Hash function

$$h : \{0,1\}^* \to \{0,1\}^n \qquad n \in \mathbb{N}_0$$

Compression: arbitrary length to fixed length.

Ease of computation: we know an efficient algorithm to perform h.

Collision

$$h(x_1) = h(x_2)$$

Preimage resistance

Given y it's infeasible to find any x such that $h(x) = y$.

Second preimage resistance

Given x_1 it's infeasible to find another x_2 such that $h(x_1) = h(x_2)$.

Collision resistance

Infeasible to find x_1 and x_2 such that $x_1 \neq x_2$ and $h(x_1) = h(x_2)$.

One-way

Efficient algorithm to calculate $f(x) = y$, no efficient algorithm to calculate $f^{-1}(y) = x$. No one has proved one-way functions really exist.
Not to be confused with not being one-to-one:

$$\texttt{rshift}(0011) = \texttt{rshift}(0010) = 0001$$

Given y, easy to find x such that $\texttt{rshift}(x) = y$.

SHA256

$$f : \{0,1\}^{256} \times \{0,1\}^{512} \to \{0,1\}^{256}$$

Padding

$$\texttt{pad}(m) = M$$

- Append a 1 bit.
- Append 0 bits such that $|M| \equiv_{512} 448$.
- Append $|M|$, least significant bit on right.

Note padding with zeros or not padding would give easy collisions.

Merkle-Damgrad