Автор: Амангельдыева Г.Т., Карьягдыев М.Д.
19.06.2025 00:16 -

# 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.

...

полный текст во вложении