УДК 003.26

# ИССЛЕДОВАНИЕ ПРИМЕНЕНИЯ МАТЕМАТИЧЕСКИХ АЛГОРИТМОВ В КРИПТОГРАФИИ

**© 2025 О. А. Евстафиади[1], С. В. Амиров[2], Е. В. Скарга[3], А. В. Шейко[4], В. В. Лапин[5]**

*[1] учитель математики, гимназия 25, г. Ставрополь*
*[2] студент Московского финансово-юридического университета, Москва*
*[3] учащийся МБОУ СОШ 20, г. Ставрополь*
*e-mail: yelizaveta.skarga@inbox.ru*
*[4] учащийся МБОУ СОШ 3, г. Пятигорск*
*[5] учащийся, гимназия 25, г. Ставрополь*
*e-mail: sheykoartem13@gmail.com*

В статье рассматривается роль математического и алгоритмического обеспечения для систем управления и обработки информации. Анализируются существующие проблемы систем обработки информации, что является важным компонентом разработки современных технологий. На основании анализа делается вывод, что математические методы и алгоритмы играют ключевую роль в управлении информацией, обработке данных и разработке новых технологий. Алгоритмическое обеспечение, в свою очередь, отвечает за разработку эффективных алгоритмов для обработки данных, решения задач управления информацией, оптимизации процессов и других задач. Описываются характерные особенности математического и алгоритмического обеспечения. Значительное внимание уделяется математическим моделям систем управления и обработки информации. Рассматриваются типы алгоритмического обеспечения. Отмечается, что исследования в области математического и алгоритмического обеспечения для систем управления и обработки информации позволяют создавать эффективные и надёжные технологии, улучшать производительность и качество работы систем, а также разрабатывать новые инновационные решения.

**Ключевые слова**: шифрование, дешифрование, симметричное шифрование, асимметричное шифрование, ключ, криптостойкость, алгоритм, хэш-функция, цифровая подпись, генерация ключей, модульная арифметика, дискретный логарифм, эллиптические кривые, псевдослучайные числа, криптоанализ, блочный шифр, поточный шифр, секретный ключ, открытый ключ, группы, кольца, поля.

# RESEARCH ON THE APPLICATION OF MATHEMATICAL ALGORITHMS IN CRYPTOGRAPHY

**© 2025 O. A. Evstafiadi[1], S. V. Amirov[2], E. V. Skarga[3], A. V. Sheiko[4], V. V. Lapin[5]**

*[1] mathematics teacher, gymnasium 25, Stavropol*
*[2] student, Moscow University of Finance and Law, MFUA, Moscow*
*[3] student, MBOU secondary school 20, Stavropol*
*e-mail: yelizaveta.skarga@inbox.ru*
*[4] student, MBOU secondary school 31, Pyatigorsk*
*e-mail: sheykoartem13@gmail.com*
*[5] student, gymnasium 25, Stavropol*

The article considers the role of mathematical and algorithmic support for control and information processing systems. The existing problems of information processing systems are analyzed, which is an important component in the development of modern technologies. Based on the analysis, it is concluded that mathematical methods and algorithms play a key role in information management, data processing and the development of new technologies. And algorithmic support, in turn, is responsible for the development of effective algorithms for data processing, solving information management problems, optimizing processes and other tasks. The characteristic features of mathematical and algorithmic support are described. Considerable attention is paid to mathematical models of control and information processing systems. The types of algorithmic support are considered. In conclusion, it is noted that research in the field of mathematical and algorithmic support for control and information processing systems allows creating effective and reliable technologies, improving the productivity and quality of systems, and developing new innovative solutions.

**Keywords:** Encryption, decryption, symmetric encryption, asymmetric encryption, key, cryptographic strength, algorithm, hash function, digital signature, key generation, modular arithmetic, discrete logarithm, elliptic curves, pseudorandom numbers, cryptanalysis, block cipher, stream cipher, secret key, public key, groups, rings, fields.

В условиях стремительного развития информационных технологий и увеличения объемов данных, которые обрабатываются и передаются, защита информации становится одной из главных задач современного общества. Киберугрозы, такие как утечки данных, атаки на системы и несанкционированный доступ, требуют внедрения надежных методов защиты. Математика играет ключевую роль в разработке криптографических алгоритмов, которые обеспечивают безопасность информации [1].

Математические методы позволяют создавать сложные системы шифрования, которые защищают данные от несанкционированного доступа и обеспечивают их целостность. Использование теории чисел, линейной алгебры и других математических дисциплин в криптографии позволяет разрабатывать алгоритмы, способные эффективно обрабатывать и защищать информацию [Там же].

Рассмотрим математические методы, используемые в криптографии.

Теория чисел, также известная как высшая арифметика, является разделом математики, который изначально сосредоточен на изучении свойств целых чисел, такие как алгебраические и трансцендентные, а также различные функции, которые имеют связь с арифметикой целых чисел и их обобщениями [2–4].

Простые числа – это числа, которые делятся на 1 и на само себя. Используются в шифровании, потому что трудно разложить на множители, но легко найти и перемножить.

Остатки и модули используются для замены символов, создавая сам шифр. Типичным значениями модулей, используемыми в криптографии, являются 2, 10 и 26. Какой бы модуль мы ни взяли, встречающиеся числа заменяются на остатки от деления этих чисел. Если в остатке получается отрицательное число, то к нему прибавляют значение модуля, чтобы остаток стал неотрицательным. Например, если используется модуль 26, то единственно возможные числа лежат в диапазоне от 0 до 25. Так, если прибавить 17 к 19, то результат равен 10, поскольку 17 + 19 = 36, а 36 при делении на 26 дает остаток 10.

Дискретная математика занимается изучением объектов, которые можно пересчитать, такие как целые числа, графы и множества.

Дискретный логарифм – это важная концепция в криптографии, которая используется в различных протоколах, включая алгоритм Диффи–Хеллмана. Суть задачи заключается в нахождении значения x в уравнении g^x mod p = y, где g и p известны, а y – результат операции шифровании.

Графы и комбинаторика – это системы применяются для разработки сложных алгоритмов и оптимизации шифров, включая следующие:

– стратегии инвестирования;
– логистику и транспортные операции;
– распределение ресурсов;
– маршрутизацию в телекоммуникационных сетях;
– планирование производственных процессов.

Алгебра обеспечивает математическую основу для разработки и анализа криптографических алгоритмов. Алгебраические структуры, такие как группы, кольца и поля, используются в шифровании и дешифровании данных, а также в генерации ключей. Например, алгоритмы RSA и Diffie-Hellman основаны на алгебраических операциях и свойствах чисел [5].

Рассмотрим основные понятия и определения алгебры, используемые в криптографии [6–8].

– Группы и полугруппы – основные математические структуры, используемые в криптографии для операций шифрования и дешифрования. Группы обладают свойством замкнутости, ассоциативности, наличием нейтрального элемента и обратимостью каждого элемента. А в программировании группоид – это множество с заданной на нём бинарной операцией, а полугруппа – алгебраическая система с заданной на ней ассоциативной бинарной операцией.

– Кольца и поля – используются для операций шифрования и дешифрования с использованием алгебраических операций.

1. $a + (b + c) = (a + b) + c$ – ассоциативность
2. $a + b = b + a$ – коммутативность
3. $a + 0 = a$ – нейтральный элемент
4. $a + a = 0$ – симметричный элемент
5. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ - ассоциативность
6. $a \cdot 1 = 1 \cdot a = a$ – нейтральный элемент
7. $a \cdot (b + c) = a \cdot b + a \cdot c$ – левый закон дистрибутивности

– Линейная алгебра – применяется в криптографии для работы с линейными преобразованиями к системам уравнений.

– Криптографические функции, такие как хэш-функции и функции шифрования, основаны на алгебре и используются для обеспечения конфиденциальности и целостности данных.

Теория вероятностей и математическая статистика – важный инструмент, который помогает создавать случайные числа для симуляции в криптографии, улучшать алгоритмы и структуры данных, это раздел математики, который изучает случайные процессы и ищет в них закономерности. Теория вероятностей является основой криптографических протоколов с нулевым раскрытием информации [9].

Вероятность некоторого события – это величина $p(0 \leq p \leq 1)$, которая показывает частоту появления этого события в ряде однотипных испытаний:

– если событие невозможно, то его вероятность: $p = 0$;
– если событие достоверно, то его вероятность: $p = 1$;
– если событие может наступить или не наступить с одинаковой вероятностью, то его вероятность: $p = 0{,}5$.

Американский ученый Клод Шеннон был одним из основоположников теории и криптографии. Им была выведена в 1948 г. формула для вычисления количества информации равновероятных событий

$$I = -\sum_{i=1}^{N} p_i * log_2 p_i$$

где n – число символов, из которых может быть составлено сообщение (алфавит), H – информационная двоичная энтропия. На практике значения вероятностей pi в формуле заменяют их статистики оценками: p = Ni – относительная частота i-го символа в сообщении, где N – число всех символов в сообщении, Ni – абсолютная частота i-го символа в сообщении, то есть число встречаемости i-го символа в сообщении.

Один из наглядных примеров применения теории вероятностей в разработке можно увидеть на примере корпорации Apple. Разработчики использовали генератор случайных чисел для перемешивания треков, однако после выхода устройства на рынок поступило множество жалоб. Оказалось, что плеер иногда воспроизводил одну и ту же композицию подряд. В результате возникла необходимость внести изменения в алгоритм, добавив проверку на совпадение в плейлисте.

В Python существует свой алгоритм, который помогает решить эту проблему [10]:

```
>>> lst = [int(i) for i in range(1, 13)]
>>> random.shuffle(lst)
>>> print(*lst)
9 6 1 10 12 2 7 5 11 4 8 3
```

На первый взгляд, это не глобальная проблема, но без математики не обойтись. Таким образом, теория вероятностей оказывается необходимой дисциплиной для разработчиков.

Рассмотрим примеры алгоритмов и методов криптографии, основанных на алгебре.

– RSA: алгоритм RSA основан на теории чисел и алгебре модульных вычетов. Он использует операции возведения в степень и вычисление остатка от деления для шифрования и дешифрования.

– Эллиптическая кривая: эллиптическая кривая – это математическая структура, используемая в криптографии для создания систем с открытым ключом. Она основана на алгебре над полями и позволяет выполнить операции шифрования и дешифрования.

– AES: алгоритм AES(Advanced Encryption Standard) – это симметричный алгоритм шифрования, основанный на линейной алгебре. Он использует матричные операции и подстановки для шифрования и дешифрования данных.

– Хэш-функции: Хэш-функция – это математический алгоритм, который преобразует данные в битовый массив неизменяемого размера.

Таким образом, математические алгоритмы являются основополагающим элементом в области криптографии, обеспечивают защиту данных через сложные вычислительные задачи [11]. Современные системы шифрования, цифровые подписи и хэш-функции основываются на таких областях, как теория чисел, дискретная математика и алгебра. С развитием квантовых технологий возникает необходимость в новых математических методах, способных обеспечить безопасность данных в будущем. Таким образом, математика продолжает оставаться фундаментом для создания безопасного цифрового пространства.

### *Библиографический список*

1. *Константинова, С. В.* Информационная безопасность и математика / С. В. Константинова, Е. А. Осипчук, А. А. Честнов // Студент и наука: актуальные

вопросы современных исследований: сборник статей Международной научно-практической конференции в 2 частях. Часть 1. – Пенза: Наука и просвещение, 2023. – С. 11–15.

2. *Мухина, Д. А.* Математические методы в криптографии / Д. А. Мухина // Фундаментальные и прикладные исследования в современном мире. – 2017. – №. 18-1. – С. 97–100.

3. *Мометова, Д. Ф.* Алгебраическая геометрия и ее применение в криптографии / Д. Ф. Мометова //Multidisciplinary Journal of Science and Technology. – 2024. – Т. 4. – №. 7. – С. 75–86

4. *Пихтилькова, О. А.* Алгебраические и теоретико-числовые методы при решении Олимпиадных задач по криптографии / О. А. Пихтилькова, А. Н. Благовисная, Т. А. Горшунова, С. С. Закожурников, Т. А. Морозова, Е. В. Пронина // Перспективные материалы и технологии (ПМТ-2024): сборник докладов Международной научно-технической конференции. – Москва, 2024. – С. 437–440.

5. *Придорогина, А. Е.* Ииспользование методов вычислительной математики в криптографии / А. Е. Придорогина // Международная научно-техническая конференция молодых ученых БГТУ им. В. Г. Шухова, посвященная 170-летию со дня рождения В. Г. Шухова: сборник докладов. Часть 20. Фундаментальные и прикладные исследования в области естественнонаучных и технических дисциплин. – Белгород, 2023. – С. 285–290.

6. *Грошева, Е. К.* Блокчейновая революция / Е. К. Грошева, П. И. Невмержицкий // Бизнес-образование в экономике знаний. – 2018. – №. 1 (9). – С. 17–23.

7. *Ширшова, П. А.* Интеграция математики и информатики при изучении элементов криптографии в классах с углубленным изучением математики: выпускная квалификационная работа (магистерская диссертация) студентки 2 курса очной формы обучения по направлению подготовки 44.04.01 Педагогическое образование, магистерская программа «Современное математическое образование» / П. А. Ширшова; научный руководитель Д. В. Шармин; Тюменский государственный университет, Институт математики и компьютерных наук. – Тюмень, 2021. – 1 файл (842 Кб). – Текст: электронный.

8. *Шиповац, Р.* Компьютеры и технологии защиты информации / Р. Шиповац, Р. Тепавац, В. Шиповац // Актуальные проблемы экономики, социологии и права. – 2015. – №. 3. – С. 73–76.

9. *Баев, И. В.* Генерация случайных чисел / И. В. Баев // Международная научно-техническая конференция молодых ученых БГТУ им. В. Г. Шухова, посвященная 170-летию со дня рождения: сборник докладов. Часть 13. – Белгород, 2023. – С. 55–58.

10. *Шарибченко, Е. И.* Анализ математического и алгоритмического обеспечения для систем управления и обработки информации / Е. И. Шарибченко, Р. В. Мальчева //Информатика и кибернетика. – 2024. – №. 2 (36). – С. 66–75.

11. *Димов, Е. Д.* Формирование базовых знаний по информационной безопасности интернет-сайтов и порталов при подготовке специалистов по информатике / Е. Д. Димов // Вестник Московского городского педагогического университета. Серия: Информатика и информатизация образования. – 2006. – №. 7. – С. 57–63.