KRIPTOGRAFIYA VA TARMOQ XAVFSIZLIGIDAGI ROLI

Qodirov Farrux Egash o'g'li
Matematika va ta'limda axborot texnalogiyasi kafedrasi mudiri, ilmiy rahbar
Usmonova Diyora Uchqun qizi
Shahrisabz davlat pedagogika instituti matematika va informatika yo'nalishi
2- bosqich talabasi
https://doi.org/10.5281/zenodo.15117598

Annotatsiya: Ushbu maqolada kriptografiyaning tarmoq xavfsizligidagi roli, asosiy usullari va zamonaviy xavf-xatarlar oldini olishdagi ahamiyati tahlil qilinadi. Kriptografiya axborot xavfsizligini ta'minlashning muhim vositasi bo'lib, ma'lumotlarni shifrlash, autentifikatsiya qilish va butunlikni tekshirish kabi mexanizmlarni o'z ichiga oladi. Tarmoq xavfsizligida kriptografiya ma'lumotlarning maxfiyligi va yaxlitligini ta'minlash, hujumlardan himoyalash va ruxsatsiz kirishlarning oldini olish uchun foydalaniladi. Zamonaviy kriptografik algoritmlar, jumladan, assimetrik va simmetrik shifrlash usullari, raqamli imzolar va blokcheyn texnologiyalari kiberxavfsizlikni ta'minlashda muhim ahamiyatga ega hisoblanadi.

Kalit so'zlar: Kriptografiya, tarmoq xavfsizligi, shifrlash, autentifikatsiya, ma'lumotlar yaxlitligi, raqamli imzo, blokcheyn, simmetrik shifrlash, assimetrik shifrlash, kiberxavfsizlik.

Аннотация: В данной статье анализируется роль криптографии в обеспечении сетевой безопасности, основные методы и значение в предотвращении современных угроз. Криптография является важным инструментом информационной безопасности, включая механизмы шифрования данных, аутентификации и проверки целостности. В сетевой безопасности криптография используется для обеспечения конфиденциальности и целостности данных, защиты от атак и предотвращения несанкционированного доступа. Современные криптографические алгоритмы, включая симметричное и асимметричное шифрование, цифровые подписи и блокчейн-технологии, играют важную роль в обеспечении кибербезопасности.

Ключевые слова: Криптография, сетевая безопасность, шифрование, аутентификация, целостность данных, цифровая подпись, блокчейн, симметричное шифрование, асимметричное шифрование, кибербезопасность.

Annotation: This article analyzes the role of cryptography in network security, its key methods, and its significance in preventing modern threats. Cryptography is a crucial tool for information security, incorporating mechanisms such as data encryption, authentication, and integrity verification. In network security, cryptography is used to ensure data confidentiality and integrity, protect against attacks, and prevent unauthorized access. Modern cryptographic algorithms, including symmetric and asymmetric encryption, digital signatures, and blockchain technologies, play a vital role in ensuring cybersecurity.

Keywords: Cryptography, network security, encryption, authentication, data integrity, digital signature, blockchain, symmetric encryption, asymmetric encryption, cybersecurity.

Kirish. Axborot texnologiyalarining jadal rivojlanishi bilan birga, ma'lumotlarning xavfsizligini ta'minlash dolzarb masalaga aylandi. Zamonaviy dunyoda har kuni katta hajmdagi ma'lumotlar global tarmoqlar orqali uzatiladi va saqlanadi. Shu sababli, bu ma'lumotlarni ruxsatsiz kirish, o'zgartirish yoki o'g'irlashdan himoya qilish muhim ahamiyat kasb etadi. Kriptografiya tarmoq xavfsizligining ajralmas qismi bo'lib, ma'lumotlarni shifrlash,

autentifikatsiya qilish va yaxlitligini ta’minlash orqali axborotni himoya qiladi. Shifrlash algoritmlari axborot faqat vakolatli shaxslar tomonidan o‘qilishi va qayta ishlanishini ta’minlaydi, bu esa kiber hujumlarga qarshi samarali himoya vositalaridan hisoblanadi. Zamonaviy kriptografik usullar, simmetrik va assimetrik shifrlash, raqamli imzo va blokcheyn texnologiyalari, ma’lumotlarning xavfsizligini ta’minlashda keng qo‘llanilmoqda.

Asosiy qism. Kriptografiya bu — maxfiy kod yordamidagi yozishmalar. Ba’zan “kod” so‘zi o‘rniga “shifr” so‘zi ishlatiladi. Yuliy Sezar o‘zining maxfiy xabarlarini dushmanlardan himoya qilish uchun shifrni qo‘llagani ma’lum. Hozirgi kunda shifr va kodlar davlat hamda biznesning maxfiy yozishmalarida keng qo‘llaniladi. Kriptografiya tarmoq xavfsizligining ajralmas qismi bo‘lib, axborotni ruxsatsiz kirishlardan, o‘zgartirishlardan va firibgarlikdan himoya qiladi. Bugungi kunda ma’lumotlarni himoya qilish uchun turli kriptografik usullardan qo‘llaniladi. Shifrlash – axborotni maxfiy saqlash uchun uni kodlash. Shifrlash ikki asosiy turga bo‘linadi:

Simmetrik shifrlash (AES, DES) – bitta kalit yordamida shifrlash va deshifrlash amalga oshiriladi. Assimetrik shifrlash (RSA, ECC) – ikkita kalit (ochiq va yopiq) yordamida amalga oshiriladi.

Raqamli imzo – axborotning haqiqiyligini tasdiqlash va uning o‘zgartirilmaganligini kafolatlash vositasi. Xesh-funktsiyalar (SHA-256, MD5) – ma’lumotlar yaxlitligini tekshirish va autentifikatsiyani ta’minlash uchun ishlatiladi. Blokcheyn texnologiyasi – markazlashmagan va o‘zgartirib bo‘lmaydigan ma’lumotlar bazasi bo‘lib, tranzaktsiyalar xavfsizligini ta’minlaydi.

Tarmoq xavfsizligidagi muammolar. Hozirgi vaqtda tarmoq xavfsizligiga tahdid soluvchi muammolar quyidagilardan iborat: Ma’lumotlarni o‘g‘irlash va ruxsatsiz kirish – xakerlar tarmoqqa hujum qilib, maxfiy ma’lumotlarni qo‘lga kiritishlari mumkin. Man-in-the-Middle (MITM) hujumlari – ma’lumot almashinuvi jarayonida uchinchi tomon foydalanuvchilar o‘rtasidagi ma’lumotlarni o‘zgartirishi yoki o‘g‘irlashi mumkin. Zararli dasturlar va viruslar – tarmoq orqali tarqalib, ma’lumotlarni shifrlash, o‘chirish yoki o‘zgartirish bilan tahdid soluvchi zararli kodlar. Identifikatsiya va autentifikatsiya muammolari – parollarni buzish, qalbaki sertifikatlar orqali tizimga noqonuniy kirish xavfi mavjud. Kriptografik algoritmlarning buzilishi – eskirgan yoki zaif kriptografik algoritmlar (masalan, MD5 yoki SHA-1) xakerlar tomonidan buzilishi mumkin.

Muammolarning yechimlari. Kuchli shifrlash algoritmlaridan foydalanish – AES-256, RSA-4096 kabi zamonaviy shifrlash usullari ma’lumotlarni himoya qilishda yuqori darajada samarali hisoblanadi. Xavfsiz protokollardan foydalanish – ma’lumotlarni uzatishda SSL/TLS protokollaridan foydalanish hujumlarning oldini oladi. Ko‘p bosqichli autentifikatsiya (MFA) – faqat parol bilan cheklanmay, qo‘shimcha autentifikatsiya (SMS-kod, biometrik ma’lumotlar) tizimlarini joriy qilish kerak. Zararli dasturlarga qarshi vositalarni ishlatish – antivirus va xavfsizlik devorlarini (firewall) doimiy ravishda yangilab borish kerak . Raqamli sertifikatlar va ishonchli sertifikatlash markazlaridan foydalanish – autentifikatsiya jarayonini kuchaytirish muhim hisoblanadi.. Kriptografik tizimlarni doimiy ravishda yangilash – eskirgan algoritmlardan voz kechib, yangi va ishonchli texnologiyalarga o‘tish. Blokcheyn texnologiyasidan foydalanish – markazlashmagan tizimlar orqali ma’lumotlarning yaxlitligini ta’minlash va firibgarlikdan himoya qilish muhim hisoblanadi.

Kriptografiyaning kelajakdagi istiqbollari. Zamonaviy texnologiyalar rivojlanishi bilan birga, kriptografiyaning yangi yo‘nalishlari ham shakllanmoqda.

Kvant kriptografiyasi – kvant kompyuterlari paydo bo‘lishi bilan an’anaviy kriptografik usullar zaiflashishi mumkin, shuning uchun kvant shifrlash usullari ishlab chiqilmoqda.

Sun’iy intellekt va kriptografiya – AI yordamida kiberhujumlarni oldindan aniqlash va kriptografik tizimlarni optimallashtirish.

Post-kvant kriptografiya – kvant kompyuterlariga qarshi bardosh bera oladigan yangi algoritmlar ishlab chiqilmoqda.

Kriptologiya ikki yo‘nalish, ya’ni kriptografiya va kriptotaxlildan iborat. Kriptografiyaning vazifasi xabarlarning maxfiyligini va haqiqiyligini ta’minlashdan iborat. Kriptotahlilning vazifasi esa kriptograflar tomonidan ishlab chiqilgan himoya tizimini ochishdan iborat.

Kriptografiya va tarmoq xavfsizligi bir-biri bilan uzviy bog‘liq bo‘lib, zamonaviy axborot texnologiyalarida muhim rol o‘ynaydi. Kelajakda yanada kuchliroq va bardoshli kriptografik tizimlar ishlab chiqilishi axborot xavfsizligini mustahkamlashga yordam beradi.

Mavzuga doir adabiyotlar tahlili. Kriptografiya va tarmoq xavfsizligi bo‘yicha olib borilgan tadqiqotlar axborot texnologiyalarining rivojlanishi bilan yanada dolzarb bo‘lib bormoqda.

Kriptografiya nazariyasiga oid ilk ilmiy ishlanmalar Klod Shenonning "Communication Theory of Secrecy Systems" (1949) asariga borib taqaladi. U kriptografik tizimlarning matematik asoslarini belgilab, shifrlash algoritmlarining mustahkamligini tahlil qildi. Bugungi kunda William Stallingsning "Cryptography and Network Security: Principles and Practice" kitobi kriptografiyaning asosiy tamoyillarini tushuntiruvchi eng muhim manbalardan biri hisoblanadi.

Simmetrik va assimetrik shifrlash usullari bo‘yicha Bruce Schneierning "Applied Cryptography" asari keng qo‘llanilib, unda AES, RSA, DES va boshqa algoritmlar tafsilotlari keng yoritilgan. Zamonaviy shifrlash usullarining tahlili bo‘yicha Menezes, van Oorschot va Vanstonening "Handbook of Applied Cryptography" kitobi ham asosiy manbalardan biri sifatida tavsiya etiladi.

Kriptografiyaning kelajagi va yangi tendensiyalar. Kvant kompyuterlar paydo bo‘lishi bilan an’anaviy kriptografik tizimlarning zaiflashish xavfi oshmoqda. Ushbu sohadagi ilmiy ishlanmalar orasida Michele Moscaning "Quantum Computing and Post-Quantum Cryptography" asari post-kvant kriptografiyasi bo‘yicha asosiy manbalardan biri hisoblanadi. Shuningdek, sun’iy intellekt va kriptografiyaning integratsiyasini o‘rganish bo‘yicha David J. Handning "Artificial Intelligence and Cybersecurity: Advances and Challenges" asari kiberxavfsizlikda AI imkoniyatlarini keng miqyosda ochib beradi.

Xulosa. Kriptografiya va tarmoq xavfsizligi zamonaviy axborot texnologiyalarining ajralmas qismi bo‘lib, ma’lumotlarni ruxsatsiz kirishlardan, buzilishlardan va firibgarliklardan himoya qilishda muhim hisoblanadi. Tarmoq xavfsizligiga tahdid soluvchi muammolar, jumladan, ma’lumotlarni o‘g‘irlash, MITM hujumlari, zararli dasturlar va viruslar, autentifikatsiya muammolari hamda eskirgan kriptografik algoritmlar xavfi yoritildi. Ushbu muammolarni hal qilish uchun kuchli shifrlash algoritmlaridan foydalanish, xavfsiz protokollarni qo‘llash (SSL/TLS, VPN), ko‘p bosqichli autentifikatsiya tizimlarini joriy etish,

zararli dasturlarga qarshi vositalarni ishlatish va blokcheyn texnologiyalaridan foydalanish tavsiya etildi.

Kelajakda kvant kriptografiyasi, sun'iy intellekt asosida kiberxavfsizlikni mustahkamlash va blokcheyn texnologiyalarining rivojlanishi axborot xavfsizligini yangi bosqichga olib chiqishi kutilmoqda. Xulosa qilib aytganda, axborot xavfsizligini ta'minlash uchun kriptografiya vositalaridan to'g'ri foydalanish, zamonaviy tahdidlarga mos ravishda himoya strategiyalarini ishlab chiqish va yangi texnologiyalardan foydalanish muhim ahamiyat kasb etadi. Kelajakda ushbu soha yanada rivojlanib, tarmoq xavfsizligini ta'minlashning yangi usullari va yo'nalishlari paydo bo'lishi kutilmoqda.

Foydalanilgan adabiyotlar/Используемая литература/References:

1. Кодиров, Ф. Э., and О. Д. Дониёров. "ЭФФЕКТИВНЫЕ МОДЕЛИ РАЗВИТИЯ МЕДИЦИНСКОГО ОБСЛУЖИВАНИЯ НАСЕЛЕНИЯ КАШАКАДЬИНСКОЙ ОБЛАСТИ." Символ науки 7-2 (2022): 15-17.
2. Zoxidov, J. B., F. E. Qodirov, and I. J. Bozorova. "QUARTUS II PROJECT CONCEPT AND ITS OPPORTUNITIES AND PROBLEMS." АКТУАЛЬНЫЕ ПРОБЛЕМЫ ТЕХНИЧЕСКОГО И ТЕХНОЛОГИЧЕСКОГО ОБЕСПЕЧЕНИЯ ИННОВАЦИОННОГО РАЗВИТИЯ. 2019.
3. Uzakov, Gulom, et al. "Simulation of a tubular pyrolysis reactor using comsol multiphysics software." International Scientific and Practical Conference Digital and Information Technologies in Economics and Management. Cham: Springer Nature Switzerland, 2023.
4. Қодиров, Ф. "ХУДУДЛАРДА ТИББИЙ ХИЗМАТЛАРНИ ДАСТУРИЙ ПАКЕТЛАР ЁРДАМИДА ЭЛЕКТРОН ТИББИЙ БАЗАСИНИ ЯРАТИШ." O'zbekiston Respublikasi Oliy Va o'rta Maxsus ta'lim Vazirligi Namangan Muhandislik-Qurilish Instituti (2022).
5. Qodirov, F. E., O. D. Doniyorov, and H. Shokirov Sh. "Basic concepts of information security in information systems. Wide threats and their consequences." концепции устойчивого развития науки в современных условиях (2021): 153-155.
6. Bozorova, Irina Jumanazarovna, and Dilfuzaxon Mamasharipovna Karayeva. "Modern programming technologies and their role." интеллектуальный капитал xxi века. 2020.
7. Ergash o'g'li, Qodirov Farrux. "Hududlarni ijtimoiy-iqtisodiy rivojlantirishda har bir hududning o 'ziga xos xususiyatlari." Scientific Journal of Actuarial Finance and Accounting 4.09 (2024): 178-183.
8. Qodirov, Farrux, and Muxlisa Mavlonova. "O'ZBEKISTONDA ZIYORATGOH VA QADAMJOLAR, TURIZM XIZMATLARINI JADAL RIVOJLANTIRISH ISTIQBOLLARI." YANGI O 'ZBEKISTONDA MILLIY TURIZM ISTIQBOLLARI 1.01 (2024).
9. Qodirov, F., N. Sirojev, and S. Negmatova. "FEATURES OF THE ANDROID STUDIO SOFTWARE PACKAGE." Академические исследования в современной науке 2.17 (2023): 130-146.
10. Қодиров, Ф. Э., et al. "ДЛЯ ПРОВЕРКИ МОДЕЛЕЙ АДЕКВАТНОСТИ, ЧУВСТВИТЕЛЬНОСТЬ И СОПРОТИВЛЕНИЯ." ИНТЕГРАЦИЯ НАУКИ, ОБЩЕСТВА, ПРОИЗВОДСТВА И ПРОМЫШЛЕННОСТИ. 2019.11. Qodirov, F. E., D. A. Akbarova, and S. H. Shokirov. "SOFTWARE FOR WORKING WITH COMPUTER GRAPHICS AND THEIR TASKS. APPLICATION OF DIGITAL IMAGE PROCESSING FIELDS." (2021): 57-58.

11. Jumanazarovna, Bozorova Irina, and Kodirov Farruh Ergash O'G'Li. "Principle of electrocardiographic work and its role in modern medicine." Вопросы науки и образования 15 (99) (2020): 31-36.
12. Kodirov, F. E., and J. E. Nematov. "BASIC TECHNOLOGY AND SERVICE MANAGEMENTMULTISERVICE NETWORKS." Инновации в технологиях и образовании: сб. ст. участников XII Между (2019): 214.
13. Қодиров, Ф. Э., and Ж. Э. Нематов. "РАЗВИТИЕ ЛОКАЛЬНОЙ СЕТИ НА ОСНОВЕ ТЕХНОЛОГИИ GPON." Инновации в технологиях и образовании: сб. ст. участников XII Между (2019): 288.
14. Кодиров, Ф. Э., and М. У. Маматмурадова. "РАЗРАБОТКА ЦИФРОВОЙ ПРОГРАММЫ ШИФРОВАНИЯ И ВНЕДРЕНИЕ В ПРАКТИКУ." Инновации в технологиях и образовании: сб. ст. участников XII Между (2019): 275.
15. Абдирасулов, Ж. У., and Ф. Э. Кодиров. "ЭФФЕКТИВНОСТЬ ANGULAR JS ДЛЯ СОЗДАНИЯ ДИНАМИЧЕСКИХ ВЕБ-САЙТОВ И ОПТИМИЗАЦИИ ИХ ПРОИЗВОДИТЕЛЬНОСТИ." Инновации в технологиях и образовании: сб. ст. участников XII Между (2019): 228.
16. Qodirov, F. E., J. B. Zohidov, and H. I. Karamatova. "ADVANTAGES OF PROGRAMMING LANGUAGES JAVASCRIPT, JAVA AND PYTHON." МОДЕЛИРОВАНИЕ И АНАЛИЗ СЛОЖНЫХ ТЕХНИЧЕСКИХ И ТЕХНОЛОГИЧЕСКИХ СИСТЕМ. 2019.
17. Qodirov, F. E., J. U. Abdirasulov, and J. E. Nematov. "FORMING GOVERNMENT AGENCY WEBSITES WITH WORDPRESS CONTENT MANAGEMENT SYSTEM." Инновации в технологиях и образовании: сб. ст. участников XII Между (2019): 219.
18. Турдиев, У. К., and Ф. Э. Кодиров. "Задача Коши Для Одномерной Системы Уравнений Типа Бюргерса Возникающей В Двухскоростной Гидродинамике." Инновации в технологиях и образовании: сб. ст. участников XI Между (2018): 349.
19. Qodirov, F. E. "Methodological aspects and importance of development of medical services through econometric modeling and forecasting options." academy. uz/index. php/yo.