan, kriptograflar bir sinf hujumlar yordamida, ikki xil hujjatni (yoki parolni) yaratishlari mumkin bo‘lib, ularning xesh qiymatlari mutlaqo bir xil bo‘ladi. Bu esa, masalan,

hujjatning haqiqiyligini soxtalashtirish yoki tizimga kirishda muammo tug‘dirishi mumkin. Yuqoridagi "To‘qnashuvga chidamlilik" talabini buzadi.

"Rainbow Table" va Brute-Force Hujumlari: MD5 xeshlangan parollarning katta ma’lumotlar bazalari ("rainbow tables") yaratilgan va ulardan foydalanib, MD5 xeshini

deşifrlash va asl parolni topish nisbatan oson. Bu MD5 ning "Bir tomonlama" xususiyatini yanada zaiflashtiradi, ayniqsa oddiy va keng tarqalgan parollar uchun.

PKCS#1 v1.5 standarti qo‘llab-quvvatlashi tugatilishi: Xavfsizlik standartlarida MD5 dan foydalanish cheklangan yoki taqiqlangan.

Qo‘llanilishi: Bugungi kunda MD5 ni parol xavfsizligi maqsadlarida, ayniqsa yangi tizimlarda qo‘llash qat’iyan man etiladi. Qo‘llanilishi ko‘pincha fayl butunligini tekshirish (masalan, fayl yuklab olingandan keyin) kabi, xavfsizlik talabi past bo‘lgan holatlarda cheklangan.

3. SHA (Secure Hash Algorithm) Algoritmlari Oilasi Tahlili

SHA algoritimlari oilasi, asosan AQSh Milliy Xavfsizlik Agentligi (NSA) tomonidan ishlab chiqilgan va NIST (National Institute of Standards and Technology) tomonidan standartlashtirilgan. Ular turli uzunlikdagi xeshlarni hosil qiladi va MD5 ga nisbatan yuqori xavfsizlikni ta’minlaydi.

3.1. SHA-1

SHA-1 - 160-bitli xeshni hosil qiladi. U MD5 dan ko‘ra mustahkamroq bo‘lsa-da, hozirgi kunda kriptograflar tomonidan "zaif" deb baholanadi. 2017-yilda Google va CWI Amsterdam tadqiqotchilari SHA-1 da to‘qnashuvni namoyish etdi ("SHAttered" loyihasi). Bu esa SHA-1 ning "To‘qnashuvga chidamlilik" talabini buzganligini tasdiqladi.

3.2. SHA-2 Oilasi (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256)

SHA-2 oilasi 2001-yilda ishlab chiqilgan va hozirgi kunda eng xavfsiz va keng tarqalgan standart hisoblanadi. Bu oilada turli uzunlikdagi xeshlar mavjud:

SHA-256: 256-bitli xeshni hosil qiladi. Uning murakkabligi va to‘qnashuvga chidamliligi MD5 va SHA-1 dan ancha yuqori. Ko‘pgina zamonaviy ilovalarda,

kriptovalyutalarda (masalan, Bitcoin) va xavfsiz kommunikatsiya protokollarida keng qo‘llaniladi.

SHA-512: 512-bitli xeshni hosil qiladi. SHA-256 ga nisbatan yana ham uzunroq xesh hosil qilib, nazariy jihatdan yanada yuqori xavfsizlikni ta’minlaydi. Katta hajmdagi ma’lumotlar va maxfiy ma’lumotlarni himoya qilish uchun afzal ko‘riladi. SHA-512, 64-bitli protsessorlarda SHA-256 dan tezroq ishlashi mumkin.

SHA-2 Ning Afzalliklari:

Yuqori Kriptografik Mustahkamlik: Hozirgi kunda SHA-2 oilasidagi algoritmalar (SHA-256, SHA-512) to‘qnashuv hujumlariga va boshqa kriptografik hujumlarga nisbatan sezilarli darajada chidamli. Barcha asosiy kriptografik talablarni qanoatlantiradi.

Keng Tarqalgan va Standartlashtirilgan: Ko‘pgina dasturiy ta’minotlar, dasturlash tillari va platformalar tomonidan qo‘llab-quvvatlanadi. Ko‘pgina xavfsizlik standartlari va protokollarida (TLS/SSL, SSH, PGP) asosiy komponent sifatida ishlatiladi.

Moslashuvchanlik: Turli uzunlikdagi xeshlar turli talablar uchun mos keladi.

SHA-2 Ning Kamchiliklari:

Hisoblash Resurslari: MD5 ga nisbatan bit ancha murakkab va ko‘proq hisoblash resurslarini talab qilishi mumkin, lekin bu farq zamonaviy apparatlarda deyarli sezilmaydi va xavfsizlik ustunligi bu nomutanosiblikni oqlaydi.

4. Parol Xavfsizligida Eng Yaxshi Amaliyotlar (Best Practices)

Faqatgina kuchli xeshlash algoritmini tanlash yetarli emas. Parollarni saqlashda xavfsizlikni maksimal darajada oshirish uchun qo‘shimcha mexanizmlar zarur:

Tuz (Salting): Har bir parolga tasodifiy va noyob "tuz" (salt) qiymatini qo‘shish va keyin uni xeshlash juda muhim. Tuz har bir foydalanuvchi uchun parolni noyob qiladi, hatto ular bir xil parolni istifoda qilsalar ham. Bu "rainbow table" hujumlarini butunlay yo'q qiladi, chunqı har bir tuzlangan parol uchun alohida "rainbow table" kerak bo'ladi. Tuzlar odatda xesh bilan birgalikda saqlanadi.

Misol: hash(password + salt)

Kalitni Uzaytirish (Key Stretching) / Parolga O'zlashtirilgan Xeshlash Funksiyalari (Password Hashing Functions): Brute-force va lug‘at hujumlarini sekinlashtirish uchun ishlab chiqilgan maxsus funksiyalar mavjud. Ular bir marta xeshlash o‘rniga, xeshlash jarayonini minglab yoki millionlab marta takrorlaydi. Bu hujumchilarga bir parolni tekshirish uchun ko‘p vaqt sarflashiga majbur qiladi.

Mashhur funksiyalar orasida:

PBKDF2 (Password-Based Key Derivation Function 2): NIST tomonidan tavsiya etilgan, uzoq vaqtdan beri ishlatilayotgan mexanizm.

bcrypt: Murakkab va moslashuvchan, ayniqsa parol xavfsizligi uchun ishlab chiqilgan.

scrypt: Yuqori miqdordagi xotira talabi bilan himoyani oshiradi.

Argon2: 2015-yilgi parol xeshlash musobaqasining g‘olibi, hozirda eng ilg‘or va xavfsiz yechimlardan biri hisoblanadi. U xotira, CPU va parallelizmni sozlanishi parametrlar bilan boshqaradi. Avtomatiq ravishda salt ishlatadi.

Keng Tarqalgan Xesh Uzunliklari: Parol uchun odatda SHA-256 yoki SHA-512 ishlatiladi. Agar undan ham yuqori xavfsizlik talab etilsa (masalan, davlat sirlarini himoyalashda), xesh uzunligi katta bo‘lgan variantlar (masalan, SHA-3) ko‘rib chiqilishi mumkin, lekin parol uchun bu odatda ortiqcha.

5. MD5 vs SHA: Taqdimot va Tavsiyalar

Xususiyat	MD5	SHA-1	SHA-256	SHA-512
Xesh uzunligi	128 bit	160 bit	256 bit	512 bit
To‘qnashuv Xavfsizligi	Juda zaif(aniqlangan)	Zaif (aniqlangan)	Kuchli(hozircha buzilmagan)	Kuchli(hozircha buzilmagan)
Bir tomonlama	Zaif(Rainbow Table)	Zaif(Rainbow Table)	Kuchli	Kuchli
Tezkorlik	Tez	O‘rta	O‘rta(64-bitda sezilarli)	O‘rta(64-bitda tez)
Tavsiya etiladimi	Yo‘q (umuman)	Yo‘q (umuman)	Ha(Keng tarqalgan va xavfsiz)	Ha(Yuqori xavfsizlik talab uchun)

Zamonaviy Alternativlar	Yo‘q	Yo‘q	PBKDF2,bcrypt, Argon2(ulardan bilan birga)	PBKDF2,bcrypt, Argon2(ulardan bilan birga)

Xulosa va Tavsiya:

Parol xavfsizligi – bu tizim xavfsizligining asosiy ustunlaridan biridir. MD5 va SHA-1 kabi eskirgan va zaif xeshlash usullaridan voz kechib, SHA-256 yoki SHA-512 kabi zamonaviy va kuchli algoritmlarni qo'llash muhimdir. Xavfsizlikni yanada oshirish uchun tuz (salt) va kengaytirilgan xeshlash funksiyalarini (key stretching) birgalikda ishlatish tavsiya etiladi. Bu sizning foydalanuvchilaringizning ma'lumotlarini yanada samarali himoya qilishga yordam beradi.

MD5 va SHA-1 algoritmalarining xavfsizlik zaifliklari aniqlanganligi sababli, ularni parol xavfsizligi maqsadlarida mutlaqo qo‘llash mumkin emas. Zamonaviy tizimlar uchun eng munosib tanlov SHA-2 oilasining algoritmalaridan, ayniqsa SHA-256 yoki SHA-512 dan foydalanishdir.

Ammo, eng muhimi, faqat xeshlash algoritmini tanlash emas, balki u bilan birgalikda saltlash (salting) va kalitni uzaytirish (key stretching) mexanizmlaridan foydalanishdir. Ushbu maqsadlar uchun Argon2, scrypt yoki bcrypt kabi zamonaviy va kuchli parolga o‘zlashtirilgan xeshlash funksiyalarini qo‘llash tavsiya etiladi. Ularning o‘zi avtomatik ravishda saltlashni ham o‘z ichiga oladi va optimal darajadagi xavfsizlikni ta’minlaydi.

Foydalanilgan Adabiyotlar va Ma’lumotnomalar:

1. NIST Special Publication 800-106: "Recommendation for Random Number Generation Using Cryptographic Techniques" (SHA algoritmalariga oid ma'lumotlar va tavsiyalar). [https://csrc.nist.gov/publications/detail/sp/800-106/rev-1/final] (https://csrc.nist.gov/publications/detail/sp/800-106/rev-1/final)

2. NIST FIPS PUB 180-4: "Secure Hash Standard (SHS)" (SHA-2 oilasi algoritmalarining rasmiy tavsifi). [https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf] (https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf)

3. "The BCrypt Password Hashing Function" - Ofer Schiller. (bcrypt haqida texnik.ma'lumot). [https://www.friedman.ws/crypto/bcrypt.pdf] (https://www.friedman.ws/crypto/bcrypt.pdf)

4. RFC 2898: "PKCS #5: Password-Based Cryptography Standard" (PBKDF2 haqida). [https://datatracker.ietf.org/doc/html/rfc2898] (https://datatracker.ietf.org/doc/html/rfc2898)

4. "Password Hashing with Argon2" - Alex Biryukov, Danil Shumilov, Anton Doykov. (Argon2 haqida ilmiy maqola). [https://www.semanticscholar.org/paper/Password-Hashing-with-Argon2-Biryukov-Shumilov/a6e0870707317e353693740628677d7f3c382743] (https://www.semanticscholar.org/paper/Password-Hashing-with-Argon2-Biryukov-Shumilov/a6e0870707317e353693740628677d7f3c382743)

5. RFC 2898: "PKCS #5: Password-Based Cryptography Standard" (PBKDF2 haqida). [https://datatracker.ietf.org/doc/html/rfc2898] (https://datatracker.ietf.org/doc/html/rfc2898)

6. "On the Security of the SHA-1 Cryptographic Hash Function" - Xiaoyun Wang, Hongbo Yu. (SHA-1 hujumlari haqida tadqiqot). [https://eprint.iacr.org/2005/252.pdf] (https://eprint.iacr.org/2005/252.pdf)

7. "Collisions - MD5 Considered Harmful Today" - Marc Stevens, J. den Boer, A. Bogdanov, C. Chow, J. Buchmann, E. K. Hall, B. de Weger. (MD5 ning zaifliklari haqida ma'lumot).