УДК 004.056.55

97. ШИФРОВАНИЕ И ДЕШИФРОВАНИЕ ИНФОРМАЦИИ НА ОСНОВЕ ДИСКРЕТНОЙ МАТЕМАТИКИ

Соловьева К. А., студентка группы 473903, Бабичева А. А., студентка группы 473903

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Русина Н. В. – ст. преп., каф. ЭИ

Аннотация. В данной статье обсуждается растущая значимость шифрования и дешифрования данных в условиях цифровизации и информационной безопасности. Основное внимание уделяется методам дискретной математики, которые лежат в основе симметричных и асимметричных алгоритмов шифрования. Рассматриваются ключевые алгоритмы, такие как AES, ECC, RSA, и DES, их принципы работы, особенности реализации и критерии, необходимые для обеспечения надежности защиты данных. Отдельно подчеркивается роль дискретной математики в разработке криптографических методов и ее перспективы в будущем. Также проанализированы практические аспекты использования шифрования и требования к современным алгоритмам.

Ключевые слова. Шифрование, дешифрование, симметричное шифрование, асимметричное шифрование, DES, AES, RSA, ECC.

В условиях растущей цифровизации и обмена информацией через Интернет, защита конфиденциальности и целостности данных становится все более важной, поэтому значимость шифрования и дешифрования данных в сфере информационной безопасности возрастает. В данной статье мы разберем алгоритмы шифрования и дешифрования, используя методы дискретной математики. Мы рассмотрим основные принципы работы симметричных и асимметричных алгоритмов, применяемых для обеспечения безопасности данных в сети. Также будет затронута роль дискретной математики в создании криптографических алгоритмов и ее будущие перспективы в этой области.

Криптография – наука о математических методах, разрабатывающая алгоритмы, протоколы и системы, которые гарантируют конфиденциальность и безопасность данных.

Дешифрование - это процесс восстановления зашифрованной информации в исходный, понятный формат, за счет использования специального ключа. Он представляет собой процесс, который позволяет восстановить защищенную информацию, используя методы, противоположные тем, что применялись для ее шифрования.

Шифрование - это процесс преобразования информации в защищённый формат., обеспечивающий ее защиту от несанкционированного доступа, но при этом авторизованные пользователи имеют доступ к ней. Основная задача шифрования заключается в защите конфиденциальности передаваемых данных. Для каждого алгоритма шифрования требуется ключ, который определяет конкретное преобразование из множества доступных вариантов.

Существует два вида алгоритмов шифрования: программное и аппаратное. Производительнее, проще в использовании и дает более высокую защиту аппаратное шифрование данных, но оно обходится дороже. В то время как программное шифрование данных более практично и универсально.

Современные методы шифрования должны соответствовать определённым критериям. Во-первых, стойкость шифра к криптоанализу должна быть такой, чтобы его можно было взломать только с помощью полного перебора ключей. Криптостойкость обеспечивается не секретностью самого

алгоритма, а конфиденциальностью ключа. При этом шифротекст не должен значительно превышать по размеру исходные данные, время, затрачиваемое на шифрование, должно быть минимальным, а стоимость процесса шифрования должна быть сопоставима с ценностью защищаемой информации.

Дополнительно алгоритм шифрования должен соответствовать ряду дополнительных требований. Он должен быть достаточно простым для реализации, чтобы снизить вероятность программных ошибок. Алгоритм должен иметь плоское пространство ключей и принимать любую случайную последовательность бит нужной длины в качестве ключа. Наличие слабых ключей считается нежелательным. Также алгоритм должен легко адаптироваться для различных уровней безопасности и удовлетворять как минимальным, так и максимальным требованиям. Все операции с данными должны проводиться над блоками, кратными байту или 32-битным словам.

Существуют два вида шифрования: симметричное и асимметричное.

Симметричное шифрование - это метод криптографического шифрования, в котором шифрование и дешифрование информации происходит при помощи одного и того же ключа. Из этого можно сделать вывод, что расшифровать зашифрованную информацию может только тот, у кого есть ключ. Симметричное шифрование представляет собой быстрый и эффективный метод защиты данных, но для обеспечения безопасности ключ необходимо передать через защищённый канал связи.

Для шифрования информации сначала используется ключ, затем исходные данные, которые необходимо защитить. При помощи математических вычислений и преобразований ключ объединяется с данными. Например, каждый байт сообщения перемножается с числом из ключа, формируя новое значение. Аналогичным образом обрабатывается весь массив исходных данных, что в результате превращает их в зашифрованную последовательность чисел.

Эту зашифрованную информацию можно безопасно передавать по любым каналам связи. Даже если кто-то перехватит данные, без доступа к ключу расшифровка невозможна. Получатель, обладая ключом, может восстановить первоначальное сообщение, разделяя каждое число из массива на соответствующее значение ключа, и таким образом получает исходные данные для чтения.

Простой пример использования симметричного шифрования:
Предположим, мы с коллегой захотели создать защищённую систему передачи данных. Для этого мы согласовали специальное число, которое станет нашим уникальным ключом. Процесс шифрования будет следующим:

1. Вы придумываете сообщение, которое хотите отправить.
2. В качестве ключа выбирается определённое число, с помощью которого шифруются все символы. Например, если ключ равен 5, то каждая буква в сообщении сдвигается на пять позиций дальше по алфавиту. Таким образом: буква А (1-я позиция) превращается в Д (6-я позиция), К превращается в П и так далее. Если при смещении символы выходят за пределы алфавита, то счёт продолжается с начала алфавита.
3. Вы преобразуете всё сообщение таким образом, шифруя его буква за буквой.
4. Зашифрованный текст передаёте коллеге.
5. Коллега берёт полученный текст, применяет ключ, но с обратным направлением смещения, возвращая буквы на нужное количество позиций назад по алфавиту. В результате он восстанавливает оригинальное сообщение.

Распространенные алгоритмы симметричного шифрования: AES, DES.

Стандарт шифрования DES (Data Encryption Standard) был разработан в 1970-х годах и основан на алгоритме DEA (Data Encryption Algorithm). Идеи алгоритма DEA были предложены компанией IBM в 1960-х годах, опираясь на концепции, изложенные Клодом Шенноном в 1940-х. Первоначально метод шифрования назывался Lucifer, и разработан он был Хорстом Фейштелем. Название DEA было присвоено только в 1976 году.

DEA оперирует с блоками данных размером 64 бита и использует ключ длиной 56 бит. Такая длина ключа соответствует 1017 комбинаций, что обеспечивало до недавнего времени достаточный уровень безопасности. В дальнейшем можно ожидать расширения ключа до 64 бит (например, LOKI) или вообще замены DES другим стандартом.

Входной блок данных, состоящий из 64 бит, преобразуется в выходной блок идентичной длины. Ключ шифрования должен быть известен, как отправляющей так и принимающей сторонам. В алгоритме широко используются перестановки битов текста. В настоящее время DES считается устаревшим и небезопасным, поскольку существуют методы, позволяющие взломать и расшифровать данные, зашифрованные с использованием этого алгоритма.

Процесс шифрования в DES включает в себя следующие шаги: 1. Начальная перестановка (Initial Permutation, IP): входные данные размером 64 бита подвергаются перестановке согласно заданному порядку. 2. Раунды шифрования (Encryption Rounds): алгоритм включает 16 раундов, каждый из которых включает следующие шаги: 2.1 Замена (Substitution): 48-битный блок, полученный из исходных данных с помощью функции расширения, заменяется на другой 48-битный блок с использованием S-блоков, которые представляют собой таблицы замен, определяющие соответствие входных и

выходных данных. 2.2 Перестановка (Permutation): после замены блок данных снова переставляется в установленном порядке. 2.3 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. 2.4 Финальная перестановка (Final Permutation, FP): по завершении 16 раундов шифрования выходные данные проходят финальную перестановку, которая является обратной начальной перестановке.

Процесс дешифрования в DES происходит в обратном порядке: сначала выполняется финальная перестановка, а затем начальная перестановка завершается последней.

Алгоритм представлен на рисунке 1.

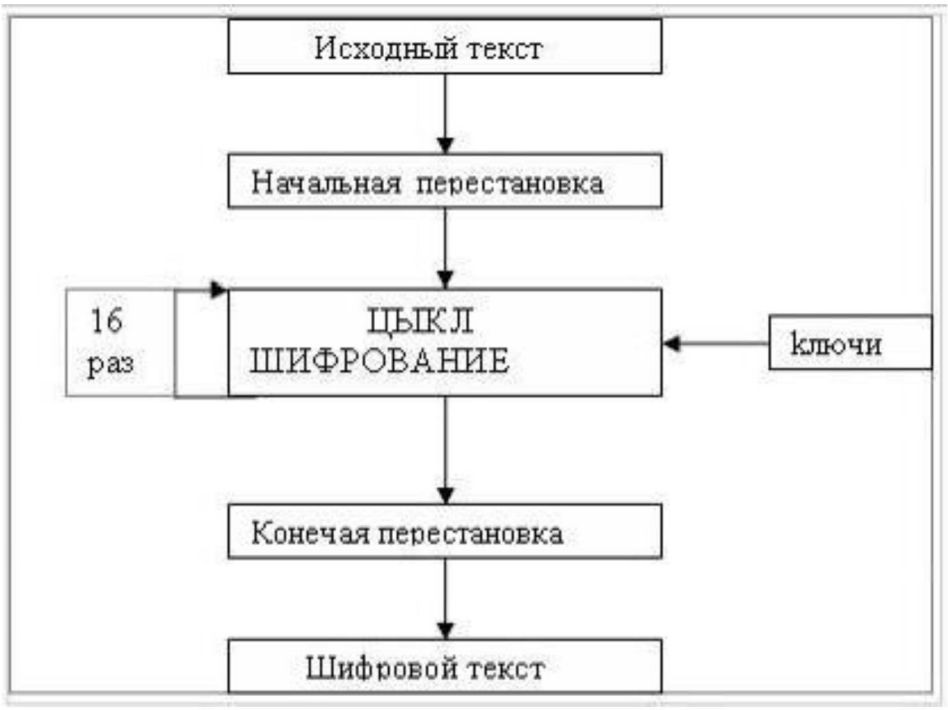

Рисунок 1 – Алгоритм работы симметричного шифрования DES

AES (Advanced Encryption Standard) — это симметричный алгоритм шифрования, который был принят Национальным институтом стандартов и технологий (NIST) в 2001 году в качестве стандарта для защиты конфиденциальности данных.

AES представляет собой блочный шифр, что означает, что в отличие от потоковых шифров, которые обрабатывают данные по одному биту за раз, блочные шифры работают с фиксированными блоками данных. Каждый блок обрабатывается независимо от остальных, что упрощает параллельные вычисления и ускоряет процесс шифрования. Наглядная схема работы алгоритма шифрования AES представлена на рисунке 2.

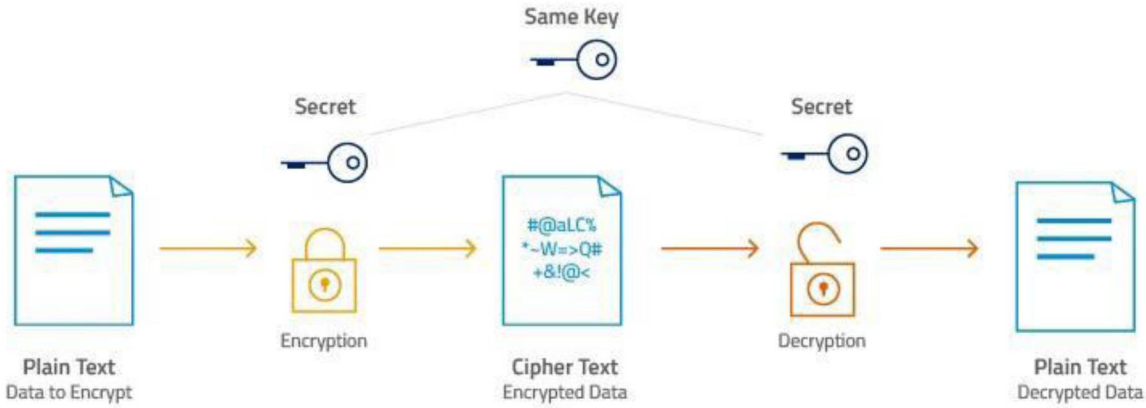

Рисунок 2 – схема работы алгоритма AES

AES применяет несколько раундов шифрования, количество которых зависит от размера ключа: для ключа длиной 128 бит используется 10 раундов, для 192 бит — 12 раундов, а для 256 бит — 14 раундов.

Рассмотрим алгоритм шифрования AES с ключом длиной 128 бит. Сначала входные данные необходимо разбить на блоки по 16 байт. Если общий размер данных не кратен 16 байтам, их следует дополнить до необходимого размера. Каждый блок можно представить в виде матрицы 4x4, называемой state. Далее выполняется процедура расширения ключа, и к каждому блоку state применяются операции 2-4. Алгоритм можно описать следующими шагами (рисунок 3):

1. Процедура расширения ключа (KeyExpansion).
2. Начальный раунд, в котором state складывается с основным ключом.
3. Проведение девяти раундов шифрования, каждый из которых включает ряд преобразований: замена байтов (SubBytes): каждый байт исходных данных заменяется на соответствующий байт из заранее подготовленной таблицы замен (S-блок), сдвиг строк (ShiftRows): строки данных подвергаются циклическому сдвигу влево, смешивание столбцов (MixColumns): столбцы данных перемешиваются с использованием линейных преобразований, добавление ключа (AddRoundKey): блок данных комбинируется с раундовым ключом (128 бит), который был сгенерирован из основного ключа AES (длиной 128, 192 или 256 бит) через процесс сжатия и циклического сдвига битов..
4. Завершающий раунд, состоящий из преобразований: SubBytes, ShiftRows и AddRoundKey.

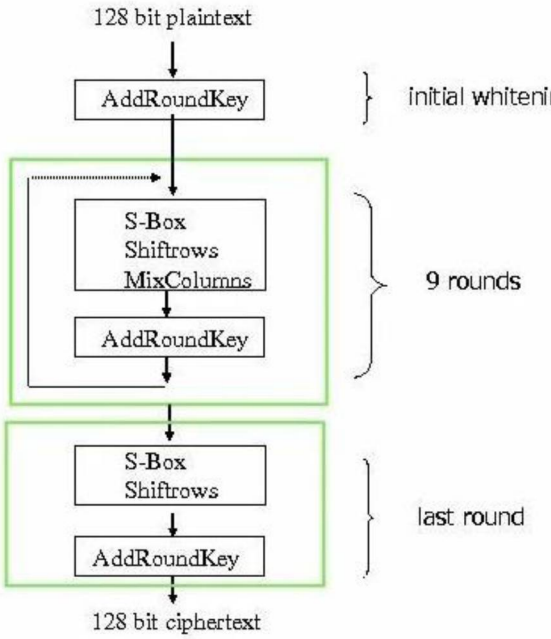

Рисунок 3 – алгоритм работы шифрования AES

Асимметричное шифрование основывается на использовании пар чисел. Одно из них — открытый ключ, который доступен любому желающему. С его помощью можно зашифровать сообщение, однако расшифровать его с помощью этого же ключа невозможно. Для расшифровки требуется второе число — закрытый ключ, который должен оставаться в тайне.

Эти два ключа не являются случайными. Открытый и закрытый ключи всегда связаны между собой через алгоритм, который их генерирует. Важным аспектом является наличие третьего, также секретного числа, которое связывает оба ключа.

Наиболее простой способ установить такую связь — взять два больших простых числа и перемножить их. Результатом будет большее число, которое служит основой нашего алгоритма. Внутри этого алгоритма применяется математика, зависящая от разложения чисел на множители. Если мы не знаем ни одно из исходных простых чисел, задача разложения такого большого числа на множители становится крайне сложной.

Распространенные алгоритмы симметричного шифрования: RSA, ECC.

RSA (Rivest–Shamir–Adleman) представляет собой алгоритм асимметричного шифрования, который функционирует на основе пары ключей: открытого и закрытого. Этот алгоритм широко используется для обеспечения безопасности данных, передаваемых по сети, и стал стандартом для цифровых подписей. Процесс работы RSA начинается с генерации двух ключей: открытого, который

предназначен для шифрования сообщений, и закрытого, который хранится в секрете. Открытый ключ состоит из двух элементов — модуля (n) и открытой экспоненты (e). Закрытый ключ также включает модуль (n), но содержит закрытую экспоненту (d), которая вычисляется так, чтобы быть мультипликативно обратной к (e) по модулю (p-1)(q-1), где (p) и (q) — это простые числа, используемые для определения (n).

Когда необходимо зашифровать сообщение, его текст преобразуется в числовое значение, которое затем возводится в степень (e) и берется по модулю (n). Это преобразование создает зашифрованный текст, который можно безопасно передать. Только обладатель соответствующего закрытого ключа имеет возможность расшифровать данное сообщение. Для расшифровки зашифрованного текста получатель использует свой закрытый ключ: он возводит зашифрованный текст в степень закрытой экспоненты (d) и берет по модулю (n), что позволяет восстановить исходное числовое значение сообщения. Этот процесс обратим лишь для того, кто знает закрытый ключ, что делает RSA надежным методом шифрования для защиты конфиденциальности передаваемых данных.

Таким образом, RSA обеспечивает безопасный обмен информацией, позволяя отправителю шифровать сообщения с использованием открытого ключа, который может быть свободно распространен, в то время как только получатель с закрытым ключом может их расшифровать. Безопасность RSA основана на математической сложности факторизации больших чисел. В дополнение к этому, для создания цифровых подписей в рамках алгоритма RSA применяются хэш-функции, на которых я хотел бы акцентировать внимание в данной работе.

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.

Шифрование с использованием эллиптических кривых (ECC) представляет собой метод криптографии с открытым ключом, основанный на математических свойствах эллиптических кривых. Этот подход обеспечивает надежный способ выполнения различных криптографических операций, включая обмен ключами, создание цифровых подписей и шифрование данных. ECC является альтернативой алгоритму RSA, который был представлен в 1977 году.

Алгоритм шифрования на основе эллиптических кривых (ECC) можно изложить следующим образом: 1. Генерация ключей: в первую очередь выбираются параметры эллиптической кривой, которые необходимы для создания ключей. Это включает в себя установление уравнения кривой и коэффициентов, определяющих её форму. Затем выбирается точка P на кривой, которая будет использоваться для формирования пары ключей. Приватный ключ представляет собой случайное число d, а публичный ключ — это точка Q, вычисляемая как dP. 2. Шифрование: для защиты сообщения M применяется публичный ключ Q. Сначала сообщение M преобразуется в точку Pm на эллиптической кривой. Далее выбирается случайная точка k на кривой, и вычисляется шифротекст C, который состоит из пары точек (kP, Pm + kQ).

Расшифрование: для восстановления сообщения C используется приватный ключ d. Сначала вычисляется kP, после чего из второй части шифротекста вычитается это значение: Pm = Pm + kQ - d(kP). Полученная точка Pm соответствует исходному сообщению M.

Значение дискретной математики в области криптографии

Дискретная математика играет ключевую роль в криптографии, так как множество алгоритмов, используемых для шифрования и расшифровки данных, основываются на различных математических концепциях и методах. К числу этих концепций относятся теория чисел, теория групп, теория полей и комбинаторика. Эти математические дисциплины предоставляют криптографам необходимые инструменты для разработки надежных систем защиты информации и безопасной передачи данных.

Например, благодаря дискретной математике возможно создание сложных математических функций, которые применяются для шифрования информации и генерации криптографических ключей. Более того, она позволяет разработать методы для проверки надежности криптографических систем и выявления потенциальных уязвимостей в них. Без применения дискретной математики современная криптография не могла бы существовать в том виде, в каком мы её знаем сегодня.

Заключение

В заключение следует подчеркнуть, что использование методов дискретной математики в криптографии является основополагающим для обеспечения безопасности передаваемых данных. Алгоритмы шифрования и дешифрования, основанные на дискретных функциях, обеспечивают надежную защиту информации от несанкционированного доступа. Также важно отметить, что разработка новых шифровальных алгоритмов остаётся актуальной задачей, особенно с учётом постоянно эволюционирующих угроз в сфере кибербезопасности. Таким образом, дискретная математика не только укрепляет основы криптографии, но и способствует её развитию в ответ на современные вызовы.

Список использованных источников:

1.Код журнал Яндекс Практикума. Симметричное шифрование[Электронный ресурс] Режим доступа: https://thecode.media/symmetric/amp/ Дата доступа: 28.03.2025

2.Код журнал Яндекс Практикума. Алгоритмы шифрования, на которых держится мир[Электронный ресурс] Режим доступа: https://thecode-media.turbopages.org/thecode.media/s/5-encrypts/ Дата доступа: 28.03.2025

3.Код журнал Яндекс Практикума. Ассиметричное шифрование[Электронный ресурс] Режим доступа: https://thecode-media.turbopages.org/thecode.media/s/asymmetric/ Дата доступа: 28.03.2025

4.Wenbo Mao, Modern Cryptography: Theory and Practice , 2003. Дата доступа: 28.03.2025

UDC 004.056.55

ENCRYPTION AND DECRYPTION OF INFORMATION BASED ON DISCRETE MATHEMATICS

Solovieva K. A., student of group 473903, Babicheva A. A., student of group 473903

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Rusina N. V. – Senior Lecturer

Annotation. This paper discusses the growing importance of data encryption and decryption in the context of digitalization and information security. The focus is on discrete mathematics methods that underlie symmetric and asymmetric encryption algorithms. Key algorithms such as AES, ECC, RSA, and DES, their working principles, implementation features, and criteria necessary to ensure the reliability of data protection are considered. The role of discrete mathematics in the development of cryptographic methods and its future prospects are emphasized. Practical aspects of encryption use and requirements for modern algorithms are also analyzed.

Keywords. Encryption, decryption, symmetric encryption, asymmetric encryption, DES, AES, RSA, ECC.