Ответы на РОЯ

1. Предмет и задачи криптографии. История криптографии. Основные термины.

*Криптография* - наука о защите данных через шифрование и дешифрование, обеспечивая конфиденциальность, целостность и аутентичность информации.

*Задачи криптографии*: Конфиденциальность (секретность данных), Целостность (защита от несанкционированных изменений), Аутентичность (подтверждение подлинности). *История криптографии*: Начало криптографии уходит в древние времена и включает шифры, используемые в Египте, Месопотамии и Римской империи. Во время Второй мировой войны криптография достигла значительного прогресса с появлением механических и электромеханических шифровальных машин, таких как "Энигма". В современной эпохе криптография включает разнообразные методы, алгоритмы и протоколы для защиты информации в цифровом мире.

*Основные термины в криптографии:*

* Шифрование: процесс преобразования открытого текста в зашифрованный текст с использованием шифра или ключа.
* Расшифрование: процесс преобразования зашифрованного текста в открытый текст с использованием правильного ключа или алгоритма.
* Ключ: секретная информация, используемая для шифрования и расшифрования данных.
* Шифр: алгоритм или метод, используемый для преобразования данных в нечитаемую форму.
* Криптосистема: совокупность алгоритмов, протоколов и ключей, используемых для шифрования и рас

1. Элементы теории множеств. Группы, кольца, поля. Делимость чисел. Признаки делимости. Простые и составные числа.

*Элементы теории множеств* - изучение свойств и отношений множеств, включая операции объединения, пересечения, разности и декартова произведения.

*Группы* - алгебраическая структура, состоящая из множества элементов и операции, обладающей свойствами ассоциативности, замкнутости и наличия нейтрального и обратного элементов.

*Кольца* - алгебраическая структура, состоящая из множества элементов и двух операций: сложения и умножения. Кольцо должно удовлетворять определенным аксиомам.

*Поля* - это кольцо, в котором каждый ненулевой элемент обратим относительно умножения. Поля используются в алгебре и математическом анализе.

*Делимость чисел* - отношение между двумя числами, когда одно число делится нацело на другое. Если число A делится нацело на число B, то говорят, что B является делителем A. *Признаки делимости* - методы определения, делится ли одно число на другое без остатка, например, проверка на делимость на 2, 3, 5, 9 и 11, основанные на свойствах цифр числа. *Простые числа* - имеют только два делителя: 1 и само число. *Составные числа* - имеют более двух делителей и могут быть разложены на простые множители.

1. Взаимно простые числа. Алгоритм Евклида для нахождения НОД. Отношения сравнимости. Свойства сравнений. Модульная арифметика.

*Взаимно простые числа*: Два числа считаются взаимно простыми, если их наибольший общий делитель (НОД) равен 1. Это означает, что у них нет общих делителей, кроме 1. *Алгоритм Евклида для нахождения НОД*: Алгоритм Евклида - это эффективный метод нахождения наибольшего общего делителя двух чисел. Он основан на принципе, что НОД двух чисел равен НОД их остатка от деления одного числа на другое.   
*Отношение сравнимости* определяет, какие числа взаимно сравнимы или эквивалентны по определенным правилам. Например, два числа считаются сравнимыми по модулю n, если их разность делится нацело на n.   
*Свойства сравнений:* Сравнения обладают несколькими свойствами:   
 1. Рефлексивность: любое число сравнимо с самим собой.  
 2. Симметричность: если a сравнимо с b, то b сравнимо с a.   
 3. Транзитивность: если a сравнимо с b и b сравнимо с c, то a сравнимо с c.  
 4. Добавление и умножение: если a сравнимо с b по модулю n и c сравнимо с d по модулю n, то a+c сравнимо с b+d, а a\*c сравнимо с b\*d по модулю n.  
 *Модульная арифметика* - это система вычислений, основанная на операциях с остатками. Она использует модуль (число, по которому производится деление) для ограничения значений и работает с остатками от деления. Модульная арифметика имеет много применений в криптографии, компьютерной науке и других областях.

1. Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю.

*Классы* - это наборы чисел, которые имеют одинаковые остатки при делении на заданное число. *Полная и приведенная система вычетов*: Полная система вычетов по модулю n состоит из всех возможных вычетов от 0 до n-1. Приведенная система вычетов - это набор наименьших неотрицательных вычетов, каждый из которых представляет свой класс вычетов. *Функция Эйлера* φ(n) для положительного целого числа n определяет количество положительных целых чисел, которые меньше n и взаимно просты с n. Она имеет важное значение в теории чисел и в криптографии.   
*Теорема Ферма-Эйлера* устанавливает, что для любого положительного целого числа n и взаимно простого целого числа a, a возводимое в степень φ(n) (функция Эйлера от n), даёт остаток 1 при делении на n.   
*Алгоритм быстрого возведения в степень по модулю* используется для эффективного вычисления больших степеней числа по модулю. Он основан на свойствах бинарного разложения показателя степени и позволяет сократить количество операций умножения. Этот алгоритм широко применяется в криптографии и других областях, где требуется работа с большими числами и модулями.

1. Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида.

*Сравнения первой степени* (или линейные сравнения) представляют собой уравнения вида ax ≡ b (mod n), где a, b и n - целые числа, и ≡ обозначает сравнимость по модулю n. Задача состоит в нахождении всех целых решений x, которые удовлетворяют данному сравнению. *Линейные диофантовы уравнения* имеют вид ax + by = c, где a, b, c, x и y - целые числа, и требуется найти целочисленные решения x и y, которые удовлетворяют уравнению. Решение таких уравнений может быть найдено с использованием расширенного алгоритма Евклида.   
*Расширенный алгоритм Евклида* - это алгоритм, который позволяет находить наибольший общий делитель (НОД) двух чисел, а также представлять его в виде линейной комбинации этих чисел. Этот алгоритм является модификацией обычного алгоритма Евклида и позволяет эффективно находить НОД и решать линейные диофантовы уравнения.

1. Китайская теорема об остатках. Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.

*Китайская теорема* об остатках позволяет решать системы сравнений, состоящие из нескольких уравнений. *Проверка чисел на простоту* - это процесс определения, является ли число простым или составным. *Алгоритмы генерации простых чисел* - методы создания последовательности простых чисел. *Метод пробных делений* - метод проверки чисел на простоту путем последовательной проверки деления на все числа, меньшие квадратного корня числа. *Решето Эратосфена* - алгоритм для нахождения всех простых чисел до заданного числа N путем вычеркивания кратных чисел из начального списка.

1. Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.

*Разложение числа на множители* - это процесс разбиения данного числа на простые множители. Это важная задача в математике и криптографии, так как многие криптографические алгоритмы основаны на сложности факторизации больших чисел.  
*Алгоритмы факторизации -* это методы и процессы разложения чисел на их простые множители. Факторизация чисел играет важную роль в математике, криптографии и других областях, так как многие алгоритмы и системы защиты основаны на сложности факторизации больших чисел. Алгоритмы факторизации разрабатываются для нахождения множителей чисел, особенно когда эти числа являются большими и состоят из большого количества цифр.  
*Факторизация Ферма* основана на предположении Ферма, которое гласит, что если число N является составным и может быть разложено на множители, то оно может быть представлено в виде разности двух квадратов: N = a^2 - b^2. Используя это предположение, мы можем выразить N как произведение двух множителей: N = (a + b)(a - b). Таким образом, мы ищем числа a и b, которые удовлетворяют этому равенству. Этот метод может быть эффективным для некоторых чисел, но для других может потребоваться использование других алгоритмов.  
*Метод Полларда* основан на идее поиска периодов в последовательности чисел, генерируемых функцией. Этот метод называется "методом кроликов и черепах". Он использует случайные числа и функцию, которая генерирует последовательность чисел. Затем метод Полларда анализирует полученную последовательность, и если есть периодические повторения, то можно получить множитель числа N. Этот метод особенно эффективен для чисел с малым различием между множителями.

1. Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.

*Алгоритмы дискретного логарифмирования* - это методы вычисления дискретного логарифма, то есть нахождения значения x в уравнении a^x ≡ b (mod m), где a, b и m - заданные числа.  
*Метод Полларда*, также известный как "метод кроликов и черепах", основан на принципе поиска периодов в последовательности чисел. Он использует случайные числа и функцию, которая генерирует последовательность чисел. Затем метод Полларда анализирует полученную последовательность и ищет периодические повторения. Это позволяет найти приближенное значение дискретного логарифма. Метод Полларда является одним из наиболее распространенных и эффективных алгоритмов для вычисления дискретного логарифма.  
*Метод Шорра* - это квантовый алгоритм, разработанный Питером Шором. Он использует принципы квантовой вычислительной теории для эффективного вычисления дискретного логарифма и факторизации больших чисел. Метод Шорра основан на алгоритме периодической оценки Фурье (Period Finding) и факторизации больших чисел. В квантовых вычислениях этот алгоритм демонстрирует экспоненциальное ускорение по сравнению с классическими алгоритмами.

1. Арифметические операции над большими числами.

Арифметические операции над большими числами - это операции сложения, вычитания, умножения и деления, выполняемые над числами, которые превышают размерность стандартных целых чисел в языках программирования. Когда работают с большими числами, не помещающимися в стандартные типы данных, требуется использовать специальные алгоритмы и структуры данных для выполнения арифметических операций.

Некоторые из таких методов включают:   
 - Большие числа в виде строк;   
 - Методы длинной арифметики: Длинная арифметика - это техника, при которой числа представлены в специальных структурах данных, таких как массивы или списки, где каждый элемент представляет одну цифру числа.

1. Эллиптические кривые и их приложения в криптографии.

*Эллиптические кривые* - геометрические объекты, используемые в криптографии. Они обладают сложными математическими свойствами и применяются для построения криптографических протоколов. Эллиптические кривые находят применение в эллиптическом криптографическом шифровании (ECIES), эллиптических цифровых подписях (ECDSA) и эллиптических криптосистемах общего секрета (ECDH). Они обеспечивают высокую безопасность и эффективность при работе с криптографическими операциями.

1. Классификация основных методов криптографической защиты. Методы симметричного шифрования.

Криптографическая защита данных основывается на использовании различных методов и алгоритмов. Они могут быть классифицированы на основе различных критериев, таких как тип ключей, использование одного или нескольких ключей, и симметричные или асимметричные алгоритмы. Один из основных способов классификации - это разделение на методы симметричного шифрования и асимметричного шифрования. Давайте рассмотрим методы симметричного шифрования.  
*Методы симметричного шифрования:*   
 Шифр замены:

Это один из самых простых методов симметричного шифрования. Он основан на замене каждого символа входного текста на соответствующий символ из заранее определенной таблицы замены (например, шифр Цезаря). Таблица замены может быть представлена в виде алфавита, числовых значений или других символов.

Шифр перестановки:

Этот метод основан на перестановке символов во входном тексте с использованием заданного правила или ключа. Каждый символ перемещается на новую позицию в шифрованном тексте согласно определенным правилам. Шифр перестановки может быть одноступенчатым или многоступенчатым (например, шифр Шиффера).

Блочные шифры:

Блочные шифры оперируют над блоками данных фиксированного размера и применяют определенные преобразования к каждому блоку. Примером блочного шифра является шифр DES (Data Encryption Standard) или AES (Advanced Encryption Standard).

Поточные шифры:

Поточные шифры преобразуют данные побитово или по-байтово, используя генератор псевдослучайных чисел (PRNG). Они применяются к каждому биту или байту входного текста с использованием ключа и псевдослучайной последовательности. Примером поточного шифра является шифр RC4.

Методы симметричного шифрования обеспечивают высокую скорость шифрования и дешифрования, а также эффективное использование ресурсов. Однако они требуют, чтобы отправитель и получатель имели доступ к общему секретному ключу. Это делает методы симметричного шифрования подходящими для шифрования больших объемов данных и выполнения быстрых операций шифрования в реальном времени.

1. Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр.

*Шифры замены* - это методы шифрования, которые заменяют символы или группы символов в открытом тексте на другие символы или группы символов в зашифрованном тексте.   
*Простая замена:* Этот тип шифра заменяет каждую букву или символ в открытом тексте на другую букву или символ в зашифрованном тексте. Простая замена может быть реализована с использованием шифровальной таблицы, где каждой букве или символу соответствует другая буква или символ. Примером такого шифра является шифр Цезаря, где каждая буква сдвигается на определенное количество позиций в алфавите.   
*Многоалфавитная подстановка*: В этом типе шифра замены используется несколько алфавитов для замены символов. Например, шифр Виженера использует ключевую фразу для определения последовательности алфавитов, которые используются для замены символов. Каждая буква открытого текста заменяется буквой из соответствующего алфавита.   
*Пропорциональный шифр*: Этот тип шифра замены основан на частотах символов в языке. Чаще всего встречающиеся символы заменяются на более редкие символы, что усложняет анализ частотности и расшифровку текста. Примером такого шифра является шифр Атбаш, где каждая буква заменяется на букву, стоящую в обратном порядке в алфавите.   
Все эти методы шифрования замены представляют собой простые исторические техники, которые могут быть легко разгаданы с использованием методов криптоанализа. Они не рекомендуются для использования в современных системах шифрования, где применяются более сложные и надежные алгоритмы.

1. Методы перестановки. Табличная перестановка, маршрутная перестановка. Гаммирование. Гаммирование с конечной и бесконечной гаммами.

Методы перестановки - это методы шифрования, которые изменяют порядок символов или блоков символов в открытом тексте для создания зашифрованного текста. Вот некоторые примеры методов перестановки:

Табличная перестановка: В этом методе символы открытого текста переупорядочиваются в соответствии с определенной таблицей или матрицей. Каждый символ занимает новую позицию в таблице или матрице, а затем зашифрованный текст читается в порядке, заданном новыми позициями. Примером такого метода является шифр "квадрат Полибия".   
Маршрутная перестановка: Этот метод переставляет символы открытого текста в определенном порядке в соответствии с заданным алгоритмом перестановки. Одним из известных методов маршрутной перестановки является шифр "маршрутной транспозиции", где символы открытого текста записываются в матрицу по строкам или столбцам, а затем зашифрованный текст читается по определенному пути. Гаммирование: Гаммирование - это метод комбинирования открытого текста с гаммой, которая представляет собой случайную или псевдослучайную последовательность символов. Гамма складывается с открытым текстом по модулю алфавита, что приводит к получению зашифрованного текста. Для расшифровки используется та же гамма. Гаммирование может быть реализовано с использованием конечной гаммы (гамма фиксированной длины) или бесконечной гаммы (гамма, которая повторяется циклически).

Методы перестановки обеспечивают дополнительную степень защиты и усложняют криптоанализ, так как они изменяют структуру открытого текста. Однако они могут быть уязвимы к другим методам атак, таким как частотный анализ. Поэтому в современных системах шифрования часто используются комбинированные методы, которые объединяют как методы перестановки, так и методы замены для обеспечения более высокого уровня безопасности.

1. Основные методы криптоанализа. Криптографические атаки.

*Основные методы криптоанализа* - это техники и алгоритмы, которые используются для расшифровки зашифрованной информации без знания ключа или для нарушения безопасности криптографической системы. Вот некоторые основные методы криптоанализа:   
 1) Частотный анализ: Этот метод основан на анализе частоты появления символов или символьных групп в зашифрованном тексте. Используя статистическую информацию о частотах символов в языке, криптоаналитик может определить соответствия между зашифрованными символами и символами в открытом тексте, что помогает расшифровать сообщение.   
2) Атаки по известному открытому тексту: В этом методе криптоаналитик имеет доступ к некоторым парам зашифрованного текста и соответствующего открытого текста. Используя эти данные, можно попытаться определить закономерности и уязвимости в шифровании, что помогает взломать остальные части зашифрованного сообщения.  
 3) Атаки по выбранному открытому тексту: Здесь криптоаналитик может выбирать определенные открытые тексты и наблюдать соответствующие зашифрованные тексты. Поэтому атакующий может использовать полученные данные для изучения связей между открытыми и зашифрованными текстами и выявления уязвимостей в системе шифрования.   
 4) Словарные атаки: В этом методе используется словарь с предполагаемыми ключами или открытыми текстами для попыток расшифровки зашифрованного сообщения. Криптоаналитик перебирает возможные ключи или открытые тексты и сравнивает их с зашифрованным текстом, чтобы найти соответствие.   
 5) Линейное и дифференциальное криптоанализы: Это сложные методы криптоанализа, основанные на математических моделях и статистических анализах шифров. Они позволяют выявить слабые места в алгоритмах шифрования и использовать их для расшифровки сообщений.

*Криптографические атаки* - это попытки взлома или нарушения безопасности криптографических систем и алгоритмов с целью получения доступа к защищенной информации или нарушения ее конфиденциальности, целостности или аутентичности.

1. Криптогафическая стойкость. Абсолютно стойкие криптосистемы**.** Принципы Киркхоффса. Перспективные направления криптоанализа, квантовый криптоанализ

*Криптографическая стойкость* - способность криптографического алгоритма противостоять криптоанализу. Стойким считается алгоритм, который для успешной атаки требует от противника недостижимых вычислительных ресурсов, недостижимого объёма перехваченных открытых и зашифрованных сообщений или же такого времени раскрытия, что по его истечении защищенная информация будет уже не актуальна, и т. д. В большинстве случаев криптостойкость нельзя математически доказать, можно только доказать уязвимости криптографического алгоритма.

*Принципы Киркхоффса* - это принципы, сформулированные французским математиком Аугустом Киркхоффсом в 19 веке, которые считаются основами современной криптографии. Согласно этим принципам, стойкость криптосистемы должна основываться на секретности ключа, а не на секретности алгоритма. Это означает, что алгоритмы должны быть известны всем, но без знания ключа невозможно восстановить оригинальные данные.

*При перспективных направлениях* криптоанализа исследуются новые методы и алгоритмы для взлома криптографических систем, а также улучшение существующих методов. Криптоанализ может быть симметричным, когда исследуется возможность восстановления оригинальных данных без знания ключа, или асимметричным, когда исследуется возможность восстановления закрытого ключа.

*Квантовый криптоанализ* - это направление криптоанализа, основанное на использовании принципов квантовой физики. Квантовые компьютеры, обладающие особенностями, такими как суперпозиция и квантовая запутанность, могут быть использованы для разработки алгоритмов, способных обойти существующие криптографические защиты, такие как RSA или Эль-Гамаля.  
  
*Абсолютно стойкие криптосистемы*  
Шифр Вернама. Система симметричного шифрования, изобретённая в 1917 году Гилбертом Вернамом. Шифр является разновидностью криптосистемы одноразовых блокнотов. В нём используется булева функция «исключающее или». Шифр Вернама является примером системы с абсолютной криптографической стойкостью.

1. Поточные шифры и генераторы псевдослучайных чисел.

*Поточные шифры* - это криптографические алгоритмы, которые шифруют данные побитово или побайтово, используя поток псевдослучайных чисел. Они отличаются от блочных шифров, которые шифруют данные блоками фиксированного размера.

*Генераторы псевдослучайных чисел (ГПСЧ)* - это алгоритмы, которые генерируют последовательность чисел, которая, на первый взгляд, выглядит случайной. Они используют начальное значение, называемое семенем, и генерируют последующие числа на основе этого семени. ГПСЧ не генерируют идеально случайные числа, а только числа, которые статистически похожи на случайные.

Поточные шифры используют генераторы псевдослучайных чисел для генерации потока ключевой информации. Входные данные шифруются, или скремблируются, с использованием битов потока ключей. После шифрования, данные могут быть отправлены по каналу связи или сохранены в зашифрованном виде.

Один из наиболее известных поточных шифров - это шифр RC4

1. Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии. Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.

*Основные принципы поточного шифрования* заключаются в использовании генераторов псевдослучайных чисел (ПСЧ) для создания потока случайных битов, которые затем комбинируются с открытым текстом для получения зашифрованного сообщения.

*Генераторы псевдослучайных чисел (ПСЧ) используются в криптографии* для создания псевдослучайных последовательностей, которые могут быть использованы для шифрования данных или создания криптографических ключей.

*Основные методы получения псевдослучайных последовательностей включают:*

*1. Линейный конгруэнтный генератор (ЛКГ)* - это один из простейших алгоритмов генерации псевдослучайных чисел. Он использует линейное рекуррентное соотношение для генерации последовательности чисел. Однако, ЛКГ имеет некоторые ограничения и может быть предсказуемым, если его параметры не выбраны правильно.

*2. Метод Фибоначчи* - этот метод основан на рекуррентном соотношении Фибоначчи, где новое число в последовательности вычисляется путем сложения двух предыдущих чисел. Метод Фибоначчи может быть использован для генерации псевдослучайных последовательностей, хотя его периодические свойства могут иметь некоторые ограничения в криптографических приложениях.

*3. Метод Блюма-Блюма-Шуба (BBS)* - это криптографический алгоритм генерации псевдослучайных последовательностей, основанный на вычислениях в кольце вычетов. Он использует большие простые числа и операции в кольце для генерации последовательности битов. BBS считается криптографически безопасным при выполнении некоторых условий.

1. Кодирование информации. Компьютеризация шифрования. Символьное кодирование. Смысловое кодирование.

*Кодирование информации* - это процесс представления информации в виде определенного кода или символов. Оно позволяет представить данные в удобной и компактной форме для передачи, хранения и обработки.

*Компьютеризация шифрования*, как уже упоминалось ранее, относится к использованию компьютерных технологий и алгоритмов для защиты информации путем шифрования и дешифрования. Это позволяет обеспечить конфиденциальность и целостность данных при передаче и хранении.

*Символьное кодирование* - это процесс представления символов и символьных последовательностей в виде числовых значений или кодов. Например, таблица ASCII, которую уже упоминали, представляет символы алфавита и другие символы в виде соответствующих числовых значений.

*Смысловое кодирование* - это использование кодов или символов для представления смысловой информации или семантики. Он стремится не только представить данные, но и сохранить их смысл или контекст. Примером смыслового кодирования может быть использование меток или тегов для классификации и обозначения определенных аспектов информации.

1. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII.

*Механизация шифрования* относится к автоматизации процесса шифрования данных с использованием специальных машин или устройств. Это предполагает использование механических, электромеханических или электронных устройств для выполнения операций шифрования и дешифрования.

Механизация шифрования позволяет ускорить процесс шифрования и обеспечить масштабируемость, что делает его более эффективным для обработки больших объемов данных.

*Представление информации в двоичном коде* является основой для механизации шифрования и компьютерных операций в целом. Двоичный код использует две цифры - 0 и 1 - для представления информации и выполнения логических операций. Каждая цифра в двоичном коде называется битом (от англ. binary digit).

В двоичной системе каждый символ или символьное значение может быть представлено с использованием соответствующего набора битов. Например, для представления чисел от 0 до 9 обычно достаточно 4 битов. Один байт состоит из 8 битов и может представлять широкий спектр символов и значений.

*Таблица ASCII* (от англ. American Standard Code for Information Interchange) представляет собой стандартное кодирование для представления символов на компьютере. Она определяет соответствие между каждым символом и его числовым представлением в двоичном коде, используя один байт (8 бит).

Таблица ASCII включает в себя основные символы, цифры, специальные символы и управляющие символы. Например, символ "A" представлен в ASCII коде как 65, а символ "a" - как 97.

Таблица ASCII является основой для многих других кодировок символов, таких как Unicode, которая позволяет представить символы разных языков и культур. Она также играет важную роль в процессе шифрования и дешифрования данных, где каждый символ может быть представлен своим числовым значением в соответствующей кодировке.

1. Компьютеризация шифрования. Аппаратное и программное шифрование.

*Компьютеризация шифрования* относится к использованию компьютерных технологий и алгоритмов для защиты информации. Она предоставляет средства и методы для шифрования данных, что позволяет обеспечить их конфиденциальность, целостность и доступность.

В компьютеризации шифрования можно выделить два основных подхода: аппаратное и программное шифрование.

*Аппаратное шифрование* основано на использовании специализированного аппаратного обеспечения, такого как криптографические процессоры или аппаратные модули безопасности. Они выполняют операции шифрования и дешифрования с использованием аппаратных ресурсов, что делает их более эффективными и быстрыми по сравнению с программным шифрованием. Аппаратные средства также могут обладать дополнительными физическими механизмами защиты, такими как защита от физического доступа или защита от аппаратных атак.

*Программное шифрование*, с другой стороны, основано на использовании программных алгоритмов и кодирования для шифрования информации. Это может быть реализовано с использованием криптографических библиотек и программ, которые выполняют операции шифрования и дешифрования на уровне операционной системы или приложений.

Оба подхода имеют свои преимущества и недостатки. Аппаратное шифрование обычно является более быстрым и эффективным, но может быть дороже в реализации. Программное шифрование, с другой стороны, является более гибким и доступным, но может требовать больше вычислительных ресурсов и иметь некоторые ограничения по производительности.

1. Стандартизация программно-аппаратных криптографических систем и средств. Изучение современных программных и аппаратных криптографических средств.

*Стандартизация программно-аппаратных криптографических систем и средств* - это процесс разработки и утверждения стандартов для использования в криптографической защите информации. Стандарты устанавливают общепринятые протоколы, алгоритмы, аппаратные и программные компоненты, которые должны использоваться в системах безопасности для обеспечения конфиденциальности, целостности и аутентичности данных.

Современные программные и аппаратные криптографические средства включают в себя широкий спектр технологий и продуктов, разработанных для обеспечения защиты данных. Это включает в себя криптографические алгоритмы, такие как AES (Advanced Encryption Standard) и RSA (Rivest-Shamir-Adleman), программы для шифрования и дешифрования данных, аппаратные средства для обеспечения безопасности, такие как криптопроцессоры и модули аппаратного шифрования, а также платформы и системы для управления ключами и аутентификации.

*Изучение современных программных и аппаратных криптографических средств* включает в себя понимание основных принципов криптографии, алгоритмов и протоколов, а также умение выбирать и применять правильные средства и методы в зависимости от конкретных потребностей безопасности. Это также требует знания о текущих стандартах и спецификациях, понимания уязвимостей и методов криптоанализа, а также способности проводить тестирование и оценку криптографической стойкости систем и средств.

1. Симметричные системы шифрования. Основные сведения. Структурная схема симметричных криптографических систем.

*Симметричные системы шифрования* - это системы, в которых для шифрования и расшифровки используется один и тот же секретный ключ. Они основываются на преобразовании исходного текста (plaintext) в шифрованный текст (ciphertext) и наоборот с использованием определенного алгоритма и секретного ключа.

*Основные сведения о симметричных системах шифрования:*

1. Секретный ключ: В симметричных системах для шифрования и расшифровки используется один и тот же секретный ключ, который должен быть известен только отправителю и получателю.

2. Алгоритм шифрования: Симметричные алгоритмы определяют правила и методы шифрования, которые применяются для преобразования исходного текста в шифрованный.

3. Режимы шифрования: Симметричные системы поддерживают различные режимы шифрования, которые определяют способ применения алгоритма шифрования к сообщению.

*Структурная схема симметричной криптографической системы может быть представлена следующим образом:*

1. Генерация ключа: Отправитель и получатель должны сгенерировать и согласовать общий секретный ключ перед началом обмена сообщениями.

2. Шифрование: Отправитель использует секретный ключ и алгоритм шифрования для преобразования исходного текста в шифрованный текст.

3. Передача шифрованного сообщения: Шифрованный текст отправляется получателю по каналу связи.

4. Расшифровка: Получатель использует тот же секретный ключ и алгоритм расшифровки для восстановления исходного текста из полученного шифрованного текста.

Симметричные системы шифрования широко применяются для защиты данных, таких как конфиденциальные сообщения и файлы. Они обеспечивают высокую скорость шифрования и расшифровки, но требуют безопасного распределения секретных ключей между отправителем и получателем.

1. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4.

Симметричные алгоритмы шифрования используют один и тот же ключ для шифрования и дешифрования данных. Вот краткое описание некоторых известных симметричных алгоритмов:   
 1) DES (Data Encryption Standard): DES был разработан в 1970-х годах и является одним из наиболее широко использовавшихся симметричных алгоритмов. Он использует 56-битный ключ и блочную структуру с размером блока 64 бита. Однако в настоящее время DES считается устаревшим, так как его ключевая длина слишком коротка, и существуют методы криптоанализа, которые позволяют взламывать его.   
 2) AES (Advanced Encryption Standard): AES является наиболее распространенным и рекомендуемым стандартом симметричного шифрования. Он был выбран как замена DES и предоставляет более высокий уровень безопасности. AES поддерживает ключи различной длины (128, 192 или 256 бит) и использует блочную структуру с размером блока 128 бит. Он считается надежным и безопасным алгоритмом шифрования.   
 3) ГОСТ 28147-89: ГОСТ 28147-89 является российским стандартом симметричного шифрования, который был разработан в СССР. Он использует блочную структуру с размером блока 64 бита и поддерживает ключи длиной 256 бит. ГОСТ 28147-89 также включает в себя режимы работы, такие как режим простой замены и режим гаммирования. Однако он не так широко используется за пределами России, как DES и AES.   
 4) RC4: RC4 - это потоковый шифр, который был разработан Роном Ривестом в 1987 году. Он использует переменный ключ (обычно от 40 до 2048 бит) и генерирует псевдослучайный поток байтов, который применяется побитово к открытому тексту для шифрования. RC4 был широко использован в протоколах безопасности, таких как WEP в беспроводных сетях, но имеет известные уязвимости и считается устаревшим алгоритмом.

1. Отечественные алгоритмы «Магма» и «Кузнечик».

«Магма» и «Кузнечик» - это симметричные алгоритмы шифрования, разработанные в России и принятые в качестве стандартов для защиты информации.

*Алгоритм шифрования «Магма»* был разработан в России в 1990-х годах. Он используется для шифрования информации в различных сферах, включая государственные и коммерческие системы. Магма использует блочную структуру с размером блока 64 бита и 256-битный ключ. Он также поддерживает различные режимы работы, такие как режим простой замены и режим гаммирования.

*Алгоритм шифрования «Кузнечик»* был разработан в России в 2015 году как замена алгоритма «Магма». Он является усовершенствованной версией «Магмы» и предлагает более высокий уровень безопасности. Кузнечик также использует блочную структуру с размером блока 128 бит и 256-битный ключ. Он поддерживает различные режимы работы, включая режим простой замены, режим гаммирования и режимы аутентификации.

И «Магма», и «Кузнечик» являются государственными стандартами России для шифрования информации. Они обеспечивают защиту данных и используются в различных областях, включая государственные организации и коммерческие предприятия. Важно отметить, что оба алгоритма прошли широкое тестирование и анализ, и их безопасность подтверждена независимыми экспертами.

1. Криптографический алгоритм IDEA.

*IDEA (International Data Encryption Algorithm)* - это симметричный блочный шифр, разработанный в 1991 году Xuejia Lai и James L. Massey. Он широко использовался в различных коммерческих приложениях и стандартах, таких как PGP (Pretty Good Privacy).

IDEA использует 64-битный блок данных и ключ длиной 128 бит. *Он основан на более раннем шифре "PES" (Proposed Encryption Standard), который в свою очередь основан на шифре "HPC" (Hermes Product Code), разработанном Lai и Massey в 1987 году*.

Алгоритм IDEA использует ключевое расписание ключа для создания раундовых ключей, которые применяются на каждом раунде шифрования.

IDEA позиционировался как алгоритм с высоким уровнем безопасности и надежности, однако его использование стала угасать со временем. Это связано с развитием более современных и безопасных алгоритмов шифрования, которые имеют более высокие скорости и лучшую устойчивость к атакам. Тем не менее, IDEA продемонстрировал свою надежность и был популярным шифром на протяжении многих лет.

1. Асимметричные системы шифрования. Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.

*Асимметричные системы шифрования*, также известные как криптосистемы с открытым ключом, используют два ключа: открытый и закрытый. Отправитель шифрует сообщение с использованием открытого ключа получателя, а получатель дешифрует его с помощью своего закрытого ключа. Эти системы обеспечивают безопасный обмен ключами и поддерживают функции цифровых подписей для подтверждения подлинности данных. Примеры асимметричных алгоритмов включают RSA, DSA, ElGamal и ECC.*Криптосистемы с открытым ключом,* или асимметричные криптосистемы, используют пару ключей для шифрования и дешифрования данных. Одним из ключей является открытый ключ, который может быть распространен свободно, а другим ключом является закрытый ключ, который остается в секрете у владельца.   
Открытый ключ используется для шифрования сообщений, а закрытый ключ — для их дешифрования. Криптосистемы с открытым ключом также поддерживают цифровые подписи для подтверждения подлинности данных. Они обеспечивают безопасный обмен ключами и обеспечивают целостность данных. Криптосистемы с открытым ключом позволяют безопасно обмениваться ключами между сторонами без необходимости передачи секретных ключей по открытым каналам связи. Цифровые подписи: Криптосистемы с открытым ключом поддерживают создание и проверку цифровых подписей, что обеспечивает подлинность и целостность данных.

*Необратимость системы* в криптографии означает, что невозможно восстановить исходное сообщение или ключ из его зашифрованного представления без знания специальной информации, такой как секретный ключ или другие параметры системы. Является важным свойством в криптографии, так как обеспечивает защиту данных и ключей от несанкционированного доступа и восстановления.

*Структурная схема шифрования с открытым ключом* включает генерацию ключей, шифрование сообщения с использованием открытого ключа отправителя, передачу зашифрованного сообщения и дешифрование полученного сообщения с помощью закрытого ключа получателя.

1. Элементы теории чисел в криптографии с открытым ключом. Применение теории чисел в криптографии с открытым ключом.

Теория чисел является важным элементом криптографии с открытым ключом. Она обеспечивает надежную защиту информации путем использования алгоритмов и методов, основанных на математических свойствах чисел.

Применение теории чисел в криптографии с открытым ключом позволяет обеспечить высокую стойкость к атакам и обеспечить безопасность передачи данных. Однако, с развитием вычислительных мощностей некоторые алгоритмы могут стать уязвимыми, поэтому важно постоянное исследование новых методов и алгоритмов для обеспечения безопасности.

1. Аутентификация данных. Общие понятия**.** Электронная подпись, МАС – message of authentication code.

*Аутентификация данных (data authentication)* – это процесс проверки подлинности данных для обеспечения их целостности и источника. Она обеспечивает уверенность в том, что переданные или хранимые данные не были изменены в процессе передачи или хранения, и что они действительно были созданы определенным источником.

*Электронная подпись (digital signature)* - это криптографическая конструкция, которая представляет собой зашифрованный хеш-код данных с использованием приватного ключа отправителя. Это позволяет получателю проверить подлинность данных, идентифицировать отправителя и убедиться, что данные не были изменены после подписания.

*Message Authentication Code (MAC)* - код аутентификации сообщения - это криптографический хеш-код, создаваемый с использованием секретного ключа (симметричного) и применяемый к сообщению для обеспечения аутентификации и целостности данных. MAC обычно используется в симметричной криптографии для проверки целостности и аутентичности сообщений.

Как электронная подпись, так и MAC обеспечивают проверку целостности данных и подтверждают авторство или источник данных. Однако электронная подпись является асимметричным механизмом, использующим два разных ключа (приватный и публичный), в то время как MAC является симметричным механизмом, использующим один секретный ключ.

1. Однонаправленные хеш-функции. Алгоритмы цифровой подписи.

*Однонаправленные хеш-функции* (или просто хеш-функции) - это криптографические алгоритмы, которые принимают на вход произвольные данные и преобразуют их в фиксированный хеш-код определенной длины. Отличительной чертой таких функций является то, что хеш-код нельзя обратить обратно и получить исходные данные. Хеш-функции широко используются для обеспечения целостности данных, аутентификации и защиты от подделки.

Некоторые из наиболее распространенных алгоритмов хеширования включают:

1. MD5 (Message Digest 5)

2. SHA (Secure Hash Algorithm) семейство: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512. Эти алгоритмы являются более безопасными и устойчивыми к коллизиям.

*Алгоритмы цифровой подписи (Digital Signature Algorithms)* - это криптографические алгоритмы, используемые для создания и проверки электронных цифровых подписей. Цифровая подпись представляет собой криптографическую конструкцию, которая позволяет устанавливать аутентичность, целостность и невозможность отказа от подписи данных.

Некоторые из наиболее распространенных алгоритмов цифровой подписи включают:

1. RSA (Rivest-Shamir-Adleman): асимметричный алгоритм, который использует пару ключей - приватный ключ для создания подписи и публичный ключ для проверки подписи.

2. DSA (Digital Signature Algorithm): алгоритм, который выполняет подпись и проверку подписи с использованием публичного и приватного ключей.

Цифровые подписи являются обеспечивают аутентификацию и целостность данных, а также предотвращают отказ от подписи.

1. Алгоритмы распределения ключей с применением симметричных и асимметричных схем.

*Алгоритмы распределения ключей* являются криптографическими механизмами, используемыми для обмена ключами между двумя или более участниками коммуникации. Эти ключи используются для обеспечения конфиденциальности, целостности и аутентификации данных. В симметричных схемах используется один и тот же секретный ключ как для шифрования, так и для расшифровки данных.

В асимметричных схемах используется пара ключей: публичный ключ для шифрования и приватный ключ для расшифровки данных.

1. Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация.

*Протоколы аутентификации* - это механизмы или процедуры, используемые для проверки подлинности участников коммуникации в компьютерных сетях или системах. Вот два основных вида протоколов аутентификации, взаимная аутентификация и односторонняя аутентификация:

*1. Взаимная аутентификация (Mutual Authentication):*

Взаимная аутентификация - это процесс, при котором как клиент, так и сервер проверяют друг друга и подтверждают свою подлинность. Другими словами, обе стороны доказывают, что они являются доверенными участниками коммуникации. Протоколы, такие как EAP-TLS (Extensible Authentication Protocol - Transport Layer Security), SSL/TLS и IPSec (Internet Protocol Security), обеспечивают механизмы взаимной аутентификации.

*2. Односторонняя аутентификация (One-Way Authentication):*

Односторонняя аутентификация - это процесс, при котором одна сторона, обычно клиент, проверяет подлинность другой стороны, например, сервера или устройства. То есть только одна сторона прикладывает усилия для доказательства своей подлинности. Примеры протоколов односторонней аутентификации включают протоколы SSL/TLS (где сервер предоставляет свой сертификат клиенту) и SSH (Secure Shell), где сервер предоставляет свою публичную часть своего ключа клиенту для проверки.

1. Криптозащита информации в сетях передачи данных. Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей.

Криптозащита информации в сетях передачи данных - это обеспечение безопасности информации, передаваемой в компьютерных сетях. Она включает в себя различные техники и меры для защиты данных от несанкционированного доступа, перехвата и модификации.

1. Абонентское шифрование: Это метод шифрования, при котором каждый абонент или пользователь сети использует собственный ключ и алгоритм шифрования для защиты своих данных. Каждый абонент обменивается публичными ключами с другим участником передачи данных и использует их для шифрования и расшифровки информации. Примером абонентского шифрования является асимметричное шифрование, основанное на паре ключей - публичном и приватном.

2. Пакетное шифрование: Это метод шифрования, при котором каждый пакет данных, передаваемый через сеть, шифруется отдельно.

3. Защита центра генерации ключей: Центр генерации ключей (Key Management Center) - это система или организация, ответственная за генерацию и распределение ключей для шифрования и дешифровки данных. Защита центра генерации ключей включает в себя физическую и логическую защиту серверов и инфраструктуры центра, а также механизмы контроля доступа и аутентификации для предотвращения несанкционированного доступа к ключам.

Центр генерации ключей также отвечает за обновление и управление ключами, включая генерацию новых ключей, отзыв или обновление старых ключей, и распределение ключей между абонентами сети передачи данных.

Все эти меры обеспечивают защиту информации в сетях передачи данных, сохраняя ее конфиденциальность, целостность и доступность. Они помогают предотвратить несанкционированный доступ и защищают данные от вредоносных атак и утечек информации.

1. Криптомаршрутизатор. Пакетный фильтр.

Криптомаршрутизатор - это сетевое устройство, которое сочетает функции маршрутизатора и криптографического аппарата для обеспечения защиты данных при их передаче через сеть.

Основная функция криптомаршрутизатора - обеспечение безопасной передачи данных между сетями или хостами. Он использует различные шифровальные протоколы и алгоритмы для защиты данных от несанкционированного доступа и перехвата. Криптомаршрутизаторы также могут предоставлять возможности аутентификации и интеграции с другими системами защиты, такими как виртуальные частные сети (VPN) и брандмауэры.

Пакетный фильтр - это технология, используемая в сетевых устройствах (например, маршрутизаторах или брандмауэрах), чтобы контролировать трафик, проходящий через сеть на основе определенных правил и критериев.

Пакетный фильтр может выполнять различные действия с сетевыми пакетами, такие как блокировка или разрешение их прохождения через сетевое устройство, в зависимости от заданных правил. Эти правила могут основываться на исходном или конечном адресе IP, портах, протоколах, или других характеристиках сетевых пакетов.

Пакетные фильтры помогают защитить сеть от различных сетевых атак, предоставляют контроль и управление над трафиком и обеспечивают возможность реализации политик безопасности в сети.

1. Криптографическая защита беспроводных соединений.

Стандарт IEEE-802.11 определяет протоколы и стандарты для беспроводных сетей (Wi-Fi). Два основных криптопротокола, используемых в сетях IEEE-802.11, это WPA (Wi-Fi Protected Access) и WEP (Wired Equivalent Privacy), хотя WEP на сегодняшний день считается устаревшим и небезопасным.

1. Использованием криптопротоколов WPA, WEP в сетях стандарта IEEE-802.11

Стандарт IEEE-802.11 определяет протоколы и стандарты для беспроводных сетей (Wi-Fi). Два основных криптопротокола, используемых в сетях IEEE-802.11, это WPA (Wi-Fi Protected Access) и WEP (Wired Equivalent Privacy), хотя WEP на сегодняшний день считается устаревшим и небезопасным.

1. WEP (Wired Equivalent Privacy): Это первый протокол безопасности, который использовался для защиты беспроводных сетей Wi-Fi. WEP использует алгоритм RC4 для шифрования данных. Однако, WEP был обнаружен уязвим к расшифровке, и его можно взломать относительно легко, особенно при использовании низкой длины ключей. В настоящее время не рекомендуется использовать WEP для защиты беспроводных сетей.

2. WPA (Wi-Fi Protected Access): В ответ на уязвимости WEP был разработан протокол WPA. WPA использует различные методы шифрования, включая TKIP (Temporal Key Integrity Protocol), а также улучшенный протокол аутентификации - EAP (Extensible Authentication Protocol). WPA улучшил безопасность Wi-Fi и стал более устойчив к атакам по сравнению с WEP. Однако, с течением времени WPA также стал уязвим к атакам, особенно при использовании простых или слабых паролей.

3. WPA2: Это следующая версия протокола WPA, которая считается наиболее безопасной и наиболее рекомендуемой для защиты Wi-Fi сетей сегодня. WPA2 использует более сильные алгоритмы шифрования - AES (Advanced Encryption Standard) - и выполняет аутентификацию посредством EAP. WPA2 может использоваться с предварительным распределением ключей (WPA2-Personal) или с использованием сервера аутентификации (WPA2-Enterprise).

В целом, использование протоколов WPA и WPA2 в сетях стандарта IEEE-802.11 является рекомендуемым для обеспечения безопасности Wi-Fi сетей. Они обеспечивают шифрование и аутентификацию данных, а также защиту от несанкционированного доступа. WEP не рекомендуется использовать, так как он считается устаревшим и небезопасным.

1. Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер.

*Принципы функционирования электронных платежных систем:*

1. Регистрация аккаунта: Пользователь регистрируется в системе, создает аккаунт и связывает его с банковской картой или электронным кошельком.

2. Аутентификация: При каждой попытке оплаты происходит аутентификация пользователя, чтобы подтвердить его личность.

3. Авторизация: После успешной аутентификации система проверяет, достаточно ли у пользователя средств на счету для совершения платежа.

4. Платеж: Если пользователь прошел успешную авторизацию и имеет достаточное количество средств, система производит платеж на указанный аккаунт или карту.

5. Подтверждение: После совершения платежа пользователю предоставляется подтверждение операции, например, электронный чек или уведомление на почту.

*Электронные пластиковые карты:*

Электронная пластиковая карта представляет собой носитель информации о банковском счете пользователя. Она может быть выпущена банком или платежной системой и содержит уникальный номер, срок действия и другую информацию. Она имеет магнитную полосу или чип, которые позволяют считывать данные карты при оплате в магазинах и снятии наличных в банкоматах.

*Персональный идентификационный номер (ПИН):*

Персональный идентификационный номер – это числовой код, используемый для аутентификации пользователя при совершении платежей с использованием электронных пластиковых карт. ПИН является конфиденциальным и должен быть известен только владельцу карты.

1. Применение криптографических протоколов для обеспечения безопасности электронной коммерции.

*Криптографические протоколы играют важную роль* в обеспечении безопасности электронной коммерции. Они используются для защиты конфиденциальности, целостности и аутентификации данных, а также для обеспечения безопасности взаимодействия между участниками системы.

Ниже приведены некоторые примеры применения криптографических протоколов в электронной коммерции:

1. SSL/TLS протоколы используются для защищенной передачи данных по сети. Они обеспечивают шифрование данных между клиентом и сервером, защищая информацию от несанкционированного доступа и подмены.

2. Протоколы асимметричного шифрования. Например, протоколы RSA или ECC (эллиптическая кривая шифрования) используются для обмена ключами и зашифрованного обмена данными.

3. Хеширование: Хеширование применяется для проверки целостности данных.

4. Электронная подпись: Электронная подпись используется для аутентификации и целостности данных. Она создается с использованием приватного ключа и проверяется с помощью соответствующего публичного ключа.

5. Протоколы аутентификации: Протоколы аутентификации, такие как протоколы Керберос и OAuth, используются для проверки идентичности пользователей и предоставления доступа к защищенным ресурсам только авторизованным лицам.

Они помогают защитить данные клиентов, обеспечивая конфиденциальность, целостность и аутентификацию во время передачи информации в онлайн-среде.

1. Компьютерная стеганография. Скрытая передача информации в компьютерных системах.

*Компьютерная стеганография* - это метод скрытой передачи информации в компьютерных системах. Она отличается от криптографии, которая направлена на обеспечение конфиденциальности информации, тем, что стеганография стремится сохранить сам факт наличия передачи информации с использованием методов, которые делают ее незаметной для посторонних.

Процесс включает в себя внедрение скрытых данных в носитель информации, такой как изображения, звуковые файлы или видео. Скрытые данные зашифровываются и затем внедряются в выбранный носитель с использованием различных методов, таких как замена младших битов или изменение структуры файлов.

Компьютерная стеганография имеет множество применений, включая:

1. Конфиденциальная передача сообщений.

2. Защита авторских прав.

3. Борьба с киберпреступностью.

4. Военное применение.   
*Скрытая передача информации в компьютерных системах* - это процесс передачи данных, который делает их незаметными для наблюдателей или несанкционированных пользователей.

Важно отметить, что использование скрытой передачи информации может подпадать под законы о кибербезопасности и незаконное использование данных. Поэтому перед применением этих методов необходимо обязательно соблюдать законодательство и убедиться, что использование скрытой передачи соответствует установленным правилам и требованиям.

1. Проблема аутентификации мультимедийной информации. Защита авторских прав.

*Проблема аутентификации мультимедийной информации* относится к проверке подлинности и целостности данных (например, изображений, видео или аудио). В связи с легкостью создания и изменения мультимедийных файлов, возникает необходимость обеспечения доверия к их источнику и подтверждения, что они не были изменены или подделаны.

Проблема аутентификации мультимедийной информации возникает из-за возможности подделки и изменения содержимого цифровых медиафайлов, таких как изображения, видео и аудиофайлы. Это может создать проблемы с подлинностью и достоверностью такой информации.

*Защита авторских прав в мультимедийных данных* может быть обеспечена аутентификацией и цифровой подписью, чтобы подтвердить источник и целостность авторских материалов. Водяные знаки могут быть использованы для визуальной идентификации владельца авторских прав и предупреждения о нарушении прав. Кроме того, существуют специальные правовые меры и организации, такие как Creative Commons, которые помогают защищать и регулировать авторские права в сфере мультимедиа.

1. Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ.

*Методы компьютерной стеганографии:*

1. Замены битов: Метод основан на замене младших битов пикселей в изображении или звуковых сэмплов в аудио для внедрения скрытой информации. При этом изменения неразличимы для человеческого восприятия.

2. Изменение частоты или фазы: В этом методе используется модификация частотных компонентов в спектре сигнала. Частоты могут быть либо повышены, либо понижены, либо смещены по фазе, чтобы внедрить скрытую информацию.

3. Встроенные файлы: Этот метод заключается в сохранении скрытой информации внутри контейнерного файла.

Например, информация может быть внедрена в неиспользуемые биты в архиве или замаскирована внутри изображения, аудио или видео.

*Цифровые водяные знаки:*

Цифровые водяные знаки представляют собой невидимые метки, которые встраиваются в цифровые мультимедийные файлы для идентификации и аутентификации. Они помогают защитить авторские права, отслеживать источник и обеспечивать целостность файла.

Виды водяных знаков включают:

1. Обнаруживаемые: Эти знаки видимы и используются для идентификации владельца или автора. Обычно отображаются на видимой поверхности изображения или видео.

2. Незаметные: Эти знаки почти невидимы и скрыты в мультимедийных файлах. Они обычно служат для аутентификации и защиты целостности.

*Алгоритмы встраивания цифровых водяных знаков:*

1. Алгоритм адаптивной вставки: Этот алгоритм анализирует содержимое файла и встраивает водяной знак в наименее значимые части, что делает его незаметным визуально. Границы встраивания могут изменяться в зависимости от контента файла.  
2. Алгоритм дискретного вейвлет-преобразования: В этом алгоритме используются коэффициенты дискретного вейвлет-преобразования для встраивания водяных знаков. Значения коэффициентов изменяются, чтобы отразить информацию в водяном знаке.  
3. Алгоритм изменения наименьших значимых разрядов: В этом алгоритме младшим разрядам пикселей назначаются значения, соответствующие скрытой информации. Процесс встраивания контролируется, чтобы избежать значительных изменений в изображении.