1. Что такое хеш-функция?

Функция однозначно преобразующая входные данные в битовую последовательность с помощью алгоритма (функция сжатия)

1. Что такое хеширование?

Действие производимое хеш-функцией

1. Перечислите алгоритмы хеширования.

Семейства MD и SHA

1. Поясните понятие «сеансовый ключ»

общий секрет — информация, которая вырабатывается на основе секретного **ключа** одной стороны и открытого **ключа** другой стороны

1. Поясните понятия «публичный» и «секретный» ключи?

Секретный - ключ, известный только своему владельцу

Публичный - ключ, который может быть опубликован и используется для проверки подлинности подписанного документа

1. Поясните понятие «дайджест».

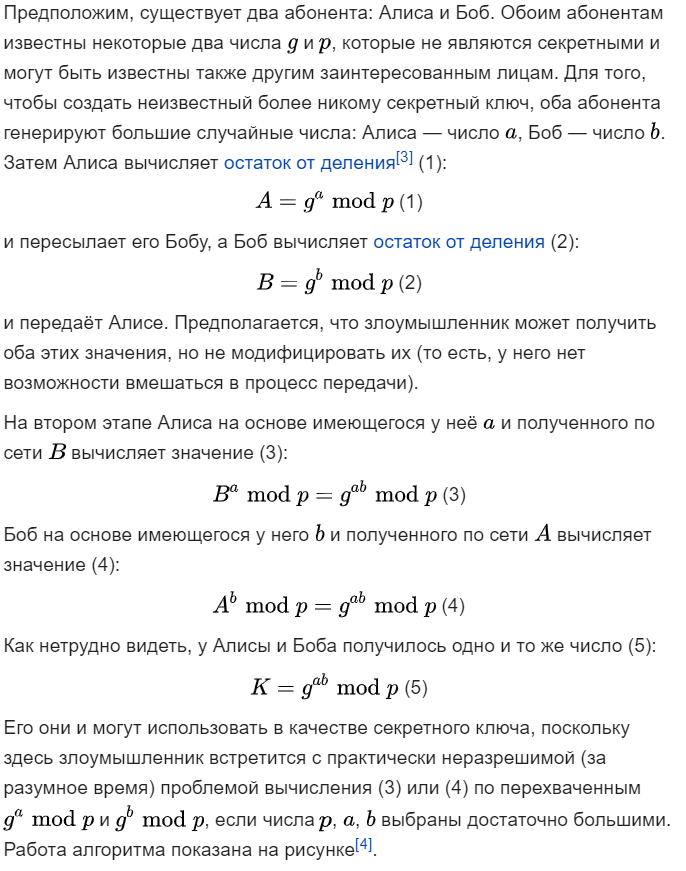
Хеш-сумма - результат обработки неких данных хеш-функцией

1. Для чего используется дайджест.

Значение хеш-суммы может использоваться для проверки целостности данных, их идентификации и поиска (например в P2P-сетях), а также заменять собой данные, которые небезопасно хранить в явном виде (например, пароли, ответы на вопросы тестов и т. д.). Также алгоритмы хеширования используются для проверки целостности и подлинности файлов.

1. Поясните принцип работы алгоритма Диффи-Хеллмана.

Позволяет двум сторонам получить общий секретный ключ, используя незащищенный от прослушивания, но защищённый от подмены канал связи.



1. Поясните понятие «цифровая подпись», объясните принцип ее применения.

это реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость).