VEB-ILOVALAR XAVFSIZLIGINI TA’MINLASHDA ZAMONAVIY KRIPTOGRAFIK USULLARNING QIYOSIY TAHLILI

Narpulatova Sabina Serik qizi
Talaba, ATT kafedrasi, 610-23-guruh
Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti
email: sabinanarpulatova33@gmail.com | Telefon: +998931000817
Zaripova Dilnoza Anvarovna
p.f.f.d., dotsent, ATT kafedrasi mudiri (ilmiy rahbar)
Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti
email: zaripovada85@gmail.com | Telefon: +998958888838

imrconf.com

Annotatsiya: *Ushbu maqolada veb-ilovalar xavfsizligini ta'minlashda qo‘llaniladigan zamonaviy kriptografik usullar - simmetrik (AES), assimetrik (RSA, ECC) va xeshlash (SHA-256, bcrypt) algoritmlari qiyosiy tahlil qilinadi. Har bir usulning ishlash tezligi, xavfsizlik darajasi va amaliy qo‘llanilish sohalari ko‘rib chiqiladi. Tadqiqot natijalari veb-ilovalar uchun eng maqbul kriptografik yechimlarni tanlashda amaliy ko'rsatmalar beradi.*

Kalit so‘zlar: *kriptografiya, veb-xavfsizlik, AES, RSA, bcrypt, SHA-256, ma’lumatlarni himoya qilish, shifrlash algoritmlari.*

Abstract: *This article presents a comparative analysis of modern cryptographic methods used to ensure web application security, including symmetric (AES), asymmetric (RSA, ECC), and hashing (SHA-256, bcrypt) algorithms. The study examines the performance speed, security level, and practical application areas of each method. The research results provide*

practical guidelines for selecting the most suitable cryptographic solutions for web applications.

Keywords: *cryptography, web security, AES, RSA, bcrypt, SHA-256, data protection, encryption algorithms.*

Kirish

Bugungi kunda internet va veb-ilovalar hayotimizning ajralmas qismiga aylangan. Bank tizimlaridan tortib tibbiyot xizmatlarigacha, ta'limdan tortib davlat boshqaruvigacha bo'lgan ko'plab sohalar veb-ilovalar orqali amalga oshirilmoqda. Jahon bank hisobotlariga ko'ra, 2023-yilda dunyo bo'ylab 5,4 milliard kishi internetdan faol foydalangan bo'lib, bu raqam yildan-yilga o'sib bormoqda. Shunday muhitda ma'lumotlar xavfsizligi global muammoga aylandi.

Kiber hujumlar soni va ulardan ko'rilayotgan zarar yildan-yilga keskin o'sib bormoqda. Cybersecurity Ventures ma'lumotlariga ko'ra, 2023-yilda global miqyosda kiber jinoyatlardan ko'rilgan iqtisodiy zarar 8 trillion AQSh dollarini tashkil etdi. Bu ko'rsatkich 2025-yilga kelib 10,5 trillion dollarga yetishi kutilmoqda. IBM Security hisobotiga ko'ra esa, bitta ma'lumotlar sizib chiqishi holatining o'rtacha narxi 4,45 million dollarga baholangan (IBM Cost of a Data Breach Report, 2023). Ayniqsa, veb-ilovalar orqali amalga oshiriladigan SQL-injection, XSS (Cross-Site Scripting), CSRF va brute-force hujumlari eng ko'p tarqalgan tahdidlar qatoridan o'rin olgan.

O'zbekiston Respublikasida ham axborot xavfsizligi masalasi davlat siyosati darajasida ko'rib chiqilmoqda. Prezidentimizning "Raqamli O'zbekiston - 2030" strategiyasi doirasida elektron hukumat xizmatlarini kengaytirish, raqamli iqtisodiyotni rivojlantirish va axborot kommunikatsiya texnologiyalarini barcha sohalarga joriy etish ko'zda tutilgan. O'zbekiston Respublikasining "Axborot xavfsizligi to'g'risida"gi qonuni va "Kiberxavfsizlik milliy markazi"ning tashkil etilishi ushbu yo'nalishdagi

imrconf.com

muhim qadamlar hisoblanadi. Biroq raqamlashtirish sur'ati tezlashgan sari axborot xavfsizligiga tahdidlar ham ko'payib bormoqda.

Veb-ilovalar xavfsizligini ta'minlashda kriptografik usullar asosiy himoya vositasi hisoblanadi. Biroq turli algoritmlarning afzalliklari va kamchiliklari haqida yaxlit tahlil etishmaydi. Ushbu tadqiqot aynan shu bo'shliqni to'ldirish maqsadida amalga oshirilgan.

Asosiy qism

1. Simmetrik kriptografik usullar (AES). AES (Advanced Encryption Standard) - hozirgi kunda eng ko'p qo'llanilgan simmetrik shifrlash standarti. U 128, 192 yoki 256 bitli kalitlar bilan ishlaydi. AES-ning asosiy afzalligi - yuqori ishlash tezligi: zamonaviy protsessorlarda sekundiga 10 GB dan ortiq ma'lumat shifrlanishi mumkin. Veb-ilovalarning HTTPS protokolida TLS/SSL sertifikatlari orqali ma'lumat uzatishda AES-256 standart sifatida qabul qilingan. Biroq asosiy kamchiligi - kalitlarni xavfsiz uzatish muammosi.

2. Assimetrik kriptografik usullar (RSA, ECC). RSA algoritmi ochiq va yopiq kalit juftligi asosida ishlaydi. 2048-bitli RSA hozircha xavfsiz hisoblanadi, lekin ishlash tezligi AES ga nisbatan 100-1000 marta sekinroq. ECC (Elliptic Curve Cryptography) esa RSA ga nisbatan kichikroq kalit o'lamlari bilan yuqori xavfsizlikni ta'minlaydi: 256-bitli ECC 3072-bitli RSA ga teng xavfsizlik beradi. Zamonaviy veb-serverlar asosan ECDHE algoritmidan foydalanadi.

3. Xeshlash algoritmlari (SHA-256, bcrypt). SHA-256 - bir tomonlama xeshlash funksiyasi bo'lib, ma'lumatlar yaxlitligini tekshirishda ishlatiladi. Parollarni saqlashda esa bcrypt, scrypt yoki Argon2 algoritmlari afzal, chunki ular sun'iy sekinlashtirishni qo'llab, brute-force hujumlariga chidamlilikni oshiradi. Masalan, bcrypt algoritmida "work factor" parametri orqali hisoblash murakkabligini boshqarish mumkin.

4. Qiyosiy tahlil natijalari. Tadqiqot ko'rsatishicha, veb-ilovalar xavfsizligi uchun eng samarali yondashuv - gibrid kriptografiya: ma'lumat

imrconf.com

uzatishda AES-256, kalit almashishda ECDHE, foydalanuvchi autentifikatsiyasida bcrypt/Argon2, ma'lumat yaxlitligi uchun SHA-256 kombinatsiyasidan foydalanish. Bu yondashuv ham yuqori xavfsizlikni, ham qabul qilingan ishlash tezligini ta'minlaydi.

Xulosa

Zamonaviy veb-ilovalar xavfsizligini ta'minlashda bitta kriptografik usulga tayanish yetarli emas. Gibrid yondashuv - simmetrik, assimetrik va xeshlash algoritmlarining optimal kombinatsiyasi - eng samarali himoya vositasi hisoblanadi. O'zbegistonda rivojlanayotgan raqamli iqtisodiyot va e-hukumat xizmatlarini kengaytirish jarayonida ushbu tamoyillarga amal qilish milliy axborot xavfsizligini mustahkamlashga muhim hissa qo'shadi. Kelajakdagi tadqiqotlar kvant kriptografiyasi va post-kvant algoritmlarini tahlil qilishga yo'naltirilishi maqsadga muvofiq.

FOYDALANILGAN ADABIYOTLAR

1. O'zbegiston Respublikasi Prezidentining "Axborot xavfsizligi to'g'risida"gi Qonuni. Toshkent. 2022.
2. NIST Special Publication 800-175B: Guideline for Using Cryptographic Standards in the Federal Government. 2020.
3. Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed. Pearson. 2022.
4. Bernstein D.J., Lange T. Post-quantum cryptography. Nature. 2017. No. 549. P. 188–194.
5. https://cybersecurityventures.com

imrconf.com