УДК 004.056.55

# АЛГОРИТМЫ ШИФРОВАНИЯ И ДЕШИФРОВАНИЯ С ПОМОЩЬЮ МЕТОДОВ ДИСКРЕТНОЙ МАТЕМАТИКИ

*Новиков В.А. студент гр.253504, Жак М.В. студент гр.253504,*

*Вашкевич Е.Г. студент гр.253504*

*Белорусский государственный университет информатики и радиоэлектроники*

*г. Минск, Республика Беларусь*

*Егорова Н. Г. – канд. физ.-мат. наук*

**Аннотация.** Статья представляет обзор основных методов шифрования и дешифрования, используемых в современных криптографических системах, которые базируются на дискретной математике. В статье рассмотрены основные принципы симметричного и асимметричного шифрования, такие как AES, DES, RSA и ECC, их преимущества и недостатки, а также методы атак на эти алгоритмы. В заключении, статья подчеркивает важность дискретной математики для современной криптографии и показывает, какие методы шифрования и дешифрования лучше использовать для защиты данных в различных сценариях использования.

**Ключевые слова.** алгоритмы шифрования, дешифрования, дискретная математика, симметричное шифрование, асимметричное шифрование, AES, DES, RSA, ECC, безопасность данных.

## Введение.

Шифрование и дешифрование информации - это одна из важнейших задач в области информационной безопасности. В условиях все большей цифровизации и передачи информации в сети Интернет, обеспечение защиты конфиденциальности и целостности данных становится все более актуальным и необходимым. Криптография, наука о методах обеспечения конфиденциальности данных, использует множество различных алгоритмов и протоколов для защиты информации. В данной статье будет рассмотрена тема алгоритмов шифрования и дешифрования с помощью методов дискретной математики. Мы рассмотрим основные принципы работы симметричных и асимметричных алгоритмов шифрования используемые для обеспечения безопасности данных в интернете. Мы также рассмотрим роль дискретной математики в разработке криптографических алгоритмов и перспективы ее развития в криптографии.

## Основные понятия криптографии и дискретной математики.

Шифрование - это процесс преобразования информации для защиты ее от несанкционированного доступа, при этом авторизованным пользователям предоставляется доступ к ней. Основная цель шифрования - обеспечение конфиденциальности передаваемой информации. Для каждого алгоритма шифрования необходимо использовать ключ, который определяет выбор конкретного преобразования из множества возможных.

Дешифрование - это процесс преобразования зашифрованной информации обратно в исходное сообщение с использованием специального ключа, который позволяет расшифровать данные. Он является обратной операцией шифрования и используется для восстановления конфиденциальной информации, защищенной при помощи шифрования.[1]

Дискретные функции могут быть использованы в криптографии для шифрования и дешифрования информации, например, при использовании алгоритма RSA. Этот алгоритм использует дискретные математические функции, включая функцию Эйлера и простые числа, для шифрования и расшифровки сообщений.

Кроме того, дискретные алгоритмы, такие как алгоритм Диффи-Хеллмана, используются для обмена ключами и обеспечения безопасной связи в интернете. Этот алгоритм основан на дискретных математических функциях и предназначен для обмена секретной информацией между двумя пользователями, не раскрывая ее третьим сторонам.

Таким образом, дискретные функции и алгоритмы имеют важное значение для криптографии и шифрования, так как позволяют создавать защищенные каналы связи и обеспечивать конфиденциальность передаваемой информации.

**Симметричное шифрование.**

Симметричное шифрование - это метод криптографического шифрования, который использует один и тот же ключ для шифрования и дешифрования информации. Таким образом, только тот, у кого есть ключ, может расшифровать зашифрованную информацию. Симметричное шифрование является быстрым и эффективным способом защиты информации, однако ключ должен быть передан по защищенному каналу связи для обеспечения безопасности. Распространенные алгоритмы: AES, DES.

DES (Data Encryption Standard) - это алгоритм шифрования, который был разработан в 1970-х годах. Он использует 56-битный ключ для шифрования данных и был одним из первых стандартных алгоритмов шифрования. В настоящее время DES считается устаревшим и небезопасным, так как существуют методы взлома, которые могут расшифровать данные, зашифрованные DES.

Процесс шифрования в DES включает в себя следующие шаги:

- Начальная перестановка (Initial Permutation, IP): входные данные (64 бита) переставляются в определенном порядке.
- Раунды шифрования (Encryption Rounds): в DES выполняется 16 раундов шифрования, каждый из которых состоит из следующих шагов:
- Замена (Substitution): 48-битный блок данных, полученный из входных данных с помощью функции расширения, подвергается замене на другой 48-битный блок с помощью S-блоков. S-блоки являются таблицами замен, которые определяют, каким блокам входных данных должны соответствовать блоки выходных данных.
- Перестановка (Permutation): после замены блок данных переставляется в определенном порядке.
- Ключевая операция (Key Mixing): блок данных объединяется с ключом раунда (48 бит), который был предварительно сгенерирован из основного ключа DES (56 бит). Это достигается путем сжатия ключа с помощью таблицы перестановок и циклического сдвига битов.
- Финальная перестановка (Final Permutation, FP): после выполнения 16 раундов шифрования, выходные данные подвергаются финальной перестановке, обратной начальной перестановке.

Процесс дешифрования в DES выполняется обратным порядком, то есть финальная перестановка выполняется первой, а начальная перестановка - последней. Алгоритм представлен на рисунке 1.


Рисунок 1 – Алгоритм DES.

AES (Advanced Encryption Standard) - это симметричный алгоритм шифрования, который был разработан в 1998 году и признан государственным стандартом США в 2001 году. AES использует 128-, 192- или 256-битные ключи и является одним из наиболее надежных алгоритмов шифрования, который широко используется в настоящее время. AES считается безопасным и надежным алгоритмом шифрования, так как его ключи очень длинные, что затрудняет процесс взлома.

Алгоритм шифрования AES включает в себя следующие шаги:

- Начальная перестановка (AddRoundKey): входные данные (128 бит) объединяются с ключом шифрования (128 бит) с помощью операции XOR.
- Раунды шифрования (Rounds): в AES выполняется 10 раундов шифрования (в зависимости от длины ключа могут использоваться и другие варианты числа раундов), каждый из которых состоит из следующих шагов:
- Замена байтов (SubBytes): каждый байт входных данных заменяется на соответствующий байт из заранее определенной таблицы замен (S-блок), представлено на рисунке 2.
- Сдвиг строк (ShiftRows): строки входных данных циклически сдвигаются влево, представлено на рисунке 3.
- Смешивание столбцов (MixColumns): столбцы входных данных перемешиваются с помощью линейных преобразований, представлено на рисунке 4.
- Добавление ключа (AddRoundKey): блок данных объединяется с ключом раунда (128 бит), который был предварительно сгенерирован из основного ключа AES (128, 192 или 256 бит). Это достигается путем сжатия ключа и циклического сдвига битов. Представлено на рисунке 5.
- Финальный раунд (Final Round): после выполнения 10 раундов шифрования, выполняется финальный раунд, который состоит из следующих шагов:
- Замена байтов (SubBytes).

- Сдвиг строк (ShiftRows).
- Добавление ключа (AddRoundKey).

Процесс дешифрования в AES выполняется обратным порядком, то есть каждый шаг в процессе дешифрования является обратным к соответствующему шагу в процессе шифрования.

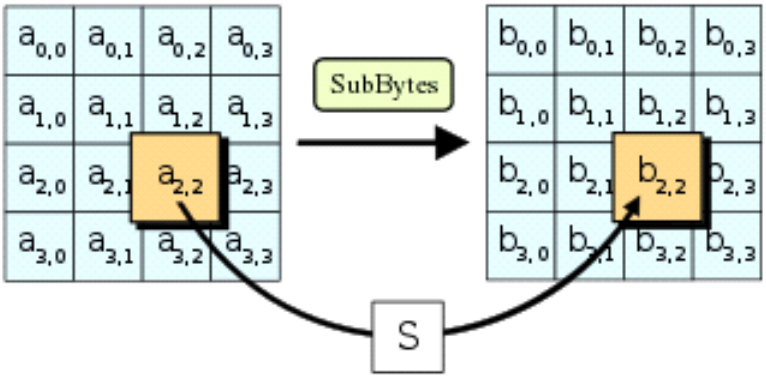


Рисунок 2 – Замена байтов.

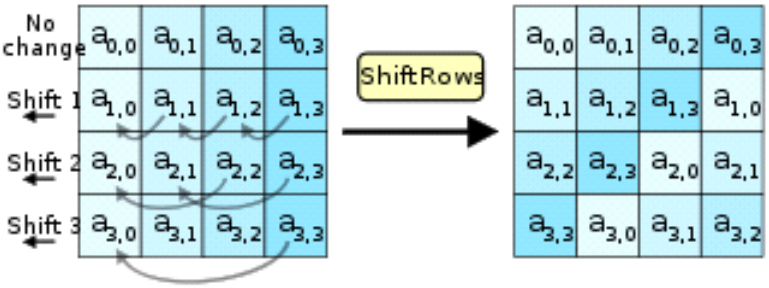


Рисунок 3 – Сдвиг строк.

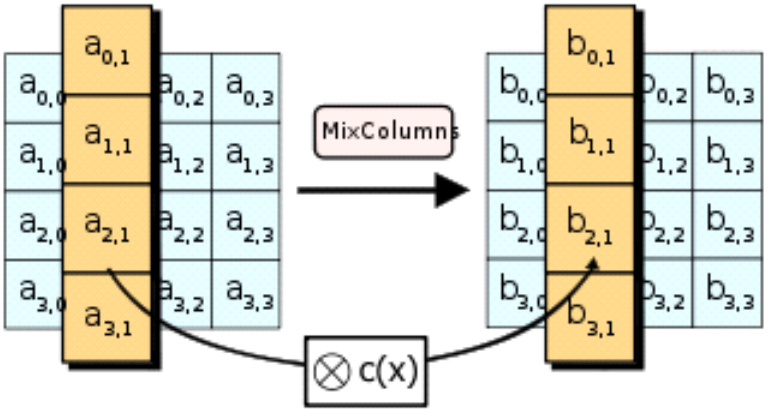


Рисунок 4 – Смешивание столбцов..

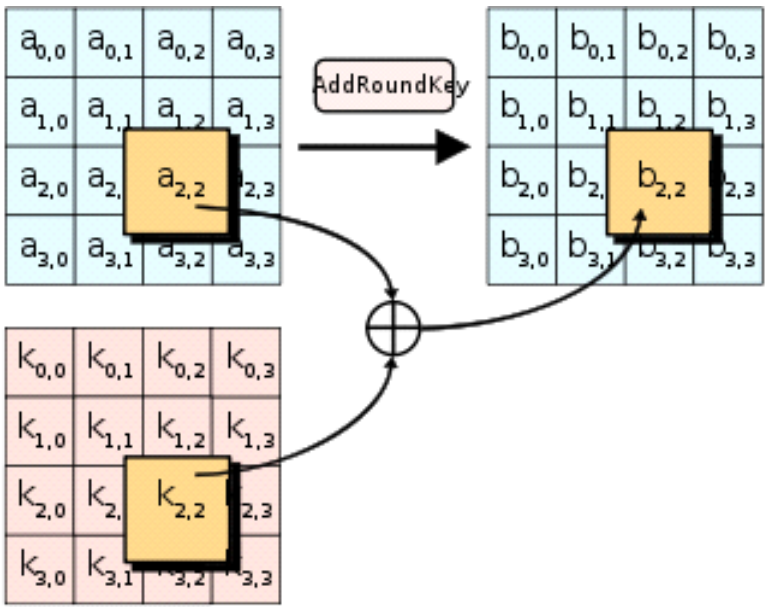


Рисунок 5 – Добавление ключа.

**Асимметричное шифрование.**

RSA (Rivest-Shamir-Adleman) основан на математических свойствах трудности разложения больших чисел на простые множители. Данный алгоритм используется для шифрования данных и для создания цифровых подписей. Он является одним из самых распространенных алгоритмов шифрования в мире, так как обеспечивает надежную защиту передаваемых данных.

Алгоритм RSA можно описать следующим образом:

- Генерация ключей: сначала генерируются два больших простых числа, обозначенные p и q. Затем вычисляется их произведение n = p*q, которое становится модулем для шифрования и расшифровки данных. Также выбирается целое число e, которое должно быть взаимно простым с (p-1)(q-1), и вычисляется число d, которое является мультипликативно обратным к e по модулю (p-1)(q-1). В результате получается пара ключей: публичный ключ (n, e) и приватный ключ (n, d).
- Шифрование: для шифрования сообщения M используется публичный ключ (n, e). Сообщение M сначала преобразуется в целое число m, которое должно быть меньше, чем n. Затем вычисляется шифртекст C, равный m в степени e по модулю n: C = m^e mod n.
- Расшифрование: для расшифровки сообщения C используется приватный ключ (n, d). Шифртекст C возводится в степень d по модулю n: m = C^d mod n. Полученное число m является исходным сообщением M.

ECC (Elliptic Curve Cryptography) использует математические свойства эллиптических кривых для шифрования данных. Этот алгоритм обеспечивает такую же степень защиты, как и RSA, но с использованием коротких ключей, что делает его более эффективным в сравнении с RSA. ECC нашел широкое применение в беспроводных сетях, где требуется надежная защита данных, но ограниченные ресурсы для вычислений и передачи информации. Алгоритм представлен на рисунке 6.

Алгоритм ECC можно описать следующим образом:

- Генерация ключей: сначала выбирается параметры эллиптической кривой, которые используются для генерации ключей. Это включает в себя определение уравнения кривой и коэффициентов, которые определяют ее форму. Затем выбирается точка P на кривой,

которая будет использоваться для генерации ключевой пары. Приватный ключ - это случайное число d, а публичный ключ - это точка Q, равная dP.

- Шифрование: для шифрования сообщения M используется публичный ключ Q. Сообщение M сначала преобразуется в точку Pm на эллиптической кривой. Затем выбирается случайная точка k на кривой и вычисляется шифртекст C, который представляет собой пару точек (kP, Pm + kQ).
- Расшифрование: для расшифровки сообщения C используется приватный ключ d. Сначала вычисляется kP, затем вычитается из второй части шифр текста: Pm = Pm + kQ - d(kP). Полученная точка Pm является исходным сообщением M.[2]

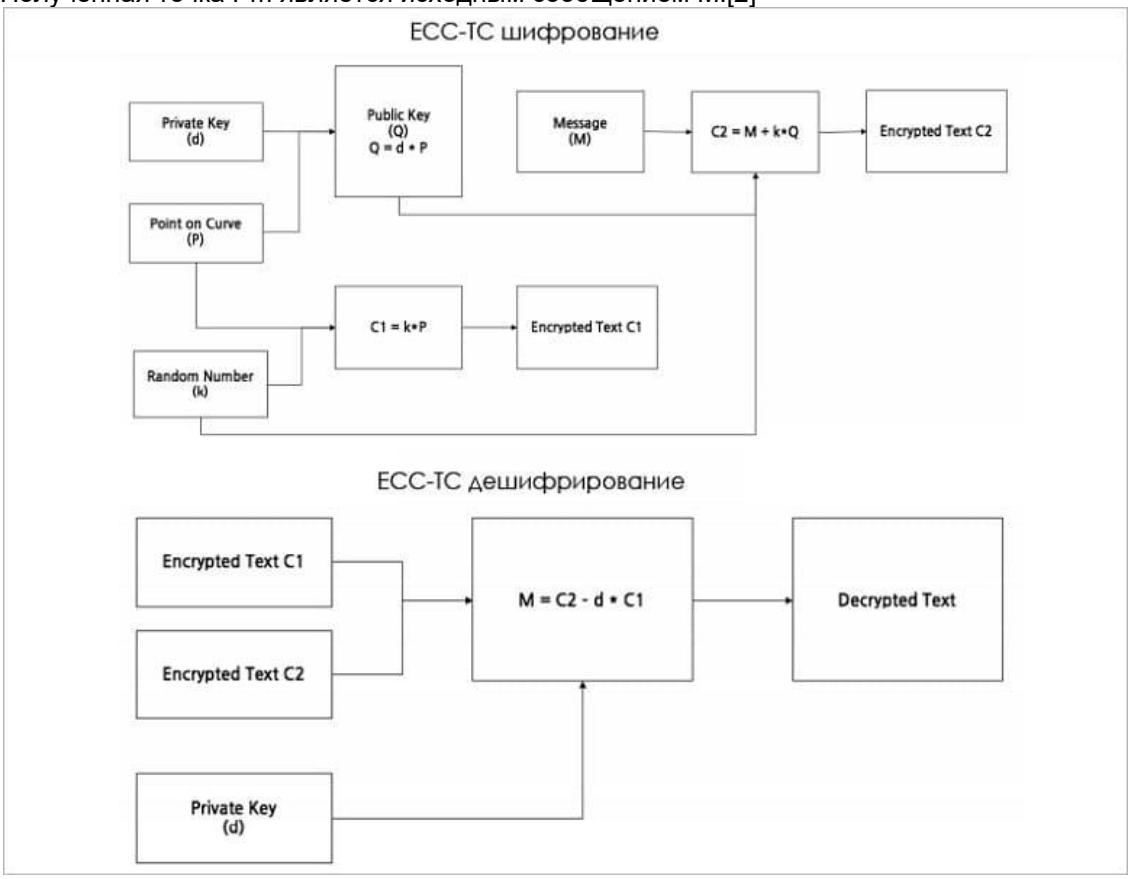


Рисунок 6 – Алгоритм ECC.

**Важность дискретной математики в криптографии.**

Важность дискретной математики в криптографии заключается в том, что многие алгоритмы шифрования и дешифрования основаны на математических концепциях и методах, таких как теория чисел, теория групп, теория поля и комбинаторика. Дискретная математика предоставляет криптографии необходимые инструменты для создания безопасных систем передачи данных и защиты информации. Например, дискретная математика позволяет создавать математические функции, которые могут быть использованы для шифрования данных и генерации криптографических ключей. Кроме того, дискретная математика также обеспечивает методы проверки безопасности криптографических систем и выявления уязвимостей в них. Без использования дискретной математики криптография как наука не могла бы существовать в своей текущей форме.[3]

**Заключение.**

В заключении можно отметить, что использование методов дискретной математики в криптографии играет важную роль в обеспечении безопасности передаваемой информации. Шифрование и дешифрование с помощью алгоритмов, основанных на дискретных функциях, позволяет надежно защитить данные от несанкционированного доступа. Важно также отметить, что

разработка новых алгоритмов шифрования является актуальной задачей с учетом постоянно меняющихся угроз в области кибербезопасности.

***Список использованных источников:***

*1. Шнайер Б.Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си, 2002*

*2. Wenbo Mao, Modern Cryptography: Theory and Practice , 2003.*

*3. Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. Handbook of Applied Cryptography, 1997*

UDC 004.056.55

# ENCRYPTION AND DECRYPTION ALGORITHMS USING METHODS OF DISCRETE MATHEMATICS

*Novikov V.A., student of group 253504, Zhak M.V., student of group 253504, Vashkevich E.G., student of group 253504*

*Belarusian State University of Informatics and Radioelectronics*

*Minsk, Republic of Belarus*

*Egorova N.G. - PhD in Physics and Mathematics*

**Annotation.** The article provides an overview of the main encryption and decryption methods used in modern cryptographic systems that are based on discrete mathematics. The article discusses the basic principles of symmetric and asymmetric encryption, such as AES, DES, RSA, and ECC, their advantages and disadvantages, as well as methods of attacks on these algorithms. In conclusion, the article emphasizes the importance of discrete mathematics for modern cryptography and shows which encryption and decryption methods are best to use to protect data in different usage scenarios.

**Keywords.** encryption algorithms, decryption algorithms, discrete mathematics, symmetric encryption, asymmetric encryption, AES, DES, RSA, ECC, data security.