**Preimage Attack**

**Description 1**

In cryptography, a **preimage attack** on [cryptographic hash functions](https://en.wikipedia.org/wiki/Cryptographic_hash_function) tries to find a [message](https://en.wikipedia.org/wiki/Message) that has a specific hash value. In other words, attacker tries to find any preimage x such that h(x) = y ( i.e. hash value of x is y) . [1]

Note: hash attack and Preimage attack both target hash algorithms and have the **same consequences**.  a collision attack is easier to mount than a preimage attack (and preimage attack is faster than brute forcing), as it is not restricted by any set value (any two values can be used to collide).

**Description 2**

A preimage attack will attempt to discover a message that can replicate the hash of a given message. A preimage attack can reproduce a hash that is the same as a known hash. This would be similar to you walking into a room of twenty-two other people and finding one of them has the same birthday as you. It's a 60 percent chance any two of the twenty-three people have the same birthday, but significantly less likely that you are one of these two people. Using strong and complex passwords make a preimage attack significantly more difficult. (warning: the reference is not known but I found the description helpful for this stage of work)

**Description 3**

A Preimage attack occurs if for given a message m1, an attacker finds a second message m2 different from m1 such that H(m1) == H(m2) (hash value of message m1 is equal to hash value of message m2)

**Refrences**

**[1]** <http://web.cs.ucdavis.edu/~rogaway/papers/relates.pdf>

**[2]** <http://www.techexams.net/forums/security/56135-difference-between-bday-attack-preimage-attack.html>

[3] <https://www.cs.cmu.edu/~perspectives/md5.html>