Attacks on Cryptographic Hash Algorithms

There are 3 types of attacks on hash algorithms:

1. Collision attack

- Find any two messages that have the same hash.
- The easiest to mount

2. First preimage attack

- Given a hash, find a message that has **the given hash** value.

3. Second preimage attack

- For a given message, find another message that has **the same** hash.