Министерство просвещения Российской Федерации

МБОУ "Гимназия №25" города Курска

Математика вокруг нас 24/25

Исследовательская работа

Способы шифрования с применением математики и криптографии

Выполнила: Байбарина Екатерина Алексеевна

ученица 9 «Г» класса

Руководитель: Жиленкова Наталья Николаевна

учитель математики

2025

Оглавление

Введение

Информация стала одним из самых ценных ресурсов современного мира. С развитием цифровых технологий, интернета и мобильных устройств объем передаваемых и хранимых данных стремительно увеличивается. В связи с этим особую актуальность приобретает вопрос защиты информации от несанкционированного доступа, подделки и разрушения. Ежедневно миллионы людей по всему миру обмениваются личными сообщениями, совершают банковские операции, отправляют электронные письма и используют облачные сервисы. Все эти действия требуют надёжных и эффективных способов защиты данных.

Криптография — наука о методах шифрования информации — играет ключевую роль в обеспечении безопасности данных. Её история насчитывает тысячи лет: от простейших шифров древности до современных сложнейших алгоритмов, основанных на высшей математике и теории информации. Криптография тесно связана с математикой: именно математические методы лежат в основе большинства алгоритмов шифрования, а их стойкость напрямую зависит от сложности математических задач, которые необходимо решить для взлома шифра.

В условиях стремительного развития вычислительной техники и появления новых угроз, таких как кибератаки и вредоносные программы, становится особенно важно понимать, как устроены современные методы защиты информации, на каких математических принципах они основаны, и какие перспективы открываются перед криптографией в будущем.

Цель данной работы - изучить математические основы криптографии и рассмотреть различные методы шифрования информации, как исторические, так и современные.

Для достижения поставленной цели были определены следующие задачи:

- проанализировать развитие криптографии от древних времён до наших дней;
- рассмотреть основные математические модели, используемые в шифровании;
- исследовать принципы работы современных криптографических алгоритмов;

Объектом исследования выступают криптографические алгоритмы, а предметом — математические методы, применяемые при их построении и анализе.

История криптографии

История криптографии насчитывает около четырех тысяч лет и тесно связана с развитием письменности и необходимостью защиты информации. Уже в древних цивилизациях - Египте, Месопотамии, Индии - встречаются примеры использования различных способов сокрытия смысла текста. В Древнем Египте для этого применялись особые иероглифы и ребусы, которые не столько скрывали смысл, сколько демонстрировали остроумие писцов и привлекали внимание к тексту. В Месопотамии около 3500 лет назад писцы использовали криптографические методы для сокрытия секретных рецептов, например, керамической глазури, что можно считать одной из первых форм коммерческой тайны

Таким образом, история криптографии — это путь от простых методов замены и перестановки к сложным математическим алгоритмам, обеспечивающим безопасность информации в современном обществе.

Шифры древности

Скитала (Древняя Спарта)

Шифр Скитала - один из самых древних способов шифрования, который применялся ещё в Древней Спарте для передачи секретных военных

сообщений. Устройство для этого шифра представляло собой цилиндрическую палочку (жезл) определённого диаметра и длины. Ключом к шифру служил именно диаметр палочки: только имея палочку с тем же диаметром, что и у отправителя, получатель мог прочитать сообщение

Описание устройства:

- Скитала — это цилиндр (жезл), на который по спирали плотно наматывалась узкая полоска пергамента, кожи или ткани
- На намотанной полоске вдоль оси цилиндра писали текст сообщения, заполняя всю длину жезла по рядам
- После написания текста полоску снимали с жезла. В таком виде буквы на ней располагались в кажущемся случайном порядке и не имели смысла для постороннего наблюдателя

Принцип работы:

- Для шифрования отправитель брал скиталу (палочку) определённого диаметра и наматывал на неё полоску пергамента виток к витку, чтобы не было промежутков
- Сообщение писалось вдоль палочки по всей длине, по строкам. Если длина сообщения превышала длину полоски, использовали новую полоску или палочку
- После окончания записи ленту разматывали и отправляли адресату

Чтобы расшифровать послание получатель должен был намотать полоску на палочку с тем же диаметром.

Пример

Если взять сообщение "НАСТУПАЙТЕ" и скиталу, на которую помещается по три буквы в ряд, то текст записывается по строкам:

```
Н А С
Т У П
А Й Т
  Е
```

Затем, разматывая ленту, получаем зашифрованный текст: "НУТАПЕСА_ТЙ"

Особенности:

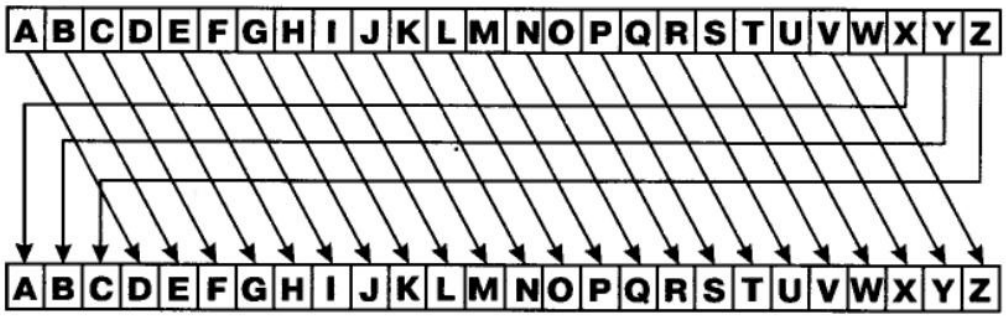
- Диаметр палочки является ключом шифрования: если он отличается, сообщение не получится прочитать
- Преимущество шифра — простота и надёжность передачи в условиях военных действий
- Недостаток — уязвимость при подборе диаметра или использовании специальных методов дешифровки

Шифр Скитала — это классический пример перестановочного шифра, где безопасность сообщения обеспечивается физическим совпадением параметров устройства у отправителя и получателя.

Шифр Цезаря

В Древнем Риме получил распространение шифр Цезаря - простой метод замены, при котором буквы алфавита сдвигались на фиксированное число позиций. Этот шифр стал одним из самых известных в истории и долгое время считался надёжным.

Шифр Цезаря - это один из самых простых и известных методов шифрования, относящийся к шифрам подстановки. Его суть заключается в том, что каждая буква исходного текста заменяется на букву, находящуюся в алфавите на фиксированное число позиций правее или левее. Это число называется сдвигом и является ключом шифра. Например, при сдвиге на 3 буква «А» превращается в «Г», «Б» - в «Д», и так далее. Если сдвиг выходит за пределы алфавита, то отсчёт продолжается с начала алфавита.



Шифр назван в честь римского полководца Гая Юлия Цезаря, который использовал этот способ для секретной переписки со своими военачальниками. Обычно он выбирал сдвиг, равный трём.

Математическая модель

Если каждой букве сопоставить её порядковый номер в алфавите, то шифрование можно выразить формулой:

$$E(x) = (x + n) mod N$$

где

- x — номер буквы исходного текста,
- n — сдвиг (ключ),
- N — количество букв в алфавите

Пример шифрования (английский язык, сдвиг 3)

Исходный текст: *HELLO*. Сдвиг: 3

H → K, E → H, L → O, L → O, O → R

Результат: *KHOOR*.

Особенностью шифра Цезаря является то, что неалфавитные символы (пробелы, знаки препинания, цифры) обычно не изменяются.

Полиалфавитные шифры

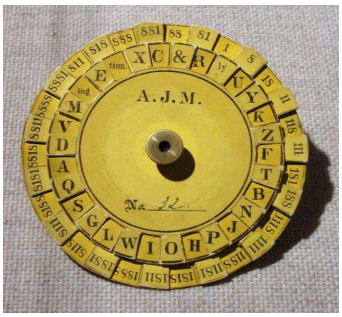
В Средние века криптография распространилась среди дипломатов, купцов и даже простых граждан. Основным методом оставались моноалфавитные шифры, где каждая буква заменялась на другую по определённому правилу. Однако с развитием методов криптоанализа, в частности частотного анализа, такие шифры стали уязвимыми. В ответ на это появились более сложные системы - полиалфавитные шифры. В IX веке арабский учёный Ал-Кинди впервые описал частотный анализ, что стало важным этапом в развитии криптоанализа.

Леон Баттиста Альберти (1404–1472) — итальянский учёный эпохи Возрождения, ставший основоположником западноевропейской криптографии. В

своём «Трактате о шифрах» (1466 г.) он впервые предложил идею многоалфавитного шифра и изобрёл диск Альберти — устройство для реализации шифра замены.

Диск Альберти состоял из двух концентрических дисков:

- внешний диск содержал стандартный алфавит и цифры;
- внутренний диск включал перемешанный алфавит и дополнительные символы.



Принцип шифрования:

- диски выравнивались по начальной позиции (ключ шифра);
- для каждой буквы открытого текста на внешнем диске находили соответствующую букву на внутреннем диске;
- после шифрования нескольких слов внутренний диск поворачивали, меняя алфавит (сигналом смены служила заглавная буква в тексте).

Этот метод позволял использовать несколько алфавитов в одном сообщении, что усложняло частотный анализ.

Другим примером полиалфавитного шифра является шифр Виженера. В нём используется ключевое слово для определения сдвига каждой буквы.

Например, для ключа *KEY* и сообщения *HELLO*:

- Ключ повторяется: *K E Y K E*.
- Каждая буква ключа определяет сдвиг:
  - *H* (7) + *K* (10) = 17 → *R*,
  - *E* (4) + *E* (4) = 8 → *I*,
  - *L* (11) + *Y* (24) = 35 → 35–26=9 → *J*,
  - *L* (11) + *K* (10) = 21 → *V*,
  - *O* (14) + *E* (4) = 18 → *S*.

Результат: *HELLO* → *RIJVS*.

Хотя шифр Виженера сложнее взломать, чем моноалфавитные, он не является абсолютно стойким. Метод Касиски позволяет определить длину ключа, анализируя повторяющиеся последовательности в зашифрованном тексте.

XX Век

Настоящую революцию в криптографии принес XX век. В этот период появились электромеханические шифровальные машины, самой известной из которых стала "Энигма". Она использовалась в гитлеровской Германии для защиты военной переписки. Принцип работы "Энигмы" основывался на сложной системе роторов, что обеспечивало огромное количество возможных комбинаций. Взлом шифра "Энигмы" польскими и британскими криптоаналитиками, в том числе с помощью математических методов, стал одним из ключевых событий Второй мировой войны

С середины XX века начался переход к математической криптографии. Клод Шеннон ввёл строгие математические понятия количества информации, энтропии и функций шифрования, что позволило анализировать стойкость шифров с научной точки зрения. В 1970-х годах появились первые асимметричные алгоритмы (например, RSA), основанные на сложных математических задачах, таких как факторизация больших чисел и вычисление дискретного логарифма. Это открыло новую эру в защите информации и сделало криптографию неотъемлемой частью цифрового мира

Энигма

"Энигма" — роторная шифровальная машина, ставшая символом криптографии XX века. Её история началась в 1918 году, когда немецкий инженер Артур Шербиус получил патент на электромеханическое устройство для шифрования. К началу Второй мировой войны «Энигма» стала основным

инструментом шифрования в нацистской Германии, а её взлом сыграл ключевую роль в победе союзников.

Машина состояла из:

- клавиатуры для ввода текста;
- набора роторов (3–8 штук), каждый с 26 контактами (по числу букв латинского алфавита);
- рефлектора, замыкавшего электрическую цепь обратно через роторы;
- коммутационные панели для дополнительных замен пар букв.

Процесс шифрования происходил следующим образом:

- при нажатии клавиши правый ротор сдвигался на одну позицию. после полного оборота он проворачивал средний ротор, а тот - левый;
- электрический сигнал проходил через роторы, рефлектор и возвращался обратно, зажигая лампочку с зашифрованной буквой;
- каждое нажатие меняло схему соединений, обеспечивая уникальное преобразование для каждой буквы. Если исходная буква A при первом нажатии превращалась в G, то при следующем нажатии (после сдвига ротора) она могла стать M.

В 1932 году польские математики Мариан Реевский, Ежи Ружицкий и Генрих Зыгальский первыми взломали "Энигму".

В годы войны в Блетчли-парк Алан Тьюринг усовершенствовал метод расшифровки, сократив время дешифровки с дней до часов, что позволило перехватывать оперативные приказы вермахта.

DES

Симметричный блочный шифр — это разновидность симметричного шифра, в котором для шифрования и расшифрования используется один и тот же секретный ключ, а данные обрабатываются не по одному символу, а группами фиксированной длины, называемыми блоками (например, 64 или 128 бит).

В процессе шифрования исходный текст разбивается на такие блоки, каждый из которых по определённому алгоритму преобразуется в блок зашифрованного текста с помощью секретного ключа. Если последний блок данных меньше установленной длины, он дополняется специальными символами.

Блочные шифры отличаются от потоковых тем, что работают с группами бит (блоками), а не с потоком данных по одному символу или биту. Примеры симметричных блочных шифров: DES, AES, ГОСТ 28147-89, Blowfish, Twofish.

К достоинствам симметричных блочных шифров относятся высокая скорость работы и простота реализации, однако для их использования стороны должны заранее обменяться секретным ключом и хранить его в тайне.

DES (Data Encryption Standard) - симметричный блочный шифр, разработанный в 1970-х годах. Он стал первым открытым стандартом, заложив основы современной криптографии. Несмотря на историческую значимость, сегодня он считается устаревшим и не используется.

RSA

Алгоритм RSA, разработанный в 1977 году Роном Ривестом, Ади Шамиром и Леонардом Адлеманом, стал прорывом в защите информации. Его появление связано с решением проблемы безопасной передачи ключей, которая существовала в симметричных системах (например, DES). До RSA для шифрования требовался общий секретный ключ, что делало коммуникацию уязвимой при перехвате ключа.

Принцип работы

Ключевые этапы:

1. Генерация ключей:
   - выбираются два больших простых числа $p и q$;
   - вычисляется модуль $p \times q$ и функция Эйлера $\phi(n) = (p-1)(q-1)$;
   - публичный ключ: пара (e, n), где e - число, взаимно простое с $\phi(n)$;
   - приватный ключ: число d, удовлетворяющее условию $e \times d \equiv 1 mod \phi(n)$;
2. Шифрование:
   - Сообщение m преобразуется в число и шифруется: $c = m^e mod\, n$
3. Дешифрование:
   - Для расшифровки используется приватный ключ: $m = c^d mod\, n$

Пример. Если Коля хочет отправить секретное сообщение Алисе, то Коля берёт публичный ключ Алисы (e, n) и шифрует им сообщение. Алиса расшифровывает его своим приватным ключом d. Даже если Весельчак У и Крыс перехватят зашифрованный текст и публичный ключ, без знания d они не смогут восстановить исходное сообщение.

Математические основы

Математические основы криптографии — это простые числа, модульная арифметика, алгебраические структуры и вероятностные методы. Без них невозможно представить ни один современный алгоритм защиты информации.

Простые числа, их свойства.

Простые числа — это такие натуральные числа больше 1, которые имеют ровно два делителя: единицу и самих себя. Например: 2, 3, 5, 7, 11, 13, 17, 19 и так далее.

Свойства простых чисел:

- Основная теорема арифметики: любое натуральное число можно единственным образом разложить в произведение простых множителей. Например, 30=2×3×5.
- Бесконечность простых чисел, что было доказано ещё Евклидом.
- Сложность факторизации: если известно произведение двух больших простых чисел, очень сложно найти сами множители. Именно на этом свойстве основана стойкость алгоритма RSA.

Применение:

- В алгоритме RSA два больших простых числа pиq перемножают, чтобы получить модуль n. Без знания pиq невозможно быстро вычислить секретный ключ.
- В протоколе Диффи-Хеллмана для обмена ключами также используются простые числа и их свойства.

Модульная арифметика

Модульная арифметика — это система вычислений, в которой результатом операции становится остаток от деления на некоторое число (модуль).

Обозначение: $a \equiv b(mod m)$ означает, что $a и b$ дают одинаковый остаток при делении на m.

Примеры:

- $17 \equiv 5 (\text{mod } 12)$, потому что $17 - 5 = 12$;
- $23 \equiv 2 (\text{mod } 7)$, потому что $23 = 3 \times 7 + 2$.

Применение в криптографии:

- В RSA шифрование и расшифрование происходят по формуле:
  - $c = m^e mod n$
  - $m = c^d mod n$
  - где m — исходное сообщение, c — зашифрованное сообщение, $e и d$ — ключи, n — модуль.

В шифре Цезаря также используется модульная арифметика: если алфавит состоит из 26 букв, то сдвиг вычисляется по модулю 26.

Алгебраические структуры: группы, поля

Группы

Группа — это множество элементов с определённой операцией, удовлетворяющей четырём основным свойствам:

- замкнутость: результат операции над двумя элементами из группы также принадлежит группе;
- ассоциативность: $(a * b) * c = a * (b * c)$;
- нейтральный элемент: существует элемент e, такой что $a * e = a$;
- обратный элемент: для каждого a есть элемент b, такой что $a * b = e$.

Пример

- Множество целых чисел с операцией сложения (Z,+) образует группу, где нейтральным элементом является ноль.

Пример из криптографии

- В протоколе Диффи-Хеллмана используется группа вычетов по модулю простого числа.

Поля

Поле — это множество, в котором определены две операции (сложение и умножение), причём обе операции образуют группы (кроме нуля для умножения), и выполняется дистрибутивность.

Пример

- Множество чисел по модулю простого $p(\mathbb{Z}_p)$ — это поле. Например, $\mathbb{Z}_7 = \{0,1,2,3,4,5,6\}$.

Пример из криптографии:

- в алгоритме Эль-Гамаля вычисления происходят в поле вычетов по простому модулю;
- в алгоритме AES используются поля Галуа $GF(2^8)$, где каждый байт рассматривается как элемент поля из 256 элементов.

Вероятностные методы

Вероятностные методы широко используются в криптографии для генерации ключей, проверки простоты чисел и создания псевдослучайных последовательностей.

Примеры:

- генерация простых чисел. Для создания ключей RSA требуется быстро находить большие простые числа. Используются вероятностные тесты простоты, например, тест Миллера-Рабина. Тест не даёт абсолютной гарантии, но вероятность ошибки можно сделать сколь угодно малой;
- псевдослучайные числа. Для создания ключей, одноразовых блокнотов, инициализационных векторов (IV) и других криптографических параметров используются генераторы псевдослучайных чисел. Например, в протоколе TLS для каждого соединения генерируется уникальный случайный ключ;
- случайный выбор параметров. В протоколе Эль-Гамаля для каждого сообщения выбирается случайное число k, чтобы даже одинаковые сообщения шифровались по-разному;
- в электронной подписи DSA каждый раз для подписи сообщения выбирается новое случайное число, чтобы подпись была уникальной.

Заключение

В ходе выполнения данного проекта были рассмотрены основные способы шифрования информации с применением математики и криптографии. Мы убедились, что защита данных невозможна без глубокого понимания математических основ: простых чисел, модульной арифметики, алгебраических структур и вероятностных методов. Именно математика позволяет создавать надёжные алгоритмы, которые ежедневно обеспечивают безопасность электронной почты, банковских операций, социальных сетей и других сфер цифровой жизни.

История криптографии наглядно показывает, как с развитием науки и техники совершенствовались методы шифрования: от простейших шифров древности до современных сложных алгоритмов, таких как RSA и AES. Особенно интересным этапом стало появление асимметричных методов, позволивших решить проблему безопасного обмена ключами и заложивших основу для цифровых подписей, электронной коммерции и защищённого интернета.

Сегодня криптография продолжает активно развиваться. На смену классическим методам приходят квантовые и постквантовые технологии, способные противостоять даже самым мощным компьютерам будущего. Это открывает новые перспективы для защиты информации, но требует постоянного изучения и совершенствования математических моделей.

Таким образом, математика и криптография неразрывно связаны между собой. Без математических знаний невозможно создать ни один современный шифр. Изучение этой области не только повышает уровень информационной безопасности, но и развивает логическое мышление, умение анализировать и решать сложные задачи.

Список литературы

4. Адаменко М. Основы классической криптологии. Секреты шифров и кодов. - М.: ДМК Пресс, 2020. - 305 с.
5. Граймс Роджер Апокалипсис криптографии. Подготовка криптографии к квантовым вычислениям - М.: ДМК-Пресс, 2021. - 286 с.
6. Жельников В. Криптография от папируса до компьютера. - М.: ABF, 2016.
7. Мандельброт Б. "Криптография и тайнопись". -М.: «Институт компьютерных исследований», 2002. - 123 с.
8. Мартынов Л. Алгебра и теория чисел для криптографии. Учебное пособие для вузов - М.:Лань, 2022. - 456 с.
9. Никифоров С. Методы защиты информации. Шифрование данных. Учебное пособие - М.:Лань, 2019. - 160 с.
10. Применко Э. А. Алгебраические основы криптографии. / Э.А. Применко. - М.: Либроком, 2018. - 288 с.
11. Червяков, Коляда, Ляхов Модулярная арифметика и ее приложения в инфокоммуникационных технологиях. - М.:Физматлит, 2017. - 400 с.