# УДК 51

#  ***Талгаткызы Каракат студент***

***«Кокшетауского университета имени Ш. Уалиханова»***

***Кафедра математики, физики и информатики***

 ***Казахстан, г. Кокшетау***

***e-mail: talkara000@gmail.com***

**МАТЕМАТИКА В КРИПТОГРАФИИ**

***Аннотация:*** *В статье рассматривается роль математики как основного инструмента в современной криптографии. Приводится обзор математических методов, используемых в криптографических алгоритмах, включая теорию чисел, дискретную математику и алгебру. Анализируются их применение в системах шифрования, цифровых подписях и криптографических протоколах. Представлены результаты и обсуждение важности математических моделей для обеспечения надежности и безопасности криптографических решений.*

**Ключевые слова:** *Простые числа, дискретная математика, теория чисел, криптография, алгебра.*

***Talgatqyzy Qaraqat student***

***«Kokshetau State University named after Shokan Ualikhanov»***

***Faculty of Mathematics, Physics and Computer Science,***

 ***Кazakhstan,Kokshetau***

 ***e-mail: talkara000@gmail.com***

 **PRIME NUMBERS AND THEIR ROLE IN MATHEMATICS**

***Abstract:*** *The article examines the role of mathematics as the main tool in modern cryptography. An overview of mathematical methods used in cryptographic algorithms, including number theory, discrete mathematics and algebra, is provided. Their application in encryption systems, digital signatures and cryptographic protocols is analyzed. The results and discussion of the importance of mathematical models for ensuring the reliability and security of cryptographic solutions are presented.*

**Key words:** *Prime numbers, discrete mathematics, number theory, cryptography, algebra .*

**Введение**

**Криптография** — это наука о способах и методах шифрования информации. Она защищает передаваемые сообщения и использует алгоритмы, которые позволяют быстро обнаруживать и устранять любые уязвимости.[[1]](https://www.wikipedia.org/)

**Основной метод криптографии — шифрование.** Оно превращает информацию в код, поддающийся расшифровке только с помощью подходящего ключа. В ситуации, когда код знает только отправитель и получатель информации, передаваемые данные остаются для остальных непереводимым набором символов.

**Криптография используется в разных сферах жизни человека, например:**

* Финансовые операции. Все транзакции кодируются банками с помощью криптографических методов защиты информации.
* Сохранность личных данных. Сайты, которые собирают личную информацию пользователей (имя, пол, возраст, контакты), используют шифрование данных.
* Конфиденциальность общения. Большинство популярных мессенджеров шифрует переписки пользователей, чтобы их могли прочитать только участники диалога.
* Безопасность обмена информацией в компьютерных сетях. Криптография помогает обеспечить безопасность обмена информацией в таких областях, как передача интернет-трафика и обеспечение связи для смартфона.

 Криптография является основой защиты данных в современном мире, где информационные технологии пронизывают практически все сферы жизни. Передача конфиденциальной информации, финансовые операции, аутентификация пользователей — все эти процессы зависят от надежных криптографических методов. Математика, как наука о числах и структурах, лежит в основе большинства криптографических решений, обеспечивая их точность и безопасность. В данной статье будут рассмотрены основные математические подходы, лежащие в основе криптографии, их значимость и применение на практике.

**Методы**

 Существует несколько главных математических методов, которые используются в криптографии:

**1. Теория чисел**

Теория чисел изучает свойства чисел и их связи между собой. В криптографии особенно важны:

 • Простые числа: Эти числа делятся только на 1 и на себя (например, 2, 3, 5, 7). Множество шифров строится на том, что найти большие простые числа и перемножить их легко, а вот разложить результат на множители — крайне сложно.

 • Остатки и модули: Используются для создания шифров, где каждое число заменяется на его остаток при делении на другое число.[2]

**2. Дискретная математика**

Дискретная математика изучает объекты, которые можно сосчитать (например, целые числа, графы и множества). Здесь важны:

• Дискретный логарифм: Это сложная задача, на которой основано несколько систем шифрования, включая протокол обмена ключами Диффи-Хеллмана.

• Графы и комбинаторика: Используются для создания сложных алгоритмов и оптимизации шифров.

**3. Алгебра**

• Эллиптические кривые: Эти математические объекты позволяют создавать эффективные и безопасные алгоритмы. При меньшем размере ключей они обеспечивают такую же защиту, как и традиционные методы.

**4. Статистика и теория вероятностей**

 Статистика помогает оценить, насколько устойчив шифр к взлому. Например, вероятность того, что злоумышленнику удастся подобрать ключ, можно рассчитать с помощью математических методов.

**Результаты**

Применение математики позволило создать надежные криптографические системы, которые сегодня используются по всему миру:

1. RSA

Один из самых популярных методов шифрования. Он основан на теории чисел, а именно на задаче разложения большого числа на простые множители. Например, число из 300 цифр практически невозможно разложить вручную, даже используя мощные компьютеры.

2. Эллиптические кривые

Системы на основе эллиптических кривых более эффективны. Например, 256-битный ключ на эллиптических кривых обеспечивает такую же защиту, как и 3072-битный ключ в RSA.[3]

3. Хэш-функции

Используются для создания уникального “отпечатка” данных. Например, алгоритм SHA-256 применяется в блокчейне и других системах, где важна целостность информации.

 4. Асимметричное шифрование (с открытым ключом):

 Этот метод использует пару ключей: открытый (публичный) и закрытый (приватный). Открытый ключ используется для шифрования, закрытый — для расшифровки. Открытый ключ можно свободно распространять, безопасность обеспечивается секретностью закрытого ключа. Этот метод медленнее симметричного, но решает проблему безопасной передачи ключа.

 В eGov: асимметричное шифрование, скорее всего, используется для аутентификации пользователя и проверки целостности электронного ключа. Открытый ключ может быть встроен в ключ, а закрытый хранится в защищенной области системы.

 В WhatsApp: используется для обмена симметричными ключами. Алгоритм Диффи-Хеллмана (часто в сочетании с ECC) позволяет участникам чата безопасно согласовывать общий секретный ключ, используя только открытые ключи, без риска перехвата ключа третьей стороной. Этот общий ключ затем используется для симметричного шифрования сообщений.

**Обсуждение**

Математика в криптографии не просто инструмент — это ее основа. Именно математические задачи с высокой сложностью делают современные шифры безопасными. Однако развитие технологий создает новые вызовы:

1. Проблема квантовых компьютеров

Квантовые компьютеры могут решать некоторые математические задачи намного быстрее классических. Например, алгоритм Шора способен разложить число на простые множители за короткое время, что угрожает алгоритмам RSA.

2. Постквантовая криптография

Для защиты от квантовых атак ученые разрабатывают новые криптографические алгоритмы, которые используют более сложные математические модели, такие как решетки и многочлены.[4]

Таким образом, математика должна развиваться вместе с технологиями, чтобы обеспечивать безопасность данных в будущем.

**Выводы**

Математика играет ключевую роль в криптографии, обеспечивая защиту информации с помощью сложных вычислительных задач. На таких разделах, как теория чисел, дискретная математика и алгебра, строятся современные системы шифрования, цифровые подписи и хэш-функции.

 Развитие квантовых технологий требует поиска новых математических подходов, которые смогут гарантировать защиту данных в будущем. Таким образом, математика остается основой для безопасного цифрового мира.

 Литература

1. Википедия: свободная энциклопедия [Электронный ресурс]. – URL: https://www.wikipedia.org/ .

2. Лей Д. Ч. Теория чисел для начинающих. – М.: Наука, 1991. – 384 с.

3. Коблиц Н. Криптография на эллиптических кривых. – М.: Мир, 1994. – 206 с.

4. Шнайер Б. Прикладная криптография: протоколы, алгоритмы и исходный код на языке Си. / Пер. с англ. – 2-е изд. – М.: Издательский дом «Вильямс», 2004. – 816 с.