VOLUME II | ISSUE 3 | MAY-JUNE | 2024

Journal of RESEARCH and INNOVATIONS

ТАДҚИҚОТ ВА ИННОВАЦИЯЛАР | ИССЛЕДОВАНИЯ И ИННОВАЦИИ

SPECIAL ISSUE

ISSN: 2181-4058

Available online at www.imfaktor.com

IMFAKTOR
Science driven pages

ISSN: 2181-4058
DOI Journal 10.56017/2181-4058

ТАДҚИҚОТ ВА ИННОВАЦИЯЛАР ЖУРНАЛИ

II-ЖИЛД, 3 СОН

ЖУРНАЛ ИССЛЕДОВАНИЯ И ИННОВАЦИИ

ТОМ-II, НОМЕР 3

JOURNAL OF RESEARCH AND INNOVATIONS

VOLUME-II, ISSUE 3

ТОШКЕНТ - 2024

ТАДҚИҚОТ ВА ИННОВАЦИЯЛАР ЖУРНАЛИ

ЖУРНАЛ ИССЛЕДОВАНИЯ И ИННОВАЦИИ | JOURNAL OF RESEARCH AND INNOVATIONS

№ 3 (2024) DOI http://dx.doi.org/10.56017/2181-4058-2024-3

Бош муҳаррир:

Салимов А. – архитектура фанлари доктори, профессор

Масъул муҳаррир:

Кадиров К. – филология фанлари номзоди, доцент

Таҳририят аъзолари:

1. Закиров Х. – қишлоқ хўжалиги фанлари номзоди, профессор
2. Гулмуродов Р. – қишлоқ хўжалиги фанлари доктори, профессор
3. Якубжон Хатамович Юлдашов – қишлоқ хўжалик фанлари номзоди, профессор,
4. Камалова Дильфуза Энуаровна – филология ф.б.ф.д (PhD)
5. Раззақов Шухрат Турсунович – техника фанлари номзоди, доцент
6. Чоршанбиев Шухрат Махматмуродович – техника ф.б.ф.д. (PhD), доцент
7. Нематов Эркинжон Ҳамроевич – техника ф.б.ф.д (PhD), доцент
8. Бобокалонов Одилшоҳ Остонович – филология ф.б.ф.д (PhD)
9. Абдуллаева Садокат Шоназаровна – техника ф.б.ф.д (PhD)
10. Шарипов Козимжон Комилжонович – техника ф.б.ф.д (PhD)
11. Норматов Ғайрат Алижанович – техника ф.б.ф.д (PhD)
12. Бозорова Гульмира Зайниддиновна – филология ф.б.ф.д (PhD)
13. Убайдуллаев Фарход Бахтияруллаевич – қишлоқ хўжалиги ф.б.ф.д (PhD)
14. Каримова Дилафрўз Ҳалимовна Филология – филология ф.б.ф.д (PhD)
15. Маҳмудова Муаттар Мақсатуллаевна – филология ф.б.ф.д (PhD)
16. Юлдашева Дилафруз Махамадалиевна – филология фанлари доктори

“Тадқиқот ва инновациялар” журнали 2022 йил 22 декабрь куни № 054912-сонли гувоҳнома билан оммавий ахборот воситаси сифатида давлат рўйхатидан ўтказилган.

Мазкур журнал 6 та халқаро маълумотлар базаларида индексланган бўлиб, жорий йил учун UIF 2023 = 7.1 “импакт-фактор” кўрсатгичига эга. Ўзбекистон Республикаси Олий таълим, фан ва инновациялар вазирлиги ҳузуридаги Олий аттестация комиссиясининг 2023 йил 24 июлдаги 01-02/1199-сонли хатига мувофиқ ушбу журналда чоп этилган мақолалар хорижий мақолалар сифатида тан олинади.

Саҳифаловчи\Page Maker\Верстка: Абдураҳмон Хасанов

Таҳририят манзили: Тошкент шаҳар, Учтепа тумани, “Ватан” МФЙ, Чилонзор 24-мавзеси, 2/27-уй. Почта индекси 100152. Веб-сайт: www.imfaktor.uz/com

Телефон номер: +99894-410 11 55, **E-mail:** tahririyat@imfaktor.uz

© “IMFAKTOR Pages” илмий нашриёти , 2024 йил.

© Муаллифлар жамоаси, 2024 йил.

ISSN: 2181-4058
www.imfaktor.uz

ТАДҚИҚОТ ВА ИННОВАЦИЯЛАР ЖУРНАЛИ

ЖУРНАЛ ИССЛЕДОВАНИЯ И ИННОВАЦИИ | JOURNAL OF RESEARCH AND INNOVATIONS

РАДЖАБОВ Нодирбек Боходирович
Высококвалифицированный инженер
в области восстановления информации
из различных носителей
Главный инженер Recovery.uz
https://doi.org/10.5281/zenodo.12570131

ИСТОРИЯ И ЭВОЛЮЦИЯ ШИФРОВАНИЯ ДАННЫХ: ОТ ЭНИГМЫ ДО БЛОКЧЕЙНА

АННОТАЦИЯ

Шифрование данных играет ключевую роль в обеспечении информационной безопасности в современном мире. В данной статье рассматривается история шифрования от машины Энигма до современных методов, таких как блокчейн. Также обсуждаются преимущества и недостатки шифрования, возможные риски и ошибки пользователей, включая потерю ключа, а также использование TPM 2.0 для защиты данных.

Технологии шифрования в настоящее время играют важную роль в обеспечении информационной безопасности. В данной статье рассматриваются история шифрования, современные методы и технологии шифрования, их преимущества и недостатки, а также ошибки и риски при шифровании. Темы, такие как машина Энигма, симметричное и асимметричное шифрование, блокчейн технологии, освещены.

Ключевые слова: шифрование, информация, безопасность, Enigma, симметрия, шифрование, асимметрия, шифрование, блок, TPM 2.0.

THE HISTORY AND EVOLUTION OF DATA ENCRYPTION: FROM ENIGMA TO BLOCKCHAIN

ANNOTATION

Data encryption plays a key role in ensuring information security in the modern world. This article examines the history of encryption from the Enigma machine to modern methods such as blockchain. The advantages and disadvantages of encryption, possible risks and user errors, including key loss, and the use of TPM 2.0 to protect data are also discussed.

Encryption technologies play a crucial role in ensuring information security today. This article covers the history of encryption, modern methods and technologies of encryption, their advantages and disadvantages, as well as errors and risks in encryption. Topics such as the Enigma machine, symmetric and asymmetric encryption, blockchain technologies are highlighted.

Keywords: encryption, information, security, Enigma, symmetry, encryption, asymmetry, encryption, block, TPM 2.0.

MA’LUMOTLARNI SHIFRLASH TARIXI VA EVOLYUTSIYASI: ENIGMADAN BLOCKCHAINGA

ANNOTATSIYA

Ma’lumotlarni shifrlash zamonaviy dunyoda axborot xavfsizligini ta'minlashda asosiy rol o‘ynaydi. Ushbu maqola Enigma mashinasidan blokcheyn kabi zamonaviy usullarga shifrlash tarixini o‘rganadi. Shifrlashning afzalliklari va kamchiliklari, yuzaga kelishi mumkin bo‘lgan xavflar va foydalanuvchi xatolari, shu jumladan kalitlarni yo‘qotish va ma’lumotlarni himoya qilish uchun TPM 2.0 dan foydalanish ham muhokama qilinadi.

Hozirgi vaqtda axborot xavfsizligini ta'minlashda shifrlash texnologiyalari muhim o‘rin tutadi. Ushbu maqolada shifrlash tarixi, zamonaviy shifrlash usullari va texnologiyalari, ularning afzalliklari va kamchiliklari, shuningdek shifrlashdagi xato va xavflar muhokama qilinadi. Enigma mashinasi, simmetrik va assimetrik shifrlash, blokcheyn texnologiyasi kabi mavzular yoritilgan.

Kalit so‘zlar: shifrlash, axborot, xavfsizlik, Enigma, simmetriya, shifrlash, assimetriya, shifrlash, blokcheyn, TPM 2.0

Шифрование данных сегодня является важнейшим инструментом для обеспечения информационной безопасности. Эта статья рассматривает историю и эволюцию шифрования данных, современные методы и технологии шифрования, а также их значение для безопасности.

1. История шифрования. 1.1. Машина Энигма.

Энигма была криптографической машиной, используемой немецкой армией во время Второй мировой войны для шифрования сообщений. Ее алгоритмы шифрования считались неприступными, пока британские криптографы не смогли взломать шифр Энигмы, что сыграло значительную роль в исходе войны.

Здесь должна быть фотография машины Энигма.

1.2. Развитие шифрования после Второй мировой войны.

После войны развитие шифрования продолжилось с появлением симметричного и асимметричного шифрования. Были разработаны такие стандарты, как DES, AES и RSA, которые используются до сих пор [1].

2. Современные методы шифрования. 2.1. Симметричное и асимметричное шифрование.

Симметричное шифрование использует один ключ для шифрования и дешифрования данных. Асимметричное шифрование использует пару ключей: открытый и закрытый. Симметричное шифрование быстрее и эффективнее, но имеет проблему с безопасной передачей ключей. Асимметричное шифрование обеспечивает высокую безопасность, но медленнее.

Здесь должна быть схема симметричного и асимметричного шифрования

2.2. Шифрование на лету. Это процесс шифрования данных в реальном времени во время их передачи. Это обеспечивает безопасность данных во время передачи [2].

3. Важность и польза шифрования.

Шифрование данных защищает конфиденциальные данные, финансовую информацию и персональные данные от несанкционированного доступа и кибератак. Важность шифрования в корпоративном и государственном секторах невозможно переоценить [3].

4. Потенциальные риски и ошибки. 4.1. Потеря ключа шифрования.

Потеря ключа шифрования может привести к невозможности доступа к данным. Методы восстановления и меры предосторожности играют важную роль в предотвращении таких ситуаций.

4.2. TPM 2.0.

TPM 2.0 (Trusted Platform Module) используется для безопасного хранения ключей шифрования. Это устройство повышает уровень безопасности данных на различных устройствах.

Здесь должна быть фотография TPM 2.0

5. Хранение данных на серверах.

Шифрование данных на серверах важно для защиты государственной и личной информации. Это обеспечивает безопасность данных и предотвращает несанкционированный доступ.

6. Блокчейн и шифрование. 6.1. Что такое блокчейн.

Блокчейн – это распределенный и децентрализованный реестр, который используется для записи транзакций и данных таким образом, чтобы они были неизменяемыми и защищенными от несанкционированного доступа. Блокчейн состоит из цепочки блоков, где каждый блок содержит набор транзакций или данных, хэш предыдущего блока и временную метку.

6.2. Принципы работы блокчейна.

Каждый блок в блокчейне связан с предыдущим блоком с помощью криптографического хэша. Этот хэш создается на основе содержимого блока и хэша предыдущего блока, что обеспечивает целостность и неизменяемость данных. Внесение изменений в один блок потребует изменения всех последующих блоков, что делает подделку данных в блокчейне практически невозможной.

6.3. Применение шифрования в блокчейне.

Шифрование играет ключевую роль в защите данных в блокчейне. Оно используется для обеспечения конфиденциальности транзакций и данных. В блокчейне применяются как симметричные, так и асимметричные алгоритмы шифрования. Симметричное шифрование используется для защиты данных во время передачи, а асимметричное шифрование – для аутентификации пользователей и создания цифровых подписей [4].

6.4. Преимущества блокчейна.

Прозрачность: Все участники сети могут видеть все транзакции, что обеспечивает высокий уровень прозрачности.

- **Безопасность**: благодаря криптографическим методам защиты и децентрализации, данные в блокчейне защищены от несанкционированного доступа и подделки.

- **Независимость**: Отсутствие централизованного органа управления позволяет исключить возможность злоупотребления властью и повысить доверие между участниками сети.

6.5. Применение блокчейна в различных отраслях.

- **Финансовый сектор**: Блокчейн используется для проведения безопасных и быстрых транзакций, а также для создания криптовалют.

- **Логистика и цепочки поставок**: Блокчейн помогает отслеживать движение товаров и предотвращать подделки [5].

- **Медицина**: Защита медицинских данных и обеспечение их целостности.

- **Государственное управление**: Создание прозрачных систем голосования и управление государственными регистрами.

Заключение.

Шифрование данных и блокчейн являются важнейшими инструментами для обеспечения информационной безопасности и доверия в цифровом мире. Эти технологии продолжают развиваться и находить новые применения в различных отраслях, предлагая инновационные решения для защиты данных и улучшения прозрачности процессов.

ИҚТИБОСЛАР. СНОСКИ. REFERENCES.

1. Сингх С. Книга шифров. – М.: Мир, 1999.
2. Шнайер Б. Прикладная криптография. – М.: Техносфера, 2006.
3. NIST. Advanced Encryption Standard (AES). – 2001.
4. Trusted Computing Group. TPM 2.0 спецификации. – 2014.
5. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. – 2008.

ISSN: 2181-4058
DOI Journal 10.56017/2181-4058

ТАДҚИҚОТ ВА ИННОВАЦИЯЛАР ЖУРНАЛИ

II-ЖИЛД, 3 СОН

ЖУРНАЛ ИССЛЕДОВАНИЯ И ИННОВАЦИИ

ТОМ-II, НОМЕР 3

JOURNAL OF RESEARCH AND INNOVATIONS

VOLUME-II, ISSUE 3

«Тадқиқот ва инновациялар» электрон журнали 2022 йил 22 декабрь куни № 054912-сонли гувоҳнома билан оммавий ахборот воситаси сифатида давлат рўйхатидан ўтказилган.

Муассис: «**IMFAKTOR Pages**» масъулияти чекланган жамияти.

Таҳририят манзили: 100152, Тошкент шаҳри, Учтепа тумани, “Ватан” МФЙ, Чилонзор 24-мавзеси, 2-уй.

Телефон номер: +99894-410 11 55

Эл. почта: tahririyat@imfaktor.uz

Веб-сайт: www.imfaktor.uz