**Приведите несколько примеров применения хеш-функций в реальной жизни.**

* Алгоритмы хеширования криптовалют.
* Создание и использование электронных подписей.
* Сохранение хэш-значений паролей.

**Создайте публичный ключ RSA и скиньте его в открытом виде.**

---- BEGIN SSH2 PUBLIC KEY ----

Comment: "rsa-key-20241025"

AAAAB3NzaC1yc2EAAAADAQABAAABAQCvyVKbaw6szoyNuwcpjIbqyClqmGvTqM7Q

ujkQPdkMg03g0IfBRE3QHmfeLSs2P/+LkAESO/cVgeUr8w9C5BVvlODNTpJjatFy

G8liJr3FBZXxyfV/FOid9zNsc5LiZe5Nmxe2uYakEVWRjRGHqBPYo0RCCqzoD0rt

SCXeaC6clqfiajBw46jpu68ulK55VjspegApVvNRRjCC68s+q1zjupLjSNLro+/k

CwpfrHwujH+Qc4NzFSA00Oh3skI5aU78su5yiH1mTS6MX2c+opkJ23649vQviRey

NrfQAai5cF2rbNqXWMvRgMP7E5QCs3sELIpUYInlMRT3zclYCZRh

---- END SSH2 PUBLIC KEY ----

**Изучить несколько различных алгоритмов хеширования, таких как MD5, SHA-1, SHA-256 и SHA-512.**

**Алгоритм MD5 (Message Digest 5):** Алгоритм по построению дайджеста сообщения. Размер – 128 бит. На вход принимает входной поток данных, хеш которого необходимо найти. Длина сообщения измеряется в битах и может быть любой (в том числе нулевой). Считается небезопасным, ранее использовался для проверки целостности файлов и хранения хэшей паролей.

**Алгоритм SHA-1(Secure Hash Algorithm):** алгоритм криптографического хеширования. Для входного сообщения произвольной длины алгоритм генерирует 160-битное хеш-значение, называемое дайджестом сообщения. Используется в криптографических приложениях и протоколах. В настоящее время обнаружены уязвимости к коллизиям.

**Алгоритм SHA-256:** применяется в алгоритмах хеширования биткойна и других криптовалют. Обеспечивает высокий уровень безопасности и устойчив к коллизиям. Входной хеш составляет 256 бит.

**Алгоритм SHA-512:** применяется в криптографических приложениях, например в цифровых подписях и блокчейн-платформах. Имеет высокий уровень безопасности, устойчив к коллизиям, но потребляет больше ресурсов, чем SHA-256. Входной хеш составляет 512 бит.

**Исследовать примеры применения хешей в реальном мире, такие как Bitcoin, блокчейн.**

В Bitcoin используется алгоритм SHA-256. Каждый блок транзакций в Bitcoin содержит хэш предыдущего блока, создавая цепочку, где каждый блок связан с предыдущим. Это свойство обеспечивает неизменность блокчейна. Каждая транзакция хешируется, создавая уникальный идентификатор транзакции. Это позволяет быстро проверять подлинность транзакций, которые включены в блоки.