СОВРЕМЕННАЯ КРИПТОГРАФИЯ И РОЛЬ МАТЕМАТИКИ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Гульширин Тойчиевна Амангельдыева, ст. преподаватель
Карьягдыев Максат Довлетович, ст. преподаватель
Институт телекоммуникаций и информатики Туркменистана, Ашхабад, Туркменистан

Аннотация. В статье рассматриваются современные подходы к криптографии как к ключевому элементу информационной безопасности. Особое внимание уделено роли высшей математики, включая теорию чисел, алгебру, комбинаторику и теорию вероятностей, в разработке криптографических алгоритмов. Обозначены тенденции развития постквантовой криптографии и применение математических структур, таких как эллиптические кривые и решётки. Статья подчеркивает необходимость дальнейших исследований в области криптографической устойчивости в условиях развития квантовых вычислений.

Ключевые слова: криптография, информационная безопасность, математика, эллиптические кривые, квантовые вычисления, постквантовая криптография

Modern cryptography and the role of mathematics in ensuring information security

Institute of Telecommunacations and Informatics of Turkmenistan, Ashgabat, Turkmenistan

Abstract: This article explores modern approaches to cryptography as a fundamental component of information security. Particular attention is given to the role of advanced mathematics—number theory, algebra, combinatorics, and probability theory—in the development of cryptographic algorithms. It outlines emerging trends in post-quantum cryptography and the use of mathematical structures such as elliptic curves and lattices. The article emphasizes the necessity for further research in cryptographic resistance in the era of quantum computing.

Keyworls: cryptography, information security, mathematics, elliptic curves, quantum computing, post-quantum cryptography.

Современное общество всё больше зависит от цифровых технологий, что делает защиту информации приоритетной задачей. Криптография как наука об обеспечении конфиденциальности, целостности и аутентичности данных стала краеугольным камнем кибербезопасности. Основой современных криптографических методов служит математика, без которой невозможны ни шифрование, ни расшифровка.

Наиболее часто используемыми областями математики в криптографии являются:

– Теория чисел: лежит в основе алгоритма RSA, основанного на сложности факторизации больших чисел [1].
– Абстрактная алгебра: используется в построении криптосистем на эллиптических кривых [2].
– Комбинаторика и теория вероятностей: применяются при анализе криптостойкости и вероятностных атак [3].
– Эти дисциплины формируют фундамент большинства асимметричных и симметричных криптосистем.

Эллиптические кривые (ECC) позволяют добиться высокой степени безопасности при меньшей длине ключей по сравнению с RSA. Они опираются на сложность задачи дискретного логарифмирования на эллиптических кривых [2].

Также развивается направление криптографии на решётках, обладающей устойчивостью к атакам квантовых компьютеров [4].

Появление квантовых алгоритмов (Шора, Гровера) угрожает традиционным криптосистемам [5]. Это породило бурное развитие постквантовой криптографии (PQ-crypto), основанной на математических задачах, неразрешимых с помощью известных квантовых алгоритмов.

Математика является неотъемлемой частью современной криптографии, определяя её возможности и ограничения. В условиях растущей квантовой угрозы необходима разработка новых криптографических схем на устойчивых математических основах.

Симметричная криптография использует один ключ как для шифрования, так и для расшифрования. Основные алгоритмы, такие как AES (Advanced Encryption Standard), построены на линейной и нелинейной алгебре, теории полей и булевой логике [3]. Несмотря на высокую скорость, основная проблема — безопасная передача ключей.

Асимметричная криптография, напротив, использует пару ключей: открытый и закрытый. Она опирается на трудные математические задачи, такие как факторизация (RSA), дискретный логарифм (DSA) и операции над эллиптическими кривыми (ECC) [1][2]. Эти системы обеспечивают безопасный обмен данными и цифровую подпись.

Современные протоколы, такие как TLS, SSH и PGP, опираются на комбинацию симметричной и асимметричной криптографии. Их безопасность напрямую зависит от математической прочности используемых алгоритмов.

Кроме того, развиваются технологии гомоморфного шифрования, позволяющие производить вычисления над зашифрованными данными без их расшифровки. Эта область активно использует теорию колец, поля Галуа и матрицы над конечными полями.

Также применяется Zero-KnowledgeProofs — доказательства с нулевым разглашением, построенные на комбинаторике и теории графов. Эти методы позволяют доказать знание секрета, не раскрывая сам секрет, и применяются в криптовалютах (например, в Zcash) [6].

Блокчейн-технологии активно используют криптографические методы для обеспечения неизменности и достоверности транзакций. Важную роль играют:

- хеш-функции (SHA-256, Keccak),
- цифровые подписи (ECDSA, EdDSA),
- консенсусные протоколы, основанные на криптографических рандомизациях и вероятностях.

Применение математики здесь ключевое: от построения криптографических хешей до теоретических моделей устойчивости децентрализованных сетей.

Среди актуальных вызовов:

- Создание устойчивых к квантовым атакам криптосистем.
- Повышение эффективности и скорости шифрования без потери безопасности.
- Разработка новых протоколов приватности и аутентификации.

В перспективе исследователи сосредоточатся на математическом моделировании криптостойкости, автоматизированном доказательстве безопасности и формализации новых криптографических задач, не решаемых с помощью квантовых алгоритмов.

Криптография представляет собой уникальное пересечение теоретической математики и практических задач кибербезопасности. Именно математика даёт возможность строить алгоритмы, на которые можно положиться в цифровом обществе. Развитие квантовых вычислений ставит перед человечеством новые задачи, решение которых возможно только на базе глубокого понимания математических принципов. Таким образом, инвестиции в математические исследования в области криптографии — это инвестиции в устойчивое цифровое будущее.

Одним из наиболее эффективных и популярных современных методов асимметричной криптографии является алгоритм на эллиптических кривых. Его математическая основа строится на алгебраических свойствах точек на кривой, описываемой уравнением вида:

$$y^2 = x^3 + ax + b,$$

где коэффициенты и принадлежат конечному полю. Операции сложения и умножения точек на кривой создают абелеву группу, на которой и строится криптосистема.

Преимущество ECC заключается в том, что при одинаковом уровне безопасности длина ключа в два раза меньше, чем у RSA. Например, 256-битный ключ ECC по уровню стойкости эквивалентен 3072-битному ключу RSA [2].

ECC активно используется в мобильных приложениях, банковских системах, протоколах TLS, а также в криптовалютах, например, Bitcoin и Ethereum.

Гомоморфное шифрование позволяет производить вычисления над зашифрованными данными, получая результат в зашифрованном виде, который может быть расшифрован без доступа к исходным данным.

Пример:Пусть пользователь зашифровал два числа и . Сервер, не имея ключа, производит вычисление, получая, который можно расшифровать локально.

Математически такие схемы строятся на кольцах, решётках, модулярных функциях и теории идеалов в кольцах многочленов. Гомоморфные методы особенно актуальны в контексте облачных вычислений и медицины, где требуется высокая степень конфиденциальности [4].

В условиях развития квантовых компьютеров традиционные криптографические схемы (RSA, DSA, ECC) становятся уязвимыми. Постквантовая криптография использует математические задачи, стойкие к квантовым алгоритмам:

- Криптография на решётках (основана на сложности задачи нахождения короткого вектора);
- Многочлены и коды (кодовая криптография — McEliece);
- Криптография на изоморфизмах графов и суперсингулярных кривых (например, алгоритм SIKE).

Эти схемы уже стандартизируются институтом NIST (National Institute of Standards and Technology), и на 2025 год ведётся активное внедрение новых алгоритмов, таких как Kyber и Dilithium [6].

Современная криптография базируется на глубокой математике, включая теорию групп, решёток, конечных полей и вероятностный анализ.

Надёжность криптосистем определяется не только вычислительной сложностью, но и стойкостью к новым типам атак, включая квантовые.

Будущее криптографии связано с усилением сотрудничества между математиками, программистами и специалистами по безопасности.

Таким образом, развитие криптографии невозможно без развития прикладной и теоретической математики. В ближайшие десятилетия именно математические новации определят уровень цифровой безопасности человечества.

Математика продолжает оставаться не только языком науки, но и инструментом цифрового щита в XXI веке. Без её теоретических основ невозможно ни создание новых стандартов безопасности, ни защита критически важной инфраструктуры. В эпоху искусственного интеллекта и квантовой угрозы значение математических методов в криптографии только возрастёт.

Литература

1. Ривест Р., Шамир А., Адлеман Л. "Метод цифровой подписи и алгоритм RSA". Communications of the ACM, 1978.
2. Koblitz N. "Elliptic curve cryptosystems". Mathematics of Computation, 1987.
3. Stinson D.R. "Cryptography: Theory and Practice". CRC Press, 2006.

4. Peikert C. "A Decade of Lattice Cryptography". Foundations and Trends in Theoretical Computer Science, 2016.
5. Shor P.W. "Algorithms for quantum computation: discrete logarithms and factoring". IEEE Symposium on Foundations of Computer Science, 1994.
6. Bernstein D.J., Buchmann J., Dahmen E. (eds). Post-Quantum Cryptography. Springer, 2009.
7. Goldreich O. Foundations of Cryptography: Basic Tools. Cambridge University Press, 2001.