Т. 9. №12. 2023
https://doi.org/10.33619/2414-2948/97

УДК 004.056 https://doi.org/10.33619/2414-2948/97/05

ВОПРОСЫ ПРАКТИЧЕСКОГО ПРИМЕНЕНИЯ КРИПТОГРАФИИ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДАННЫХ

©Карпов М. А., *ORCID: 0009-0004-8794-625X, SPIN-код: 3979-5250,*
Поволжский государственный университет телекоммуникаций и информатики,
г. Самара, Россия, Themaks000@mail.ru
©Лиманова Н. И., *ORCID: 0000-0003-2924-5602, SPIN-код: 9799-8380, д-р техн. наук,*
Поволжский государственный университет телекоммуникаций и информатики,
г. Самара, Россия, nataliya.i.limanova@gmail.com

ISSUES OF PRACTICAL APPLICATION OF CRYPTOGRAPHY TO ENSURE DATA SECURITY

©Karpov M., *ORCID: 0009-0004-8794-625X, SPIN-code: 3979-5250,*
Povolzhskiy State University of Telecommunications and Informatics,
Samara, Russia, Themaks000@mail.ru
©Limanova N., *ORCID: 0000-0003-2924-5602, SPIN-code: 9799-8380, Dr. habil.,*
Povolzhskiy State University of Telecommunications and Informatics,
Samara, Russia, nataliya.i.limanova@gmail.com

Аннотация. В современном обществе цифровые технологии внедрились в повседневную жизнь, увеличивая риск утечки данных. Криптография становится ключевым средством обеспечения конфиденциальности, целостности и аутентичности информации. Однако применение криптографии сталкивается с вызовами, такими как угрозы для систем безопасности данных и постоянное развитие методов взлома. Недостаточное осознание пользователями важности безопасности, использование слабых паролей, появление квантовых компьютеров и невнимательность к защите данных увеличивают уязвимость. Для решения проблем предложен комплексный подход, включающий образование, улучшение стандартов безопасности, разработку квантово-устойчивых методов, совершенствование технологий аутентификации и активное обновление методов шифрования. Рассматриваются современные методы шифрования, включая симметричные и асимметричные алгоритмы и примеры их использования в повседневной жизни, охватывая сферы от банковских транзакций до мессенджеров и электронной почты.

Abstract. In modern society, digital technologies have become embedded in everyday life, increasing the risk of data leakage. Cryptography is becoming a key means of ensuring the confidentiality, integrity and authenticity of information. However, the application of cryptography faces challenges such as threats to data security systems and the constant development of hacking techniques. Lack of user awareness of the importance of security, use of weak passwords, the advent of quantum computers and inattention to data protection increase vulnerability. To solve the problems, a comprehensive approach has been proposed, including education, improving security standards, developing quantum-resistant methods, improving authentication technologies and actively updating encryption methods. Modern encryption methods are reviewed, including symmetric and asymmetric algorithms and examples of their use in everyday life, covering areas from banking transactions to instant messengers and email.

Т. 9. №12. 2023
https://doi.org/10.33619/2414-2948/97

Ключевые слова: безопасность данных, криптография, симметричные алгоритмы, асимметричные алгоритмы, шифрование.

Keywords: data security, cryptography, symmetric algorithms, asymmetric algorithms, encryption.

В современном информационном обществе, где цифровые технологии стали неотъемлемой частью повседневной жизни, обеспечение безопасности данных становится критически важным аспектом. Каждый день мы взаимодействуем с различными электронными устройствами, передаем чувствительную информацию через интернет, проводим финансовые операции онлайн. В такой среде, где обмен информацией стал неотъемлемой частью нашего быта, риск утечки и несанкционированного доступа к данным значительно возрастает [1].

Применение криптографии в повседневной жизни становится ключевым инструментом для обеспечения конфиденциальности, целостности и аутентичности информации. Будь то защита личных персональных данных, шифрование сообщений в мессенджерах или обеспечение безопасности онлайн-транзакций, криптографические методы играют решающую роль в предотвращении кибератак и сохранении доверия в цифровом пространстве.

На сегодняшний день применение криптографии для обеспечения безопасности данных сталкивается с рядом вызовов и проблем. С одной стороны, с развитием технологий и повсеместным использованием цифровых средств общения и хранения информации расширяются возможности для злоумышленников проводить атаки на системы и нарушать безопасность данных. С другой стороны, сами методы криптографии также постоянно развиваются, а существующие стандарты могут оказаться уязвимыми перед новыми методами взлома [2].

Одной из основных проблем является недостаточное осознание пользователями важности применения криптографии и соблюдения базовых правил безопасности. Часто люди используют слабые пароли, не обеспечивают шифрование информации на своих устройствах или недостаточно внимательны к защите своих личных данных, что делает их уязвимыми к кибератакам. Также с развитием квантовых вычислений стоит и вопрос об устойчивости существующих алгоритмов криптографии, поскольку они могут стать уязвимыми к атакам нового типа. Это поднимает вопрос о необходимости разработки и внедрения новых квантово-устойчивых криптографических методов [3].

Для решения описанных проблем в области применения криптографии с целью обеспечения безопасности данных, в работе предлагается комплексный подход, включающий следующие шаги.

1. Образование и повышение осведомленности:

- проведение образовательных программ для пользователей о важности безопасности данных, методах шифрования и базовых правилах безопасности;
- регулярные кампании по информированию о новых угрозах и методах защиты.

2. Улучшение стандартов безопасности:

- развитие и внедрение более строгих стандартов безопасности в различных отраслях, таких как финансы, здравоохранение и государственные службы;
- обязательная сертификация систем и приложений на соответствие высоким стандартам безопасности.

Т. 9. №12. 2023
https://doi.org/10.33619/2414-2948/97

3. Разработка и внедрение квантово-устойчивых криптографических методов:

- инвестирование в исследования и разработку квантово-устойчивых алгоритмов шифрования, которые были бы устойчивы к атакам квантовых вычислений;

- постепенное внедрение этих методов в системы обработки данных.

4. Совершенствование технологий аутентификации:

- использование биометрических методов аутентификации для усиления безопасности доступа к устройствам и данным;

- развитие и внедрение многофакторной аутентификации для предотвращения несанкционированного доступа.

5. Активное обновление методов шифрования:

- регулярное обновление и адаптация криптографических алгоритмов с учетом последних открытий в области криптоанализа;

- поощрение обновления программного обеспечения и устройств для использования последних версий безопасных протоколов.

Далее поясним суть шифрования данных в общем и рассмотрим основные сферы применения криптографии. Криптология — это область науки, которая изучает два основных процесса: шифрование и дешифрование. В ее состав входят криптография, занимающаяся разработкой и анализом математических методов преобразования данных, и криптоанализ, который оценивает эффективность методов шифрования, а также разрабатывает методы для их взлома [4].

Современным средством обеспечения безопасности данных является шифрование. Этот процесс включает в себя обратимое преобразование открытого текста с использованием определенного алгоритма, чтобы получить набор бессмысленных данных. Эти данные становятся недоступными для лиц, не обладающих определенным секретным ключом. Основной целью шифрования является обеспечение конфиденциальности передаваемой информации. Каждый алгоритм шифрования характеризуется использованием ключа, который определяет конкретное преобразование данных. Зашифрованная информация может быть расшифрована только с использованием того же ключа, который может принадлежать отдельному пользователю или группе пользователей. Шифрование применяется для защиты информации при хранении в ненадежных местах и передаче по открытым каналам связи. Этот процесс включает два взаимосвязанных этапа: данные зашифровываются перед отправкой или сохранением, а затем расшифровываются для восстановления исходных данных (Рисунок) (https://kurl.ru/xdKdY). Алгоритмы шифрования подразделяются на две основные категории: симметричные и асимметричные. В симметричных методах как отправитель, так и получатель используют общий секретный ключ для обеспечения шифрования и расшифровки данных. В случае асимметричных методов отправитель использует открытый ключ для шифрования, в то время как получатель расшифровывает данные при помощи закрытого ключа [5].

Один из наиболее известных и эффективных алгоритмов симметричного шифрования — это Advanced Encryption Standard (AES). Он применяется для защиты личных файлов на компьютерах, шифрования трафика в сети Wi-Fi (например, с использованием протокола WPA2) и в сфере онлайн-банкинга для обеспечения безопасности финансовых операций. Другим примером симметричного шифрования является алгоритм Data Encryption Standard (DES), который, несмотря на свою устаревшую криптографическую стойкость, все еще может применяться в некоторых контекстах, но в современных приложениях часто заменяется более надежным вариантами, такими как Triple-DES (3DES).

Т. 9. №12. 2023
https://doi.org/10.33619/2414-2948/97

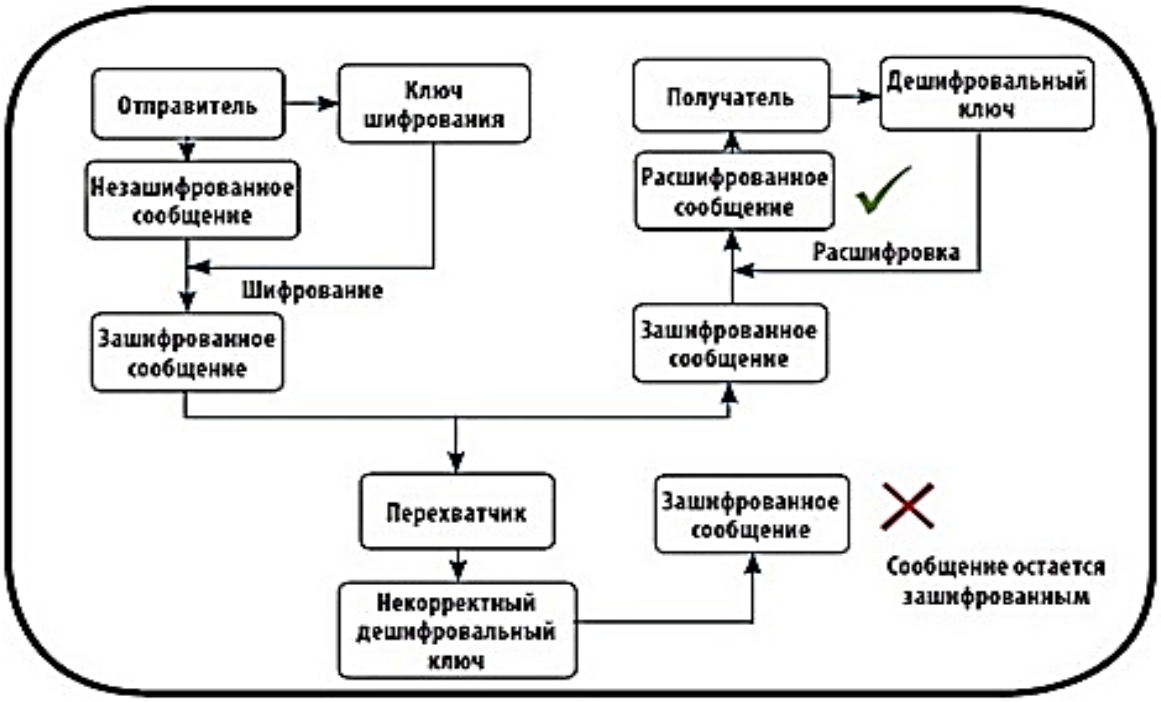

Рисунок. Упрощенная схема криптографической системы

Среди асимметричных алгоритмов шифрования наиболее распространенным является RSA (Rivest–Shamir–Adleman), который применяется для защиты данных, передаваемых по электронной почте, и создания цифровых подписей. Другим примером асимметричного алгоритма является ECC (Elliptic Curve Cryptography), который активно используется в сфере криптовалют, таких как биткоин, для создания уникальных ключей и обеспечения безопасности транзакций. ECC обладает высокой стойкостью к криптоанализу при более низкой потребности в вычислительных ресурсах по сравнению с классическими алгоритмами. Асимметричное шифрование часто используется для обеспечения безопасного соединения между веб-браузером и сервером в протоколах SSL/TLS, которые предназначены для безопасной передачи данных в интернете (например, при онлайн-покупках). Также оба типа алгоритмов часто используются в комбинации, чтобы сочетать преимущества каждого. Например, асимметричные алгоритмы могут использоваться для безопасной передачи симметричных ключей, которые применяются для последующего шифрования данных.

В заключении следует отметить, что применение криптографии в повседневной жизни играет ключевую роль в обеспечении безопасности данных. В настоящее время технологии криптографии встроены в различные аспекты, начиная от безопасности банковских транзакций и защиты личных данных в сети до обеспечения безопасности мессенджеров и электронной почты. Все это подчеркивает важность понимания и применения криптографии в повседневной цифровой среде, поскольку она служит фундаментальным инструментом для защиты личных и конфиденциальных данных, создавая основу для безопасности в современном информационном обществе.

Список литературы:

1. Бороненко Т. А., Кайсина А. В., Пальчикова И. Н., Федоркевич Е. В., Федотова В. С. Основы цифровой грамотности и кибербезопасности. СПб.: ЛГУ им. А.С. Пушкина, 2021. 431 с.

2. Гатченко Н. А., Исаева А. С., Яковлев. А. Д. Криптографическая защита информации. СПб: НИУ ИТМО, 2012. 142 с.

3. Коржик В. И., Яковлев В. А. Основы криптографии. СПб., ИЦ Интермедия, 2016. 296 с.

4. Бауэр Ф. Расшифрованные секреты. Методы и принципы криптологии. М.: Мир, 2007. 550 с.

5. Карачаев А. Р., Шогенов З. А., Курбанов Т. К., Пашаева Ф. Р. Методы защиты и технология шифрования данных // Образование и право. 2022. №9. С. 145-149. https://doi.org/10.24412/2076-1503-2022-9-145-149

References:

1. Boronenko, T. A., Kajsina, A. V., Pal'chikova, I. N., Fedorkevich, E. V., & Fedotova, V. S. (2021). Osnovy cifrovoj gramotnosti i kiberbezopasnosti. St. Petersburg. (in Russian).

2. Gatchenko, N. A., Isaeva, A. S., & Jakovlev,. A. D. (2012). Kriptograficheskaja zashhita informacii. St. Petersburg. (in Russian).

3. Korzhik, V. I., & Jakovlev, V. A. (2016). Osnovy kriptografii. St. Petersburg. (in Russian).

4. Baujer, F. (2007). Rasshifrovannye sekrety. Metody i principy kriptologii. Moscow. (in Russian).

5. Karachaev, A. R., Shogenov, Z. A., Kurbanov, T. K., & Pashaeva, F. R. (2022). Metody zashhity i tehnologija shifrovanija dannyh. *Obrazovanie i pravo,* (9), 145-149. (in Russian). https://doi.org/10.24412/2076-1503-2022-9-145-149

Работа поступила
в редакцию 19.11.2023 г.

Принята к публикации
24.11.2023 г.

Ссылка для цитирования:

Карпов М. А., Лиманова Н. И. Вопросы практического применения криптографии для обеспечения безопасности данных // Бюллетень науки и практики. 2023. Т. 9. №12. С. 47-51. https://doi.org/10.33619/2414-2948/97/05

Cite as (APA):

Karpov, M., & Limanova, N. (2023). Issues of Practical Application of Cryptography to Ensure Data Security. *Bulletin of Science and Practice, 9*(12), 47-51. (in Russian). https://doi.org/10.33619/2414-2948/97/05