Hashfunctions

**Aim:** To attach to a given message $m$ of $k$ symbols a short “fingerprint” of $l << k$ symbols.

**Informal Definition:** A function $h : \Sigma^k \rightarrow \Sigma^l$ is called a hash function if

1. $h(x)$ is easy to compute for any $x \in \Sigma^k$;
2. $h$ is collision resistant: no one can feasibly find two values $x_1, x_2$ such that $h(x_1) = h(x_2)$;
3. $h$ is preimage resistant: given $y \in \Sigma^l$, no one can feasibly find an $x$ such that $h(x) = y$.

**Remarks:**
1. The purpose of a hashfunction is to guarantee that a message has not been altered. (It is not a signature by itself.)
2. Hashfunctions are public information, i.e. the recipe for computing $h(x)$ is known to all.

**References:**
2. J. Buchmann, Introduction to Cryptography, ch. 10 (pp. 205–216).