УДК 004.056

АНАЛИЗ УСТОЙЧИВОСТИ СОВРЕМЕННЫХ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

А.М. Хамраев, А.Б. Суннатов
Государственный энергетический институт Туркменистана, Мары, Туркменистан

Аннотация. В данной работе анализируются современные криптографические алгоритмы, включая симметричные и асимметричные системы шифрования, а также хеш-функции. Рассматриваются их преимущества, недостатки и уязвимости в контексте традиционных и современных атак. Особое внимание уделено угрозам со стороны квантовых вычислений и перспективам постквантовой криптографии. Работа завершается обсуждением актуальных вызовов и тенденций в области криптографической защиты данных.
Ключевые слова: AES; хэш-функции; постквантовые; криптосистема; суперсингулярные.

ANALYSIS OF THE RESILIENCE OF MODERN CRYPTOGRAPHIC ALGORITHMS

A.M. Hamrayev, A.B. Sunnatov
The State Energy Institute of Turkmenistan, Mary, Turkmenistan

Abstract. This paper analyzes modern cryptographic algorithms, including symmetric and asymmetric encryption systems, as well as hash functions. Their advantages, disadvantages, and vulnerabilities in the context of traditional and modern attacks are examined. Particular attention is paid to threats from quantum computing and the prospects of post-quantum cryptography. The paper concludes with a discussion of current challenges and trends in the field of cryptographic data protection.
Keywords: AES; hash functions; post-quantum; cryptosystem; supersingular.

Введение

Криптография является основой цифровой безопасности, защищая данные в финансовых системах, коммуникациях, облачных сервисах и других сферах. Однако эволюция атакующих технологий, таких как квантовые компьютеры, ставит под угрозу традиционные алгоритмы шифрования. Эта статья анализирует современные криптографические алгоритмы с точки зрения их устойчивости, обсуждает их слабые стороны и прогнозирует будущее развития этой области.

Современные криптографические алгоритмы: структура и особенности

Симметричные алгоритмы используют единый ключ для шифрования и дешифрования.

AES (Advanced Encryption Standard). Устойчив к большинству известных атак, поддерживает длину ключа 128, 192 и 256 бит. Уязвимости: атаки полного перебора остаются единственным реальным способом взлома, но требуют огромных вычислительных ресурсов.

ChaCha20. Обеспечивает высокую скорость шифрования, устойчив к криптоаналитическим атакам. Преимущества: энергоэффективность, что делает его подходящим для мобильных устройств.

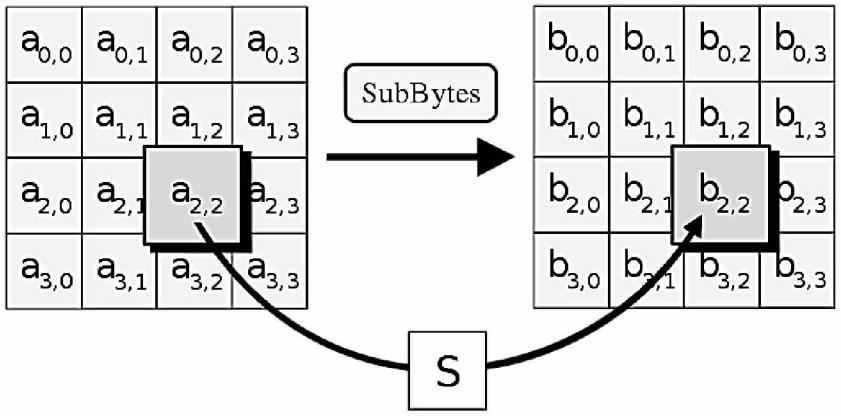

Рис. 1. SubBytes() трансформация при шифровании
Fig. 1. SubBytes() transformation during encryption

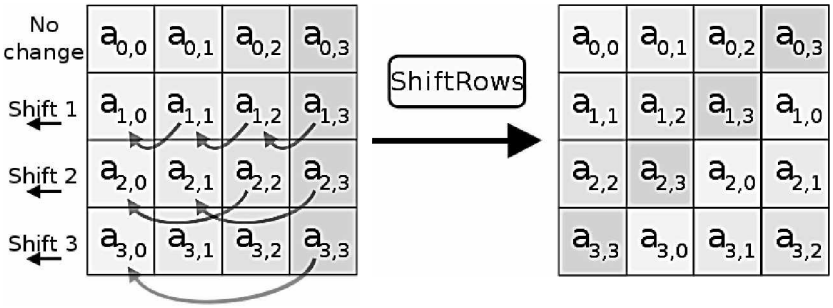

Рис. 2. ShiftRows() трансформация при шифровании
Fig. 2. ShiftRows() transformation during encryption

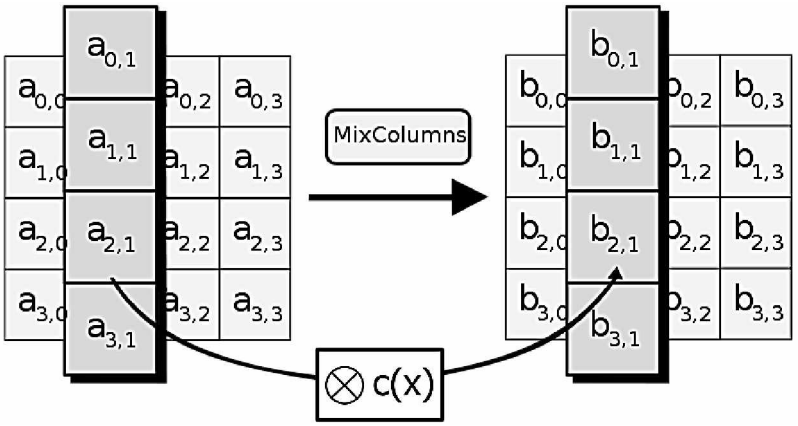

Рис. 3. MixColumns() трансформация при шифровании
Fig. 3. MixColumns() transformation during encryption

Асимметричные алгоритмы шифрования

Основаны на использовании пары ключей: публичного и приватного.

RSA. Основан на сложности факторизации больших чисел. Уязвимости: уязвим к квантовым атакам (алгоритм Шора).

Эллиптические кривые (ECC). Предлагают повышенную устойчивость при меньшем размере ключа по сравнению с RSA. Уязвимости: аналогично RSA, уязвимы к атакам квантовых компьютеров.

Хеш-функции. Используются для проверки целостности данных и создания цифровых подписей.

SHA-2 и SHA-3. Устойчивы к большинству современных атак, за исключением квантовых угроз. Уязвимости: квантовые атаки (например, атака Гровера) могут сократить сложность нахождения коллизий.

MD5 и SHA-1. Устарели из-за высокого риска коллизий.

Методы атак на криптографические алгоритмы следующие.

1. Атаки полного перебора. Основаны на переборе всех возможных ключей. Противодействие: увеличение длины ключа.

2. Криптоаналитические атаки. Линейный и дифференциальный анализ (применимы к симметричным алгоритмам).

3. Атаки на основе подобранных шифротекстов.

4. Атаки на основе квантовых вычислений: Алгоритм Шора: эффективен для решения задач факторизации и дискретного логарифма. Алгоритм Гровера: снижает сложность перебора ключей в два раза.

Угрозы квантовых вычислений

Квантовые компьютеры могут коренным образом изменить криптографический ландшафт. Для асимметричных алгоритмов угроза особенно велика:

– RSA и ECC становятся уязвимыми при наличии достаточно мощного квантового компьютера.

– Симметричные алгоритмы (например, AES) остаются более устойчивыми, но требуют увеличения длины ключа.

Постквантовые криптографические алгоритмы

Для защиты от квантовых атак разрабатываются постквантовые алгоритмы, основанные на задачах, устойчивых к квантовым вычислениям:

– Решеточные криптосистемы (Lattice-based):

– Основаны на сложных задачах, связанных с многомерными решетками. Примеры: NTRU, Kyber.

– Кодовые криптосистемы (Code-based):

– Основаны на декодировании случайных линейных кодов. Пример: McEliece.

– Суперсингулярные изогении эллиптических кривых:

– Используют вычисления на изогениях эллиптических кривых.

Проблемы и вызовы

1. Рост вычислительных ресурсов: Постквантовые алгоритмы требуют большего объема памяти и времени выполнения.

2. Необходимость стандартизации: Институт NIST проводит соревнования по выбору устойчивых алгоритмов, но процесс внедрения остается медленным.

3. Совместимость: Требуется адаптация существующих систем для работы с новыми стандартами.

4. Экономические затраты: Внедрение постквантовой криптографии требует значительных инвестиций.

Заключение

Современные криптографические алгоритмы демонстрируют высокую устойчивость к традиционным атакам. Однако квантовые вычисления требуют перехода к новым методам шифрования, способным выдерживать атаки будущего. Постквантовая криптография становится важнейшим направлением исследований,

предлагая алгоритмы, которые смогут защитить данные даже в условиях квантовых угроз.

Список использованных источников / References

1. Daemen, J., & Rijmen, V. (2002). The Design of Rijndael: AES - The Advanced Encryption Standard. Springer.

2. Rivest, R. L., Shamir, A., & Adleman, L. (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM. 21(2). 120-126.

3. NIST. (2016). SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions.

4. Bernstein, D. J., & Lange, T. (2017). Post-Quantum Cryptography. Springer.

5. Shor, P. W. (1997). "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". SIAM Journal on Computing, 26(5), 1484–1509.

Сведения об авторах

Хамраев А.М., преподаватель. Государственный энергетический институт Туркменистана, pvm87818@gmail.com.
Сунатов А.Б., студент. Государственный энергетический институт Туркменистана, pvm87818@gmail.com.

Information about the authors

Hamrayev A., teacher. The State Energy Institute of Turkmenistan, pvm87818@gmail.com.
Sunnatov A., student. The State Energy Institute of Turkmenistan, pvm87818@gmail.com.