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 ключ*** - 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.

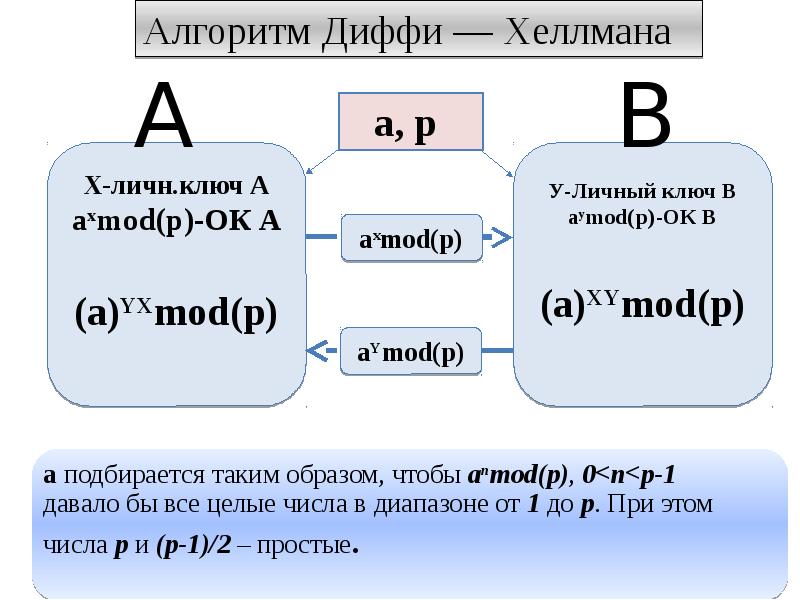
1. **Поясните понятие «дайджест».**

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.**



Алгоритм Диффи-Хэллмана:

1. Алиса и Боб сначала объявляют общий модуль и генератор (p=17, g=3)

2. Алиса выбирает своё приватное число (пусть 54), вычисляет 3^54 mod 17=15.

3. Посылает данный результат (15) Бобу.

4. Боб выбирает своё приватное число (пусть 24), вычисляет 3^24 mod 17=16, посылает это число Алисе.

5. Алиса берет публичное число Боба и возводит в своё приватное число: 16^54 mod 17=1

6. Боб берёт публичное число Алисы и возводит в своё приватное число: 15^24 mod 17=1.

7. 1 - общий секретный ключ Боба и Алисы.

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