EOC
EUROASIAN
ONLINE
CONFERENCES

ENGLAND
CONFERENCE

INTERNATIONAL CONFERENCE ON MULTIDISCIPLINARY STUDIES AND EDUCATION



Google Scholar zenodo OpenAIRE doi digital object identifier

INTERNATIONAL CONFERENCE ON MULTIDISCIPLINARY STUDIES AND EDUCATION: a collection scientific works of the International scientific conference – London, England, 2026. Issue 5

Languages of publication: Uzbek, English, Russian, German, Italian, Spanish

The collection consists of scientific research of scientists, graduate students and students who took part in the International Scientific online conference **«INTERNATIONAL CONFERENCE ON MULTIDISCIPLINARY STUDIES AND EDUCATION»**. Which took place in London 2026.

Conference proceedings are recommended for scientists and teachers in higher education establishments. They can be used in education, including the process of post - graduate teaching, preparation for obtain bachelors' and masters' degrees. The review of all articles was accomplished by experts, materials are according to authors copyright. The authors are responsible for content, researches results and errors.

HASH ALGORITMLARINI TAHLIL QILISH (MD5, SHA-1, BCRYPT)

Behzod Sobirjonov Qahramonivich
FarDu Axborot texnologiyalari kafedrasi o‘qituvchisi
behzodbekqahramonovich@gmail.com
Muxtorova Nasibaxon Axliddin qizi
FarDu Axborot tizimlari va texnologiyalari yo‘nalishi 2-bosqich talabasi
nasibaxonmuxtorova5@gmail.com
Telefon raqam:91-282-23-12

ANNOTATSIYA. Ushbu maqolada zamonaviy axborot xavfsizligi tizimlarida muhim o‘rin tutuvchi hash algoritmlarining nazariy asoslari, ishlash mexanizmlari, xavfsizlik xususiyatlari va amaliy qo‘llanilish sohalari tahlil qilinadi. Hash algoritmlar ma’lumotlarni belgilangan uzunlikdagi xesh qiymatga aylantirish orqali ularning yaxlitligini tekshirish, foydalanuvchilarni autentifikatsiya qilish, parollarni himoyalangan ko‘rinishda saqlash, elektron imzo va raqamli sertifikatlar bilan ishlash kabi jarayonlarda keng qo‘llaniladi. Maqolada ayniqsa MD5, SHA-1 va bcrypt algoritmlariga alohida e’tibor qaratilib, ularning yaratilish maqsadi, texnik imkoniyatlari, xavfsizlik darajasi, afzalliklari hamda zaif tomonlari izchil yoritiladi.

Tadqiqot davomida MD5 algoritmi yuqori tezlikka ega bo‘lsa-da, bugungi kunda collision hujumlariga nisbatan zaifligi sababli xavfsizlik muhim bo‘lgan tizimlarda foydalanish uchun mos emasligi ko‘rsatib beriladi. SHA-1 algoritmi MD5 ga nisbatan kuchliroq hash qiymat hosil qilsa ham, zamonaviy hisoblash quvvatlari va kriptotahlil usullari rivojlanishi natijasida uning ham xavfsizlik darajasi yetarli emasligi asoslanadi. bcrypt algoritmi esa umumiy ma’lumot yaxlitligini tekshirish uchun emas, balki aynan foydalanuvchi parollarini xavfsiz saqlash uchun ishlab chiqilgan maxsus password hashing algoritmi sifatida tahlil qilinadi. Uning salt va cost factor kabi mexanizmlari parollarni brute-force, dictionary attack va rainbow table kabi hujumlardan himoya qilishda muhim ahamiyatga ega ekanligi bayon etiladi.

Maqolada ushbu uch algoritm o‘zaro solishtirilib, ularning tezligi, xavfsizlik darajasi, collisionga chidamliligi, parol saqlashga mosligi va zamonaviy axborot tizimlaridagi qo‘llanish imkoniyatlari baholanadi. Shuningdek, noto‘g‘ri hash algoritm tanlash oqibatida yuzaga kelishi mumkin bo‘lgan xavfsizlik muammolari tahlil qilinadi. Tadqiqot natijasida MD5 va SHA-1 algoritmlaridan yangi xavfsizlik tizimlarida foydalanish tavsiya etilmasligi, parollarni saqlashda esa bcrypt, scrypt yoki Argon2 kabi maxsus algoritmlardan foydalanish maqsadga muvofiqligi xulosa qilinadi. Ushbu maqola hash algoritmlarni tanlashda amaliy va nazariy jihatdan to‘g‘ri yondashuvni shakllantirishga xizmat qiladi.

Kalit so‘zlar: Kiberxavfsizlik, Hash algoritm, MD5, SHA-1, bcrypt, Kriptografiya, Parol xavfsizligi, Ma’lumot yaxlitligi, Collision, Brute-force, Salt, Cost factor, Autentifikatsiya, Axborot himoyasi.

ANNOTATION. This article analyzes the theoretical foundations, working mechanisms, security properties, and practical application areas of hash algorithms used in modern information security systems. Hash algorithms play an important role in transforming data of arbitrary length into a fixed-length hash value, which makes it possible to verify data integrity, protect user passwords, support authentication

processes, and strengthen cryptographic mechanisms such as digital signatures and certificates. The study focuses on MD5, SHA-1, and bcrypt because these algorithms differ significantly in their design goals, performance characteristics, security levels, and suitability for modern cybersecurity tasks.

The article explains that MD5 was historically widely used because of its simplicity and high processing speed. However, despite these advantages, MD5 is no longer considered secure for security-critical applications due to its vulnerability to collision attacks. Such weaknesses can allow attackers to generate different inputs with the same hash value, which creates serious risks in digital signatures, file verification, and authentication systems. SHA-1 is also examined as a stronger algorithm compared with MD5, producing a longer hash value and previously being used in many cryptographic applications. Nevertheless, the development of modern computing power and advanced cryptanalysis techniques has shown that SHA-1 also fails to meet current cybersecurity requirements.

In contrast, bcrypt is analyzed as a specialized password hashing algorithm rather than a general-purpose hash function. Its main strength lies in its deliberately slow computation process, which makes large-scale password guessing attacks significantly more difficult. The article discusses the role of salt in preventing identical passwords from producing identical hash values and reducing the effectiveness of rainbow table attacks. It also explains the importance of the cost factor, which allows system administrators to adjust the computational complexity of hashing according to the required balance between security and performance. These features make bcrypt more suitable for protecting stored passwords than fast hash algorithms such as MD5 and SHA-1.

The article also provides a comparative analysis of MD5, SHA-1, and bcrypt based on processing speed, collision resistance, resistance to brute-force attacks, password storage suitability, and compliance with modern security requirements. The analysis shows that MD5 and SHA-1 should not be used in new systems where strong cryptographic protection is required. For password storage, specialized password hashing algorithms such as bcrypt, scrypt, or Argon2 are recommended. The results of this study highlight the importance of selecting hash algorithms according to their intended purpose and security context. The article may be useful for cybersecurity specialists, software developers, students, and researchers working with authentication systems, data protection, and cryptographic security mechanisms.

Keywords: Cybersecurity, Hash algorithm, MD5, SHA-1, bcrypt, Cryptography, Password security, Data integrity, Collision, Brute-force, Salt, Cost factor, Authentication, Information protection.

Zamonaviy axborot texnologiyalari rivojlanib borayotgan bir davrda ma’lumotlarni himoya qilish, ularning yaxlitligini tekshirish va foydalanuvchilarni xavfsiz autentifikatsiya qilish muhim masalalardan biri hisoblanadi. Ayniqsa, internet xizmatlari, elektron to‘lov tizimlari, mobil ilovalar va ma’lumotlar bazalarida foydalanuvchi ma’lumotlarini himoyalash katta ahamiyatga ega. Bu jarayonda kriptografik algoritmlar, xususan hash funksiyalari keng qo‘llaniladi.Hash algoritm — bu ixtiyoriy uzunlikdagi ma’lumotni belgilangan uzunlikdagi qiymatga aylantiruvchi matematik funksiyadir. Hosil bo‘lgan natija odatda **hash qiymat**, **digest** yoki **xesh**

kod deb ataladi. Hash funksiyalarining asosiy vazifasi ma'lumotning o'zgarmaganligini tekshirish, fayllar yaxlitligini nazorat qilish va parollarni xavfsiz shaklda saqlashdan iborat.

Hash algoritmlar bir qarashda oddiy ko'rinsa-da, ularning xavfsizlik darajasi juda muhim hisoblanadi. Chunki zaif hash algoritmlar orqali hujumchilar bir xil hash qiymatga ega bo'lgan boshqa ma'lumotlarni topishi yoki parollarni aniqlashi mumkin. Shu sababli hash algoritmlarini tanlashda ularning tezligi, collisionga chidamliligi, brute-force hujumlarga qarshiligi va amaliy qo'llanish sohasi hisobga olinishi kerak.

Ushbu maqolada eng ko'p uchraydigan hash algoritmlaridan MD5, SHA-1 va bcrypt tahlil qilinadi. MD5 va SHA-1 tarixan keng qo'llanilgan bo'lsa-da, bugungi kunda ularning xavfsizlik darajasi yetarli emas. bcrypt esa ayniqsa parollarni himoyalash uchun ishlab chiqilgan bo'lib, zamonaviy autentifikatsiya tizimlarida muhim ahamiyatga ega.

HASH ALGORITMLARINING ASOSIY TUSHUNCHASI

Hash algoritmlar kriptografiyada muhim o'rin egallaydi. Ular ma'lumotni maxsus matematik jarayon orqali qisqa va belgilangan uzunlikdagi ko'rinishga keltiradi. Masalan, katta hajmdagi matn, fayl yoki parol hash algoritm orqali qayta ishlanganda, natijada aniq uzunlikdagi hash qiymat hosil bo'ladi.Hash funksiyalarining muhim xususiyatlaridan biri — bir xil kiruvchi ma'lumot har doim bir xil hash qiymatni hosil qiladi. Agar ma'lumotning bitta belgisi ham o'zgarsa, hash qiymat butunlay boshqacha bo'lib chiqadi. Shu sababli hash algoritmlar fayllarning o'zgargan yoki o'zgarmaganligini tekshirishda keng qo'llaniladi.

Yaxshi hash algoritm quyidagi xususiyatlarga ega bo'lishi kerak: birinchidan, u tez ishlashi kerak; ikkinchidan, hash qiymatdan asl ma'lumotni tiklash juda qiyin bo'lishi kerak; uchinchidan, ikki xil ma'lumot uchun bir xil hash qiymat hosil bo'lish ehtimoli juda past bo'lishi zarur. Agar ikki xil ma'lumot bir xil hash qiymat bersa, bu holat **collision** deb ataladi.

Collision hash algoritmlar xavfsizligidagi eng muhim muammolardan biridir. Agar algoritmda collision topish oson bo'lsa, undan xavfsiz tizimlarda foydalanish tavsiya etilmaydi. Aynan shu sababli MD5 va SHA-1 algoritmlari bugungi kunda xavfsiz kriptografik maqsadlar uchun eskirgan hisoblanadi.

MD5 ALGORITMI TAHLILI. MD5 — Message Digest Algorithm 5 nomi bilan tanilgan kriptografik hash algoritmdir. U 128 bitli hash qiymat hosil qiladi. MD5 algoritmi avval fayllar yaxlitligini tekshirish, elektron imzolar va parollarni saqlash kabi jarayonlarda keng qo'llanilgan. Uning asosiy afzalligi — juda tez ishlashidir.

MD5 algoritmi kiruvchi ma'lumotni bloklarga ajratadi va ularni maxsus matematik amallar orqali qayta ishlaydi. Natijada 128 bitli hash qiymat hosil bo'ladi. Masalan, foydalanuvchi paroli MD5 orqali hash qilinganda, ma'lumotlar bazasida parolning o'zi emas, balki uning hash qiymati saqlanishi mumkin.Biroq MD5 bugungi kunda xavfsiz algoritm hisoblanmaydi. Chunki u collision hujumlariga nisbatan zaif. Ya'ni hujumchi turli xil ma'lumotlar uchun bir xil MD5 hash qiymat hosil qilish imkoniyatiga ega bo'lishi mumkin. Bu esa elektron imzo, sertifikat va autentifikatsiya tizimlarida katta xavf tug'diradi.

MD5 algoritmining yana bir kamchiligi uning juda tez ishlashidir. Oddiy holatda tezlik afzallik bo'lishi mumkin, lekin parollarni himoyalashda bu salbiy

jihatga aylanadi. Chunki hujumchi maxsus dasturlar yordamida qisqa vaqt ichida juda ko‘p parol variantlarini sinab ko‘rishi mumkin. Shu sababli MD5 parollarni saqlash uchun tavsiya etilmaydi.

MD5 hozirgi vaqtda faqat xavfsizlik muhim bo‘lmagan ayrim nazorat vazifalarida, masalan oddiy checksum tekshiruvida uchrashi mumkin. Ammo bank tizimlari, davlat axborot tizimlari, elektron imzo, login-parol tizimlari va boshqa muhim sohalarda MD5 dan foydalanish xavfli hisoblanadi.

SHA-1 ALGORITMI TAHLILI

SHA-1 — Secure Hash Algorithm 1 nomi bilan tanilgan hash algoritm bo‘lib, 160 bitli hash qiymat hosil qiladi. U MD5 ga qaraganda kuchliroq hisoblangan va uzoq vaqt davomida ko‘plab xavfsizlik tizimlarida qo‘llanilgan. SHA-1 elektron imzo, sertifikatlar, fayl tekshiruvi va boshqa kriptografik jarayonlarda ishlatilgan.SHA-1 algoritmi ham kiruvchi ma’lumotni bloklarga ajratib, ularni bosqichma-bosqich qayta ishlaydi. Natijada 160 bitli hash qiymat hosil bo‘ladi. Hash uzunligi MD5 ga qaraganda katta bo‘lgani sababli SHA-1 avval xavfsizroq variant sifatida qabul qilingan.Ammo vaqt o‘tishi bilan SHA-1 algoritmida ham xavfsizlik muammolari aniqlangan. Xususan, collision hujumlari SHA-1 uchun ham amaliy jihatdan mumkinligi isbotlangan. Bu esa algoritmni zamonaviy xavfsizlik tizimlarida qo‘llashni cheklaydi.

SHA-1 algoritmi hozirgi kunda yangi loyihalarda tavsiya etilmaydi. Uning o‘rniga SHA-256, SHA-3 yoki boshqa kuchliroq algoritmlardan foydalanish maqsadga muvofiq. Ayniqsa, elektron imzo, raqamli sertifikat va muhim ma’lumotlar yaxlitligini tekshirishda SHA-1 dan foydalanish xavfsizlik nuqtai nazaridan to‘g‘ri emas.Shunga qaramay, SHA-1 tarixiy jihatdan muhim algoritm hisoblanadi. U kriptografik hash funksiyalar rivojlanishida katta rol o‘ynagan. Lekin zamonaviy kiberxavfsizlik talablarida algoritm faqat eski tizimlarni tahlil qilish yoki moslikni saqlash maqsadida uchrashi mumkin.

BCRYPT ALGORITMI TAHLILI

bcrypt — parollarni xavfsiz saqlash uchun ishlab chiqilgan maxsus password hashing algoritmdir. U MD5 va SHA-1 dan farqli ravishda oddiy ma’lumot yaxlitligini tekshirish uchun emas, balki aynan parollarni brute-force hujumlardan himoya qilish uchun mo‘ljallangan.bcrypt algoritmining asosiy afzalligi shundaki, u ataylab sekin ishlaydi. Bu foydalanuvchi uchun katta noqulaylik tug‘dirmaydi, chunki login jarayonida bitta parol tekshiriladi. Ammo hujumchi uchun millionlab parollarni tezda tekshirishni qiyinlashtiradi. Shu sababli bcrypt parollar xavfsizligini oshirishda samarali hisoblanadi.

bcrypt algoritmida **salt** mexanizmi mavjud. Salt — har bir parolga qo‘shiladigan tasodifiy qiymat bo‘lib, bir xil parollar uchun ham turli hash qiymatlar hosil bo‘lishini ta’minlaydi. Masalan, ikki foydalanuvchi bir xil paroldan foydalansa ham, bcrypt ularning parollarini turli hash qiymatlar ko‘rinishida saqlaydi. Bu rainbow table kabi oldindan tayyorlangan hujum usullarining samaradorligini kamaytiradi.bcrypt algoritmida yana bir muhim tushuncha — **cost factor** hisoblanadi. Cost factor algoritmning hisoblash murakkabligini belgilaydi. Ya’ni cost factor qanchalik yuqori bo‘lsa, hash hisoblash jarayoni shunchalik sekin va murakkab bo‘ladi. Bu esa hujumchi uchun ko‘proq vaqt va hisoblash resursi talab qiladi.Biroq

bcrypt ham mutlaq mukammal algoritm emas. Uning ayrim cheklovlari mavjud. Masalan, bcrypt uzun parollarni qayta ishlashda ma'lum chegaralarga ega. Shuningdek, juda katta tizimlarda cost factor noto'g'ri tanlansa, server yuklamasi oshib ketishi mumkin. Shu sababli bcrypt ishlatilganda xavfsizlik va tizim samaradorligi o'rtasida muvozanat saqlanishi kerak.

Xulosa qilib aytganda, hash algoritmlar axborot xavfsizligining muhim qismlaridan biridir. Ular ma'lumot yaxlitligini tekshirish, parollarni himoyalash, raqamli imzo yaratish va autentifikatsiya jarayonlarida keng qo'llaniladi. Biroq har bir hash algoritmning xavfsizlik darajasi va qo'llanish sohasi farq qiladi.

MD5 algoritmi tez ishlashi bilan ajralib tursa-da, collision hujumlariga nisbatan zaif bo'lgani sababli zamonaviy xavfsizlik tizimlari uchun mos emas. SHA-1 algoritmi MD5 ga qaraganda kuchliroq bo'lsa ham, u ham bugungi kunda eskirgan va xavfsiz hisoblanmaydi. bcrypt esa parollarni himoyalash uchun samarali algoritm bo'lib, salt va cost factor mexanizmlari yordamida brute-force hujumlarga qarshi kuchliroq himoya yaratadi.

Shu sababli hash algoritmlardan foydalanishda ularning vazifasi va xavfsizlik darajasi to'g'ri baholanishi kerak. Ma'lumot yaxlitligi uchun zamonaviy SHA-2 yoki SHA-3 oilasiga mansub algoritmlar, parollarni saqlash uchun esa bcrypt, scrypt yoki Argon2 kabi maxsus password hashing algoritmlaridan foydalanish maqsadga muvofiqdir. Bu esa axborot tizimlarining ishonchliligi va kiberxavfsizlik darajasini oshirishga xizmat qiladi.

Foydalanilgan adabiyotlar

1. Rivest R. **The MD5 Message-Digest Algorithm**. RFC 1321. Internet Engineering Task Force, 1992. MD5 algoritmi ixtiyoriy uzunlikdagi xabarni 128-bitli message digestga aylantirishi RFC 1321 da tavsiflangan.
2. Turner S., Chen L. **Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms**. RFC 6151. Internet Engineering Task Force, 2011. Ushbu hujjat MD5 va HMAC-MD5 bo'yicha xavfsizlik masalalarini yangilaydi.
3. National Institute of Standards and Technology. **Secure Hash Standard (SHS)**. FIPS PUB 180-4. NIST, 2015. Ushbu standart SHA-1 va SHA-2 oilasiga kiruvchi xavfsiz hash algoritmlarini belgilaydi.
4. National Institute of Standards and Technology. **FIPS 180-4, Secure Hash Standard**. CSRC, 2015. Hujjatda hash algoritmlar ma'lumot o'zgargan yoki o'zgarmaganini aniqlash uchun digest hosil qilishi ko'rsatilgan.
5. National Institute of Standards and Technology. **NIST Policy on Hash Functions**. CSRC. NIST SHA-1 dan SHA-2 yoki SHA-3 algoritmlariga o'tishni tavsiya qiladi.