МБОУ «Камскоустьинская общеобразовательная средняя школа»

Камско-Устьинского муниципального района Республики Татарстан

**ИНДИВИДУАЛЬНЫЙ ПРОЕКТ**

«КОДИРОВАНИЕ.КРИПТОГРАФИЯ»

**Выполнила:**

ученица 10Б классШамсиева Диляра

**Руководитель проекта:** Ибатуллина Алия Гусмановна

п.г.т. Камское-Устье 2023-2024 г.

Оглавление

[ВВЕДЕНИЕ 3](#_Toc164717734)

[1. ИСТОРИЯ КРИПТОГРАФИИ 5](#_Toc164717735)

[2. КРИПТОГРАФИЯ 6](#_Toc164717736)

[3. ИСТОРИЯ КОДИРОВАНИЯ 8](#_Toc164717737)

[4. КОДИРОВАНИЕ 10](#_Toc164717738)

[5. ОБЛАСТИ ПРИМЕНЕНИЯ МЕТОДОВ КОДИРОВАНИЯ 12](#_Toc164717739)

[6. ПРАКТИЧЕСКАЯ ЧАСТЬ 14](#_Toc164717740)

[СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ 15](#_Toc164717741)

# ВВЕДЕНИЕ

Вся жизнь человека, так или иначе, связана с получением, накоплением и обработкой информации. Что бы человек ни делал: читает ли он книгу, смотрит ли он телевизор, разговаривает, он постоянно и непрерывно получает и обрабатывает информацию.

Любой живой организм, в том числе человек, является носителем генетической информации, которая передается по наследству. Генетическая информация хранится во всех клетках организма в молекулах ДНК. Молекула ДНК человека включает в себя около трех миллиардов пар нуклеотидов, и в ней закодирована вся информация об организме человека: его внешность, здоровье или предрасположенность к болезням, способности и т.д.

Человек воспринимает окружающий мир, благодаря своим органам. Чтобы правильно ориентироваться в окружающем мире, он запоминает полученную информацию, принимает решения и передаёт, и принимает информацию.

История кодирования информации начинается в доисторической эпохе, когда первобытный человек выбивал в скале образы известных ему объектов окружающего мира. Кодирование информации необычайно разнообразно. Указания водителю автомобиля кодируются в виде дорожных знаков. Музыкальное произведение кодируется с помощью знаков нотной грамоты, для записи шахматных партий и химических формул созданы специальные системы записи. Любой грамотный компьютерный пользователь знает о существовании кодировок символов. Географическая карта кодирует информацию о местности. Необходимость кодирования речевой информации возникла в связи с бурным развитием техники связи, особенно мобильной связи. Людьми были придуманы специальные коды: Азбука Брайля, азбука Морзе, флажковая азбука и т.д. Кодирование делится на три основных способа: числовой способ, символьный способ, графический способ.

Цели и задачи:

* Ознакомится с информацией кодирования и криптографии
* Узнать про основателей криптографии и кодирования и историю создания.

Актуальность в 21 веке:

На сей день эта тема очень актуальна, т.к. у людей пропала приватность. Все телефонные линии прослушиваются, а IP компьютеров и др. устройств с доступом в интернет фиксируются. И на данный момент чаще всего происходят взломы наших данных, потому что вся наша информация расписана в интернете.

# ИСТОРИЯ КРИПТОГРАФИИ

История криптографии начинается задолго до нашей эры, когда первые методы шифрования использовались для защиты военных сообщений и секретных дипломатических переговоров. Одним из самых ранних примеров криптографии является шифр Цезаря, который использовался в Древнем Риме для сокрытия военных докладов.

С развитием технологий и математических методов криптография стала более сложной и эффективной. В средние века использовались различные шифры, такие как шифр Виженера, который использовал полиалфавитный подход к шифрованию.

**Ключевые фигуры в развитии криптографии**

* Алан Тьюринг:

Во время Второй мировой войны Тьюринг был ключевой фигурой в дешифровании немецкого шифра Энигма, что существенно повлияло на ход войны. Его работы также оказали огромное влияние на развитие компьютерной науки.

* Уитфилд Диффи и Мартин Хеллман:

Они разработали концепцию асимметричного шифрования и публичных ключей, что существенно изменило подход к шифрованию и обеспечило более безопасный обмен ключами.

* Ривест, Шамир и Адлеман (RSA):

Эти ученые создали один из наиболее популярных алгоритмов асимметричного шифрования, который используется до сих пор для защиты данных в сети.

# КРИПТОГРАФИЯ

Криптография - это область информатики, которая занимается защитой информации от несанкционированного доступа, использования, раскрытия, изменения или уничтожения. Криптографические методы используются для шифрования информации, чтобы сделать ее нечитаемой для неавторизованных лиц. Наиболее распространенными криптографическими методами являются:

**Симметричное шифрование**

Симметричное шифрование — это способ шифрования данных, при котором один и тот же ключ используется и для кодирования, и для восстановления информации. До 1970-х годов, когда появились первые асимметричные шифры, оно было единственным криптографическим методом. Принцип работы симметричных алгоритмов. В целом симметричным считается любой шифр, использующий один и тот же секретный ключ для шифрования и расшифровки.

**Асимметричное шифрование**

Асимметричное шифрование — это метод шифрования данных, предполагающий использование двух ключей — открытого и закрытого. Открытый (публичный) ключ применяется для шифрования информации и может передаваться по незащищенным каналам. Закрытый (приватный) ключ применяется для расшифровки данных, зашифрованных открытым ключом.

**Хеширование**

Криптографические хеш-функции — незаменимый и повсеместно распространенный инструмент, используемый для выполнения целого ряда задач, включая аутентификацию, проверку целостности данных, защиту файлов и даже обнаружение зловредного ПО. Существует масса алгоритмов хеширования, отличающихся криптостойкостью, сложностью, разрядностью и другими свойствами. Считается, что идея хеширования принадлежит сотруднику IBM, появилась около 50 лет назад и с тех пор не претерпела принципиальных изменений. Зато в наши дни хеширование обрело массу новых свойств и используется в очень многих областях информационных технологий

# ИСТОРИЯ КОДИРОВАНИЯ

Кодирование, в отличие от криптографии, нацелено не на скрытие смысла сообщения, а на преобразование его формы для удобства передачи или хранения. История кодирования также богата событиями и личностями, которые внесли значительный вклад в это направление.

Ранние методы кодирования включали использование специальных символов или символьных замен для сжатия информации или обеспечения ее целостности. Например, в Древнем Египте использовались иероглифы для записи информации на папирусе.

С развитием технологий и появлением компьютеров методы кодирования стали более сложными и эффективными. Сегодня кодирование играет важную роль в сфере информационных технологий, включая сжатие данных, передачу информации через сети, а также обработку мультимедийных данных.

В современной эпохе существует множество методов кодирования, включая алгоритмы сжатия данных (например, алгоритмы Хаффмана, LZ77, Deflate), алгоритмы шифрования (например, AES, RSA), а также специализированные методы кодирования для обработки аудио, видео и изображений.

**Ключевые фигуры в развитии кодирования**

* Клод Шеннон:

Считается отцом информационной теории, Шеннон внес огромный вклад в развитие теории кодирования и сжатия данных. Его работа "Математическая теория связи" стала фундаментом для многих современных методов кодирования и сжатия данных.

* Ричард Хэмминг

Американский математик и инженер, известный своими работами в области обнаружения и исправления ошибок в цифровых системах передачи данных. Его код Хэмминга стал основой для многих схем обнаружения и исправления ошибок.

* Джеймс Ларкер:

Пионер в области аудиокодирования, Ларкер внес существенный вклад в разработку алгоритмов сжатия аудио данных, таких как MP3, AAC и других.

# КОДИРОВАНИЕ

Кодирование - это процесс преобразования информации из одного формата в другой. Существует множество различных методов кодирования, каждый из которых имеет свои преимущества и недостатки. Наиболее распространенными методами кодирования являются:

**Бинарное кодирование(двоичное)**

Двоичное кодирование – это кодирование информации с помощью двух знаков. Чтобы сохранить информацию в памяти компьютера, её кодируют с помощью двух конкретных знаков – цифр ноль и один. Этот способ кодирования связан с устройством компьютерной памяти. Компьютер не понимает смысла данных, которые находятся в его памяти. Он может работать только с электрическими сигналами и различает два состояния: «есть сигнал» и «нет сигнала».

**Текстовое**

Кодирование текста - это процесс преобразования символов или слов в последовательность чисел или символов, которые могут быть сохранены, переданы или обработаны компьютером. Это важная часть работы с данными и информацией, особенно в цифровой среде.

**Графическое кодирование**

Кодирование графической информации — это процесс преобразования графической информации из аналоговой формы в цифровую путём разбиения графического изображения (дискретизации).

Каждому элементу изображения назначается конкретное значение в форме двоичного кода. При кодировании изображения происходит его пространственная дискретизация. Её можно сравнить с построением изображения из большого количества цветных фрагментов (метод мозаики).

**Аудиокодирование**

В основе кодирования звука с использованием ПК лежит процесс преобразования колебаний воздуха в колебания электрического тока и последующая дискретизация аналогового электрического сигнала. Кодирование и воспроизведение звуковой информации осуществляется с помощью специальных программ (редактор звукозаписи). Качество воспроизведения закодированного звука зависит от частоты дискретизации и её разрешения (глубины кодирования звука — количество уровней).

**Видеокодирование**

Кодирование видео — это процесс преобразования видеосигнала в эффективный формат для хранения или передачи. Во время кодирования видео сокращается количество данных, необходимых для представления оригинального контента, что позволяет экономить пространство на диске и ускорять передачу информации.

Источник - Онлайн школа Skysmart: https://skysmart.ru/articles/programming/kodirovanie-videoinformacii.

# ОБЛАСТИ ПРИМЕНЕНИЯ МЕТОДОВ КОДИРОВАНИЯ

**Безопасная передача данных:**

Это процесс обеспечения защиты информации во время передачи между двумя или более устройствами.

Для обеспечения безопасной передачи данных используются различные методы шифрования, такие как SSL/TLS (Secure Sockets Layer/Transport Layer Security), которые обеспечивают защищенное соединение между клиентом и сервером.

Важно также использовать безопасные протоколы передачи данных, такие как HTTPS для веб-сайтов, чтобы защитить информацию пользователя во время передачи.

**Хранение конфиденциальных данных:**

Это процесс обеспечения защиты информации, хранящейся на устройствах или серверах, от несанкционированного доступа или утечки.

Для защиты конфиденциальных данных часто используются методы шифрования, доступ к данным контролируется через системы управления доступом, а также могут применяться другие меры безопасности, такие как аудит и мониторинг активности.

**Аутентификация:**

Это процесс проверки подлинности пользователя или устройства перед предоставлением доступа к системе или ресурсам.

Существует несколько методов аутентификации, включая пароли, биометрические данные (отпечатки пальцев, распознавание лица и т. д.), а также использование аутентификационных токенов или смарт-карт.

**Целостность данных:**

Это обеспечение того, чтобы данные оставались целостными и неизменными во время хранения, передачи и обработки.

Для обеспечения целостности данных часто используются хэш-функции, которые создают фиксированный длинный хэш-код из данных, который можно использовать для проверки целостности. Любое изменение данных приведет к изменению хэш-кода.

**Цифровые подписи:**

Это метод аутентификации и обеспечения целостности данных путем создания уникальной электронной подписи для каждого сообщения или документа.

Цифровые подписи создаются с использованием криптографических алгоритмов, которые обеспечивают уникальность подписи и позволяют проверить ее подлинность и целостность данных.

Подпись создается с использованием закрытого ключа отправителя и может быть проверена с использованием соответствующего открытого ключа. Любое изменение данных приведет к невозможности проверки подписи.

.

# ПРАКТИЧЕСКАЯ ЧАСТЬ

Одним из методов шифрования информации является азбука Морзе. Это способ знакового кодирования, в котором буквы алфавита, цифры, знаки препинания и другие символы представляются в виде последовательностей коротких и длинных сигналов, называемых точками и тире. Предназначена для передачи по последовательным каналам связи. Уникальной особенностью азбуки Морзе является возможность кодирования и декодирования человеком без применения специальных терминальных устройств.

В рамках практической части проекта мы зашифруем первое четверостишье стихотворения А. С. Пушкина «У лукоморья дуб зеленый».

*У лукоморья дуб зелёный;  
Златая цепь на дубе том:  
И днём и ночью кот учёный  
Всё ходит по цепи кругом;*

..- / .-.. ..- -.- --- -- --- .-. -..- .-.- / -.. ..- -... / --.. . .-..

-. -.-- .--- -.-.-. / --.. .-.. .- - .- .-.- / -.-. . .--. -..- / -. .- / -.. ..- -... . / - --- -- ---... / .. / -.. -.

-- / .. / -. --- ---. -..- ..-- / -.- --- - / ..- ---.

-. -.-- .--- / .-- ...

/ .... --- -.. .. - / .--. --- / -.-. . .--. .. / -.- .-. ..- --. --- -- -.-.-.

# СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Диффи У., Хеллман М. Э. (1976). Новые направления в криптографии. IEEE Transactions по теории информации,
2. Кан Д. (1967). Взломщики кодов: Всеобъемлющая история секретных коммуникаций с древних времен до появления Интернета. Скрибнер.
3. Шеннон, К. Э. (1948). Математическая теория коммуникации. Технический журнал Bell System,
4. Сингх, С. (2000). Книга кодов: Наука о секретности от Древнего Египта до квантовой криптографии. Якорь.
5. Столлингс, У. (2019). Криптография и сетевая безопасность: принципы и практика (8-е изд.). Пирсон.
6. Траппе, В., & Вашингтон, Л. С. (2006). Введение в криптографию с теорией кодирования (2-е изд.). Пирсон.
7. Возенкрафт, Дж. М., и Райфен, Б. А. (1961). Последовательная расшифровка. Издательство Массачусетского технологического института.