1. **Что такое хеш-функция?**

*Хеш-функция* – математическая или иная функция *h* = *H*(*М*), которая принимает на входе строку символов *М*, называемую также *прообразом*, переменной длины *n* и преобразует ее в выходную строку фиксированной (обычно – меньшей) длины *l*.

1. **Что такое хеширование?**

Хеширование (или хэширование, англ. hashing) – это преобразование входного массива данных определенного типа и произвольной длины (практически) в выходную битовую строку фиксированной длины.

1. **Перечислите алгоритмы хеширования.**

Семейства MD и SHA

1. **Поясните понятие «сеансовый ключ»**

Сеансовый 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

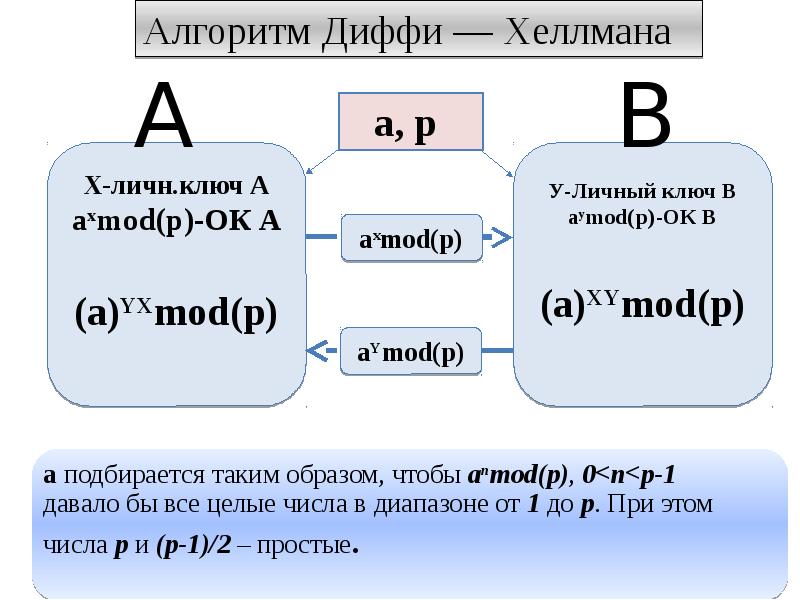
1. **Поясните понятие «дайджест».**

Хеш-суммой называется значение [хеш-функции](https://dic.academic.ru/dic.nsf/ruwiki/1179335). В [криптографии](https://dic.academic.ru/dic.nsf/ruwiki/17909) хеш-сумму иногда также называют дайджестом сообщения.

1. **Для чего используется дайджест.**

Значение хешсуммы может использоваться для проверки целостности данных, а также заменять собой данные, которые небезопасно хранить в явном виде (например, пароли, ответы на вопросы тестов и т.д.)

1. **Поясните принцип работы алгоритма Диффи-Хеллмана.**



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

электронная цифровая подпись - последовательность символов, являющаяся реквизитом электронного документа и предназначенная для подтверждения его целостности и подлинности