Понятие функции хэширования, дайджест сообщения, свойства необратимости, рассеивания и чувствительности к изменениям.

Выполнила: Аюрова Д.Ч.

Проверил: Тенгайкин Е.А.

Хэширование

- *Хэширование* (hashing) - это процесс получения индекса элемента массива непосредственно в результате операций, производимых над ключом, который хранится вместе с элементом или даже совпадает с ним.
- **Хеширование** - преобразование по определённому алгоритму входного массива данных произвольной длины в выходную битовую строку фиксированной длины. Такие преобразования также называются **хеш-функциями** или **функциями свёртки**, а их результаты называют **хешем**, **хеш-кодом**, **хеш-суммой** или **свод-кой сообщения** (англ. *message digest*)

- Хеширование применяется для построения ассоциативных массивов, поиска дубликатов в сериях наборов данных, построения достаточно уникальных идентификаторов для наборов данных, контрольного суммирования с целью обнаружения случайных или намеренных ошибок при хранении или передаче, для хранения паролей в системах защиты (в этом случае доступ к области памяти, где находятся пароли, не позволяет восстановить сам пароль), при выработке электронной подписи (на практике часто подписывается не само сообщение, а его хеш-образ).

Понятие *хеширования*

- Понятие ***хеширования***– это разбиение общего (базового) набора уникальных ключей элементов данных на непересекающиеся наборы с определенным свойством.

Дайджест сообщения

- Дайджест сообщения - это уникальная последовательность символов, однозначно соответствует содержанию сообщения Обычно дайджест имеет фиксированный размер, например, 128 или 168 бит, что не зависит от длин ни самого сообщения Дайджест включается в состав ЭЦП со сведениями об авторе и шифруется вместе с нимми.