* Checksum: is a small-sized [datum](https://en.wikipedia.org/wiki/Datum) derived from a block of [digital data](https://en.wikipedia.org/wiki/Digital_data) for the purpose of [detecting errors](https://en.wikipedia.org/wiki/Error_detection) which may have been introduced during its [transmission](https://en.wikipedia.org/wiki/Telecommunication) or [storage](https://en.wikipedia.org/wiki/Computer_storage)
* Checksums are often used to verify data integrity but are not relied upon to verify data authenticity
* Checksum Algorithm will usually output a significantly different value, even for small changes made to the input
* Cryptographic Hash Function: a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size (a hash) and is designed to be a one-way function, that is, a function which is infeasible to invert
  + input data is often called the **message**
  + output (the hash value or hash) is often called the message digest
* Main Properties of a Cryptographic Hash Function:

1. it is deterministic so the same message always results in the same hash
2. a small change to a message should change the hash value so extensively that the new hash value appears uncorrelated with the old hash value
3. it is [infeasible](https://en.wikipedia.org/wiki/Computational_complexity_theory#Intractability) to find two different messages with the same hash value

* Cryptographic Hash Functions take in a string of any length as input and produce a fixed-length hash value
* CRC32 and other cyclic redundancy checks, are designed to meet much weaker requirements (vs cryptographic hash functions), and are generally unsuitable as cryptographic hash functions
* Password Verification: only store the hash digest of each password, versus storing the cleartext (unencrypted password)
  + To authenticate a user, the password presented by the user is hashed and compared with the stored hash
  + The password is often concatenated with a random, non-secret salt value before the hash function is applied
  + a salt is random data that is used as an additional input to a one-way function that "hashes" data, a password or passphrase
  + The salt is stored with the password hash

Salts: <https://en.wikipedia.org/wiki/Salt_(cryptography)>, <https://crypto.stackexchange.com/questions/1776/can-you-help-me-understand-what-a-cryptographic-salt-is>

Cryptographic Hash Functions: <https://en.wikipedia.org/wiki/Cryptographic_hash_function>

Checksums: <https://en.wikipedia.org/wiki/Checksum>

CRC32 Exercise: <https://algs4.cs.princeton.edu/34hash/>