|  |
| --- |
| Level 1 Приведите несколько примеров применения хеш-функций в реальной жизни. Создайте публичный ключ RSA и скиньте его в открытом виде. |
| 1. **Хранение паролей**: Хеш-функции используются для безопасного хранения паролей. Вместо того чтобы хранить пароль в виде открытого текста, система хранит его хеш. Когда пользователь вводит пароль, система хеширует введенный пароль и сравнивает его с хранимым хешем. 2. **Цифровые подписи**: Хеш-функции используются для создания цифровых подписей. Подписываемое сообщение хешируется, а затем хеш подписывается закрытым ключом отправителя. Получатель может проверить подлинность подписи, используя открытый ключ отправителя и хеш сообщения. 3. **Целостность данных**: Хеш-функции используются для проверки целостности данных. Например, при передаче файлов через интернет можно создать хеш файла и передать его вместе с файлом. Получатель может вычислить хеш полученного файла и сравнить его с отправленным хешем для проверки целостности данных. 4. **Блокчейн и криптовалюты**: В блокчейне хеш-функции используются для создания уникальных идентификаторов блоков и транзакций. Например, в Bitcoin используется алгоритм SHA-256 для создания хеша каждого блока, что обеспечивает неизменяемость и безопасность данных. |
| ssh-rsa  SuperShurik@SuperShurik |

|  |
| --- |
| Level 2 Изучить несколько различных алгоритмов хеширования, таких как MD5, SHA-1, SHA-256 и SHA-512. Исследовать примеры применения хешей в реальном мире, такие как Bitcoin, блокчейн. |
| Хеширование в блокчейне реализовано путем применения криптографических  хеш-функций к блокам данных.  Блокчейн - это цепочка связанных блоков, каждый из которых содержит некоторые  данные, такие как транзакции в случае блокчейна биткойна. Хеш-функция применяется  к каждому блоку, чтобы создать уникальный хеш-код, который представляет  содержимое блока. |