KRIPTOGRAFIYA VA SHIFRLASH USULLARI

Qodirov Farrux Ergash o'g'li
Shahrisabz davlat pedagogika instituti "Matematika va ta'limda axborot texnologiyasi kafedrasi mudiri, Ilmiy rahbar
Jomurodova Go'zal Abror qizi
Shahrisabz davlat pedagogika instituti matematika va informatika yo'nalishi 2-bosqich talabasi

https://doi.org/10.5281/zenodo.15117899

Annotatsiya. Ushbu maqolada quyidagi asosiy jihatlar ta'kidlangan: Kriptografiya tushunchasi – ma'lumotlarni shifrlash va himoya qilish sohasi ekanligi. Asosiy tamoyillar – maxfiylik, yaxlitlik, autentifikatsiya va inkorsizlantirish tushunchalari. Kriptografiya turlari – Simmetrik shifrlash (AES, DES) – tezkor, ammo kalit almashinuvi muammosi bor. Assimetrik shifrlash (RSA, ECC) – ochiq va yopiq kalitdan foydalanadi. Xesh-funksiyalar (SHA-256, MD5) – ma'lumot yaxlitligini tekshiradi. Amaliy qo'llanilishi – Internet xavfsizligi (SSL/TLS, HTTPS). Elektron imzo. Blokcheyn texnologiyasi (kriptovalyutalar). Bank tizimlari va moliyaviy xavfsizlik. Kriptografiya zamonaviy axborot xavfsizligida muhim rol o'ynaydi va texnologiyalar rivoji bilan birga takomillashib boradi va kriptografik shifrlash usullari haqida batafsil ma'lumot berilgan. Shifrlashning asosiy turlari va ularning ishlash usullari tasvirlangan.

Ka'lit so'zlar. Kriptografiya, Shifrlash , Kalit , Axborot xavfsizligi, Maxfiylik , Yaxlitlik , Autentifikatsiya , Inkorsizlantirish , Shifrlash turlari, Simmetrik shifrlash , Assimetrik shifrlash , Xesh-funksiyalar , Kvant shifrlash , Shifrlash usullari, Sezar shifri , Vijiner shifri , Skital shifri .

Abstract. This article highlights the following key points: The concept of cryptography is the field of data encryption and protection. The main principles are the concepts of confidentiality, integrity, authentication and non-repudiation. Types of cryptography – Symmetric encryption (AES, DES) – fast, but has the problem of key exchange. Asymmetric encryption (RSA, ECC) – uses a public and private key. Hash functions (SHA-256, MD5) – checks the integrity of information. Practical application – Internet security (SSL/TLS, HTTPS). Electronic signature. Blockchain technology (cryptocurrencies). Banking systems and financial security. Cryptography plays an important role in modern information security and is improving with the development of technologies, and detailed information about cryptographic encryption methods is provided. The main types of encryption and how they work are described.

Keywords. Cryptography, Encryption, Key, Information Security, Confidentiality, Integrity, Authentication, Non-repudiation, Types of encryption, Symmetric encryption, Asymmetric encryption, Hash functions, Quantum encryption, Encryption methods, Caesar cipher, Vigenière cipher, Skital cipher.

Абстрактный. В этой статье освещаются следующие ключевые моменты: Концепция криптографии – это область шифрования и защиты данных. Основными принципами являются концепции конфиденциальности, целостности, аутентификации и неотказуемости. Виды криптографии – Симметричное шифрование (AES, DES) – быстрое, но есть проблема с обменом ключами. Асимметричное шифрование (RSA, ECC) – использует открытый и закрытый ключ. Хэш-функции (SHA-256, MD5) — проверяет целостность данных. Приложение – Интернет-безопасность (SSL/TLS, HTTPS). Электронная подпись. Технология блокчейн (криптовалюты).

Банковские системы и финансовая безопасность. Криптография играет важную роль в современной информационной безопасности и продолжает совершенствоваться по мере развития технологий, а методы криптографического шифрования подробно описаны. Описаны основные типы шифрования и принципы их работы.

Ключевые слова. Криптография, Шифрование, Ключ, Информационная безопасность, Конфиденциальность, Целостность , Аутентификация , Отрицание , Типы шифрования, Симметричное шифрование, Асимметричное шифрование , Хэш-функции , Квантовое шифрование , Методы шифрования , Шифр Цезаря , Шифр Виджинера , Шифр Скитала.

Kriptografiya – bu ma’lumotlarni shifrlash va himoya qilish usullarini o‘rganadigan fan sohasi bo‘lib, uning asosiy maqsadi axborot xavfsizligini ta’minlashdir. U tarixan maxfiy yozishmalarni shifrlash usullaridan boshlab, bugungi kunda zamonaviy kompyuter tarmoqlari va elektron tizimlarda axborotni himoya qilish uchun ishlatiladigan murakkab algoritmlargacha rivojlangan. Kriptografiya simmetrik va assimetrik shifrlash usullariga bo‘linadi. Simmetrik shifrlashda bir xil kalitdan foydalangan holda ma’lumotlar shifrlanadi va qayta ochiladi. Assimetrik shifrlashda esa ochiq va yopiq kalit juftligi ishlatiladi, bu esa xavfsizlikni oshirishga imkon beradi. Hozirgi kunda RSA, AES, ECC kabi kriptografik algoritmlar keng qo‘llaniladi. Shuningdek, kriptografiya elektron imzo, blokcheyn, tarmoq xavfsizligi va maxfiy aloqa sohalarida muhim ahamiyatga ega. Uning amaliy qo‘llanilishi bank tizimlarida, internet xavfsizligida va davlat axborot tizimlarida keng tarqalgan. Kriptografiyaning rivojlanishi kiberxavfsizlikni mustahkamlashga xizmat qiladi va axborotning maxfiyligi, yaxlitligi hamda autentifikatsiyasini ta’minlashda asosiy vositalardan biri hisoblanadi.

Kriptografiyaning asosiy tamoyillari. Maxfiylik (Confidentiality): Faqat ruxsat berilgan shaxslar ma’lumotni ko‘ra olishi mumkin. Yaxlitlik (Integrity): Ma’lumot uzatish yoki saqlash jarayonida o‘zgartirilmaganligiga ishonch hosil qilish. Autentifikatsiya (Authentication): Foydalanuvchi yoki tizim haqiqiyligini tasdiqlash. Inkorsizlantirish (Non-repudiation): Foydalanuvchilar amalga oshirgan harakatlarini inkor eta olmasligi.

Kriptografiyaning amaliy qo‘llanilishi: Kriptografiya zamonaviy axborot texnologiyalarida keng qo‘llaniladi. HTTPS, SSL/TLS protokollari veb-saytlar orqali xavfsiz ma’lumot almashinuvini ta’minlaydi. Elektron imzo: Hujjatlarning autentifikatsiyasini va ularning o‘zgartirilmaganligini ta’minlaydi. Blokcheyn texnologiyasi: Kriptografiya blokcheyn va kriptovalyutalar, jumladan, Bitcoin va Ethereum kabi tizimlarning xavfsizligini ta’minlaydi. Bank va moliyaviy tizimlar: Kredit kartalari, onlayn to‘lov tizimlari va elektron banking xavfsizligini ta’minlash uchun ishlatiladi. Kriptografiya bugungi kunda axborot xavfsizligi uchun muhim vosita bo‘lib, internetdan foydalanuvchilar, korxonalar va davlat tashkilotlari uchun ishonchli muhofaza tizimini yaratishga xizmat qiladi. Zamonaviy texnologiyalar rivojlanishi bilan birga kriptografik usullar ham takomillashib boradi va kiberxavfsizlik sohasida yanada muhim rol o‘ynaydi.

Kriptografiya uchta asosiy tamoyilga tayanadi:

1. Maxfiylik (Confidentiality) – faqat ruxsat etilgan shaxslar ma’lumotdan foydalana olishi.

2. Butunlik (Integrity) – ma’lumotlar ruxsatsiz o‘zgartirilmasligi.

3. Autentifikatsiya (Authentication) – ma’lumot jo‘natuvchining haqiqiyligini tasdiqlash.

Shifrlash usullari ikki asosiy turga bo‘linadi:

1. Simmetrik shifrlash (Symmetric Encryption)
2. Assimetrik shifrlash (Asymmetric Encryption)

Shifrlashning asosiy turlari va ularning ishlash usullari quyidagicha tasvirlangan: An’anaviy shifrlash usullari – Sezar shifri, Vijiner shifri va Skital shifri kabi qadimiy shifrlash usullari, ularning ishlash prinsiplari va kamchiliklari yoritilgan. Simmetrik shifrlash algoritmlari – AES, DES, Blowfish, Twofish kabi algoritmlar tushuntirilgan. Ushbu usullarda bir xil kalit ishlatilishi sababli tezkor ishlaydi, ammo kalit almashinuvi xavfsizlik muammosi tug‘dirishi mumkin. Assimetrik shifrlash algoritmlari – RSA, ECC, ElGamal kabi tizimlarda ikki xil kalit (ochiq va yopiq) ishlatilishi va ularning afzalliklari ko‘rsatib o‘tilgan. Bu usullar xavfsizroq, lekin ko‘proq hisoblash resurslari talab qiladi. Xesh-funksiyalar orqali shifrlash – MD5, SHA-256, SHA-3 kabi xesh algoritmlari tushuntirilgan. Ushbu usullar ma’lumotning yaxlitligini tekshirish va autentifikatsiya uchun ishlatiladi. Kvant shifrlash – BB84 protokoli kabi yangi texnologiyalar kelajakda kriptografiyada inqilob qilishi mumkinligi haqida qisqacha ma’lumot berilgan.

Kriptografik shifrlash usullari ma’lumot xavfsizligini ta’minlash uchun muhim. AES va RSA kabi zamonaviy algoritmlar keng qo‘llaniladi, kelajakda esa kvant kriptografiya yanada ishonchli tizimlarga asos bo‘lishi mumkin. Shifrlash usullari ma’lumotlarni himoya qilish uchun muhim vosita hisoblanadi. Simmetrik shifrlash tezkor, ammo kalit almashinuvi muammosi bor. Assimetrik shifrlash esa xavfsizroq, lekin resurs talab qiladi. Zamonaviy xavfsizlik tizimlarida AES, RSA va ECC kabi algoritmlar keng qo‘llaniladi. Shu bilan birga, kvant shifrlash kelajakda yanada ishonchli texnologiya bo‘lishi mumkin.

Foydalanilgan adabiyotlar/Используемая литература/References:

1. Ergash o’g’li, Qodirov Farrux, and Berdiyev Sardor Sobir o’g’li. "DEVELOPMENT OF MATHEMATICAL APPLICATIONS IN THE PROGRAM OF EXISTING SCRIPT LANGUAGE."
2. Qodirov, F. E., S. S. Jo'rayev, and V. N. Qalandarov. "INFORMATION ARCHITECTURE IN SITE DESIGN." НАУКА И НАУЧНЫЙ ПОТЕНЦИАЛ-ОСНОВА УСТОЙЧИВОГО ИННОВАЦИОННОГО РАЗВИТИЯ ОБЩЕСТВА. 2019.
3. Qodirov, F. E., et al. "FEATURES OF INTEL CORE i9 X-SERIES PROCESSORS AND ITS ADVANTAGE FROM OTHER PROCESSORS." ПУТИ ПОВЫШЕНИЯ РЕЗУЛЬТАТИВНОСТИ СОВРЕМЕННЫХ НАУЧНЫХ ИССЛЕДОВАНИЙ. 2019.
4. Ergash o’g’li, Qodirov Farrux, and Bozorova Irina Jumanazarovna. "METHODS OF DISPLAYING MAIN MEMORY ON CACHE." Ответственный редактор (2020): 6.
5. Qodirov, F. E. "Methodological aspects and importance of development of medical services through econometric modeling and forecasting options." academy. uz/index. php/yo.
6. 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.
7. 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.
8. Қодиров, Ф. "ЗАМОНАВИЙ КОМПЬЮ ТЕР УЙИНЛАРИ ВА УЛАРНИНГ СИНФЛАНИШИ." МУХАММАД АЛ-ХОРАЗМИЙ НОМИДАГИ ТОШКЕНТ АХБОРОТ

ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ КАРШИ ФИЛИАЛИ (2019).
9. Qodirov, F. "YOSHLAR MA'NAVIYATINI YUKSALTIRISHDA MILLIY ONLAYN KITOB DO'KONINI ISHLAB CHIQISH VA TADBIQ ETISH." МУХАММАД АЛ-ХОРАЗМИЙ НОМИДАГИ ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ КАРШИ ФИЛИАЛИ (2019).
10. Qodirov, F. "MASOFAVIY TA'LIMDA O'QISHNING QULAYLIKLARI VA KAMCHILIKLARI." МУҲАММАД АЛ-ХОРАЗМИЙ НОМИДАГИ ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҚАРШИ ФИЛИАЛИ (2020).
11. Ergash o'g'li, Qodirov Farrux. "ECONOMETRIC MODELING OF THE DEVELOPMENT OF MEDICAL SERVICES TO THE POPULATION OF THE REGION." Berlin Studies Transnational Journal of Science and Humanities 2.1.1 Economical sciences (2022).
12. Кодиров, Ф. "АНАЛИЗ БИОСИГНАЛОВ В ЭЛЕКТРОКАРДИОГРАФИИ И МЕТОДЫ ИХ ОБРАБОТКИ." МУҲАММАД АЛ-ХОРАЗМИЙ НОМИДАГИ ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҚАРШИ ФИЛИАЛИ (2020).
13. Қодиров, Ф. "СОЗДАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И АППАРАТА ЭЛЕКТРОННОЙ БИБЛИОТЕЧНОЙ СИСТЕМЫ НА ОСНОВЕ QR-КОДОВОЙ ТЕХНОЛОГИИ." Kokand University (2020).
14. Bozorova, Irina Jumanazarovna, and Dilfuzaxon Mamasharipovna Karayeva. "Modern programming technologies and their role." интеллектуальный капитал xxi века. 2020.
15. Qodirov, F. "Aholiga tibbiy xizmat ko 'rsatish sohasining kelgusi holatini bashoratlash." Samarqand iqtisodièt va servis instituti (2022).
16. Qodirov, F. "QR-kod texnologiyasi asosida elektron kutubxona tizimini dasturiy va apparat taminotini yaratish." Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Qarshi filiali (2021).
17. Қодиров, Фаррух, and Х. Мухитдинов. "АҲОЛИГА ТИББИЙ ХИЗМАТ КЎРСАТИШДАН ОЛИНГАН ДАРОМАД ВА ХАРАЖАТЛАРНИ БИЗНЕС ИННОВАЦИОН МОДЕЛИ." Raqamli iqtisodiyot va axborot texnologiyalari 2.3 (2022): 136-141.
18. Qodirov, F. "Optimum solutions for the development of medical services in private clinics." Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Qarshi filiali (2022).
19. Qodirov, F. "Қашқадарё ҳудуди аҳолисига хизмат кўрсатиш тармоқлари ва уларга таъсир этувчи омиллар." O 'zbekiston Qishloq Va Suv xo 'jaligi" Jurnali (2022).
20. Қодиров, Ф. "Вилоят аҳолисига соғлиқни сақлаш хизматлари кўрсатиш тармоқлари ривожланиш механизмининг статистик таҳлили." Andijon Mashinasozlik Instituti (2022).
21. Қодиров, Ф. "Аҳолига тиббий хизмат кўрсатиш соҳасининг келгуси ҳолатини башоратлаш." Самарқанд иқтисодиèт ва сервис институти (2022).
22. Қодиров, Фаррух, and Х. Мухитдинов. "АҲОЛИГА ТИББИЙ ХИЗМАТ КЎРСАТИШДАН ОЛИНГАН ДАРОМАД ВА ХАРАЖАТЛАРНИ БИЗНЕС ИННОВАЦИОН МОДЕЛИ." Raqamli iqtisodiyot va axborot texnologiyalari 2.3 (2022): 136-141.
23. Қодиров, Ф. "Қашқадарё вилояти аҳолисига тиббий хизмат кўрсатиш тармоқларини ривожлантиришнинг истиқболлари." o 'zbekiston qishloq va suv xo 'jaligi» ãà «Agro ilm (2022).
24. Бозорова, Ирина Жуманазаровна. "Создание программного обеспечения электронной библиотечной системы на основе QR-кодовой технологии." Теория и

практика современной науки. 2020.
25. 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.
26. Маматмурадова, М. У., И. Ж. Бозорова, and Ф. Э. Кодиров. "СОЗДАНИЕ И ЭФФЕКТИВНОЕ ИСПОЛЬЗОВАНИЕ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ И РЕСУРСОВ ЭЛЕКТРОННОГО ОБУЧЕНИЯ В НЕПРЕРЫВНОМ ОБРАЗОВАНИИ." Инновации в технологиях и образовании. 2019.
27. Ergash o'g'li, Qodirov Farrux, and Bozorova Irina Jumanazarovna. "METHODS OF DISPLAYING MAIN MEMORY ON CACHE." Ответственный редактор (2020): 6.