СОВРЕМЕННЫЕ МЕТОДЫ КРИПТОГРАФИИ.

Петрова Мария
НФИбд-02-21
Ст. Билет: 1032216450

Что такое криптография?

Криптография – наука о способах преобразования (шифрования) информации с целью ее защиты от незаконных пользователей. Исторически первой задачей криптографии была защита передаваемых текстовых сообщений от несанкционированного ознакомления с их содержанием, известного только отправителю и получателю, все методы шифрования являются лишь развитием этой философской идеи. С усложнением информационных взаимодействий в человеческом обществе возникли и продолжают возникать новые задачи по их защите, некоторые из них были решены в рамках криптографии, что потребовало развития новых подходов и методов.

Криптография в цифровую эпоху

В связи с увеличением вычислительной мощности компьютеров, криптография стала значительно более сложной. Теперь она способна намного надежнее гарантировать безопасность информации. Шифры, которые когда-то использовал Цезарь, сегодня можно расшифровать за пару секунд.

Везде, где речь идет о конфиденциальности, криптография играет важную роль. Если вы заходите на сайт под вашим паролем, как правило, это зашифровано. Шифрование используют и мессенджеры, такие как WhatsApp или Telegram. Чтобы вас не подслушали во время телефонного звонка, телефонная связь тоже может быть зашифрована.

Основные термины криптографии

Конфиденциальность – невозможность получения информации из преобразованного массива без знания дополнительной информации (ключа).

Аутентичность информации состоит в подлинности авторства и целостности.

Под ***шифром*** понимается совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, заданных алгоритмом криптографического преобразования. В шифре всегда различают два элемента: алгоритм и ключ. Алгоритм позволяет использовать сравнительно короткий ключ для шифрования сколь угодно большого текста.

Ключ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного варианта из совокупности всевозможных для данного алгоритма. Секретность ключа должна обеспечивать невозможность восстановления исходного текста по шифрованному.

Обычно ключ представляет собой последовательный ряд букв алфавита. Следует отличать понятия "ключ" и "пароль". ***Пароль*** также является секретной последовательностью букв алфавита, однако используется не для шифрования (как ключ), а для аутентификации субъектов.

Электронной (цифровой) подписью называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и целостность сообщения.

Зашифрованием данных называется процесс преобразования открытых данных в зашифрованные с помощью шифра, а расшифрованием данных – процесс преобразования закрытых данных в открытые с помощью шифра.

Дешифрованием называется процесс преобразования закрытых данных в открытые при неизвестном ключе и, возможно, неизвестном алгоритме, т.е. методами криптоанализа.

Шифрованием называется процесс зашифрования или расшифрования данных. Также термин шифрование используется как синоним зашифрования. Однако неверно в качестве синонима шифрования использовать термин "кодирование" (а вместо "шифра" – "код"), так как под кодированием обычно понимают представление информации в виде знаков (букв алфавита).

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию. Обычно эта характеристика определяется периодом времени, необходимым для дешифрования.

Современная криптография включает в себя четыре крупных раздела:

- Симметричные криптосистемы.
- Асимметричные (Криптосистемы с открытым ключом).
- Системы электронной подписи.
- Управление ключами.

Симметричное шифрование

Является самым простым алгоритмом. Криптографы часто называют его секретным ключом криптографии (SKC) или общим, поскольку шифрование и расшифровка информации происходит с использованием одного и того же ключа. Симметричное шифрование подразумевает, что секретный цифровой ключ должен быть известен как получателю, так и отправителю.

Асимметричное шифрование

Этот алгоритм широко используется во Всемирной сети. Его также называют открытым ключом криптографии (РКС). Алгоритм РКС использует два ключа: открытый и закрытый.

•Открытый может быть известен многим. Расшифровать данные с его помощью невозможно. Например, адрес электронной почты является открытым ключом.

•Закрытый является секретным, используется для расшифровки сообщения, никогда не раскрывается другой стороне. Например, пароль учетной записи электронной почты является ключом к открытию электронных писем.

•Не имеет значения, какой ключ применяется в первую очередь, но для работы необходимы оба.

•Данные могут быть зашифрованы при помощи открытого или закрытого ключа.

Управление ключами

Управление ключами – информационный процесс, включающий реализацию следующих основных функций:

· генерация ключей;

· хранение ключей;

· распределение ключей.

Для получения ключей используются аппаратные и программные средства генерации случайных значений ключей.

Под *функцией хранения ключей* понимают организацию их безопасного хранения, учета и удаления.

Распределение ключей – самый ответственный процесс в управлении ключами. К нему предъявляются следующие требования:

1) оперативность и точность распределения;

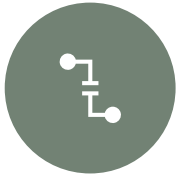
2) скрытность распределяемых ключей.

Преимущества криптографии

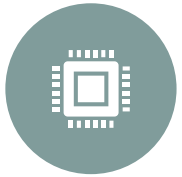
Конфиденциальность. Использование криптографии защищает конфиденциальную информацию от несанкционированного доступа.

Проверка подлинности. Криптографические методы, такие как коды аутентификации сообщений и цифровые подписи, могут защитить информацию от подмены и подделки.

Неотрекаемость, аутентификация. Сообщения, зашифрованные частным ключом или подписанные цифровой подписью, подтверждают личность заявленного отправителя.



Целостность данных. Криптографические хэши используются для сохранения целостности сообщений. С помощью дайджестов можно определить, была ли изменена информация во время ее передачи по сети.



Контроль и управление доступом. Криптография, используя различные алгоритмы шифрования, обеспечивает ограниченный контроль доступа к хранящейся или передаваемой информации. Благодаря этому, расшифровывать сообщения могут только держатели секретных ключей.

Заключение

Криптография является одним из наиболее мощных средств обеспечения конфиденциальности и контроля целостности информации. Во многих отношениях она занимает центральное место среди программно-технических регуляторов безопасности. Например, для портативных компьютеров, физически защитить которые крайне трудно, только криптография позволяет гарантировать конфиденциальность информации даже в случае кражи.

СПАСИБО ЗА ВНИМАНИЕ!