

# Security of hash functions

Brute-forcing a hash function



## CR - Collision Resistance

➡ given  $H$ , hard to find  $m$  and  $m'$  such that  $H(m) = H(m') = x$

Given a hash function  $H$  of  $n$  bits output

- Reaching all possibilities  $2^n$  cases
- On average, an attacker should try half of them  $2^{n-1}$  cases