**Что такое кодирование?**

**Метод преобразования данных из одного формата в другой,** с сохранением той же информации, **чтобы их можно было понять и использовать в различных системах**.

Обычно кодирование включает в себя таблицу преобразования, такую ​​как [таблица ASCII](https://en.wikipedia.org/wiki/ASCII) например, которая сопоставляет элемент представления в одной системе с соответствующим элементом представления в другой системе.

Некоторые кодировки:

* [Юникод](https://en.wikipedia.org/wiki/Unicode).
* [Base64](https://en.wikipedia.org/wiki/Base64)
* ASCII

Кодирование обеспечивает **совместимость** между системами. Это позволяет системам, использующим разные представления данных, обмениваться информацией.

Кодирование **не имеет цели обеспечения безопасности**. Любой, кто знает алгоритм преобразования, может кодировать и декодировать данные. Алгоритм преобразования не держится в секрете. Напротив, он является общедоступным, чтобы облегчить взаимодействие между системами.

Наконец, кодирование — **обратимый процесс**. Данные преобразуются из одного представления в другое, и обратно к исходному представлению без потери информации.

## Что такое шифрование?

Шифрование — это **метод, который делает данные нечитаемыми и трудными для декодирования нежелательным пользователям**.

Итак, по сути, шифрование — это механизм, который преобразует данные в другое представление, чтобы посторонние глаза не могли их понять.

В каком-то смысле шифрование — это форма кодирования. Он преобразует данные из одного представления в другое. По этой причине иногда люди используют термины «шифрование» и «кодирование» как синонимы. Однако цель шифрования отличается от цели кодирования.

Техника шифрования направлена ​​на то, чтобы сделать данные **нечитаемыми и трудными для декодирования –** эта задача является полностью противоположной задачи кодирования, целью которого является сделать данные максимально понятными в разных системах.

Основная цель шифрования — обеспечить **конфиденциальность данных,** т. е. защитить данные от доступа посторонних лиц.

Лучшие механизмы шифрования данных основаны на математических алгоритмах, которые можно решить только при наличии ключа или при наличии передовых вычислительных мощностей. Существуют два семейства алгоритмов шифрования на основе ключей:

* Алгоритмы с симметричным ключом: эти алгоритмы используют один и тот же ключ для шифрования и дешифрования данных. Например AES.
* Алгоритмы с асимметричным ключом: эти алгоритмы используют разные ключи для шифрования и дешифрования данных. Два ключа связаны сложной математической зависимостью. [RSA](https://en.wikipedia.org/wiki/RSA_(cryptosystem%29) является примером алгоритма этого семейства.

Как и чистое кодирование, шифрование также является **обратимым процессом**, но только для уполномоченных лиц - авторизованных пользователей — тех, у кого есть ключ дешифрования.

## Что такое хеширование?

По сути, это **метод генерации уникальной строки фиксированной длины (хеша) строго в зависимости от конкретных входных данных**.

Поскольку сгенерированный хэш зависит от конкретных входных данных, любое небольшое изменение входных данных приводит к созданию другого хеша. Имея хеш фрагмента данных, можно проверить, были ли эти данные изменены, вычислив его хэш и сравнив его с тем, который у вас уже есть. Хеширование **обеспечивает целостность данных**. Алгоритм хеширования должен обладать следующими особенностями:

1. Полученный хеш имеет фиксированную длину.
2. Один и тот же вход всегда производит один и тот же результат.
3. Несколько разных входов *не должны* давать одинаковый результат.
4. Не должно быть возможности получить входные данные из выходных данных.
5. Любое изменение входных данных подразумевает другой результирующий хэш.

Хеширование **не является обратимым процессом**, в отличие от кодирования и шифрования.

