УДК 004.056.55

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ШИФРОВАНИЯ ДАННЫХ

М.М. Ходжамаммедов, Дж.Р. Абдыев
Государственный энергетический институт Туркменистана, Мары, Туркменистан

Аннотация. В данной статье рассматриваются ключевые аспекты шифрования данных как важного инструмента защиты информации в цифровом мире. Обсуждаются основные методы шифрования, такие как симметричное и асимметричное шифрование, а также современные алгоритмы, включая AES и RSA. Особое внимание уделяется применению шифрования в различных сферах, таких как банковская деятельность, электронная коммерция и защита личных данных. Рассматриваются проблемы и вызовы, связанные с использованием шифрования, включая управление ключами и производительность систем. В заключение подчеркивается важность шифрования в обеспечении конфиденциальности и безопасности информации.
Ключевые слова: дата, AES, RSA, DES.

THE URGENT PROBLEMS OF DATA ENCRYPTION

M.M. Hojamammedov, J.R. Abdyyev
The State Energy Institute of Turkmenistan, Mary, Turkmenistan

Abstract. The article examines the key aspects of data encryption as an essential tool for information protection in the digital world. It discusses the main encryption methods, such as symmetric and asymmetric encryption, as well as modern algorithms, including AES and RSA. Special attention is given to the application of encryption in various fields, such as banking, e-commerce, and personal data protection. The challenges and issues associated with encryption are also considered, including key management and system performance. In conclusion, the importance of encryption in ensuring the confidentiality and security of information is emphasized.
Keywords: data, AES, RSA, DES

Введение

С развитием информационных технологий и увеличением объемов передаваемой и хранимой информации возросла потребность в надежных методах защиты данных. Шифрование данных стало одним из основных инструментов, позволяющих обеспечить конфиденциальность и безопасность информации. Эта статья направлена на изучение основных методов шифрования, их применения и связанных с ними проблем.

Основные методы шифрования. Шифрование данных делится на два основных типа: симметричное и асимметричное.

1. Симметричное шифрование: Использует один и тот же ключ для шифрования и дешифрования данных. Примеры: DES, AES. AES (Advanced Encryption Standard) является наиболее распространенным алгоритмом на сегодняшний день, обеспечивая - 218 - высокий уровень безопасности и производительности.

2. Асимметричное шифрование: Использует пару ключей: открытый и закрытый. Открытый ключ используется для шифрования, а закрытый – для дешифрования. Примером является RSA (Rivest– Shamir–Adleman), который часто применяется для безопасной передачи данных и цифровой подписи.

Шифрование данных находит широкое применение в различных областях.

1. Банковская деятельность: защита транзакций и личной информации клиентов.

2. Электронная коммерция: обеспечение безопасности онлайн-платежей и защиты личных данных пользователей.

3. Защита личных данных: шифрование данных на устройствах и в облачных хранилищах.

Проблемы и вызовы. Несмотря на эффективность шифрования, существуют проблемы, требующие внимания:

1. Управление ключами: Эффективное управление ключами является критически важным для обеспечения безопасности шифрованных данных. Утечка или потеря ключа может привести к утрате доступа к защищенной информации.

2. Производительность: Шифрование может негативно сказаться на производительности систем, особенно при обработке больших объемов данных.

3. Регуляторные требования: Существуют различные нормативные акты, требующие использования шифрования для защиты персональных данных, что может усложнять его внедрение.

Шифрование данных является важным элементом обеспечения безопасности информации в современном цифровом мире. С учетом растущих угроз кибербезопасности, понимание и правильное применение методов шифрования становятся необходимыми для защиты конфиденциальности и целостности данных. Важно продолжать развивать и совершенствовать технологии шифрования, а также обучать пользователей методам защиты информации.

Список использованных источников

1. Алексеев.И.В. (2020). Основы шифрования и криптографии». М.: Наука.
2. Дьяков. А.Н. (2021). Современные методы шифрования данных». М.: Горячая линия Телеком
3. Сухов. И.П. (2019). Безопасность информации: шифрование и защита - 219 - данных». СПб.: Питер.
4. Шаповалов. В.В. (2022). Криптография: теория и практика». М.: Альпина Паблишер
5. Кузнецов. А.Ю. (2021). «Информационная безопасность в цифровом обществе». М.: ИНФРА-М.

Сведения об авторах

Ходжамаммедов М.М, преподаватель. Государственный энергетический институт Туркменистана. mekanhoja2021@gmail.com.
Абдыев Дж.Р, преподаватель. Государственный энергетический институт Туркменистана. abdyýewjuma@gmail.com.

Information about the authors

Hojamammedov M.M, teacher. The State Energy Institute of Turkmenistan, mekanhoja2021@gmail.com.
Abdyyev J.R, teacher, The State Energy Institute of Turkmenistan, abdyýewjuma@gmail.com.