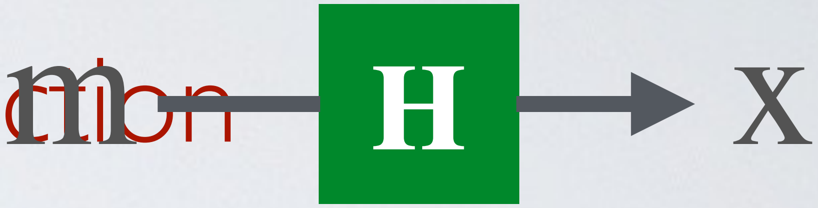
Security of hash functions

Brute-forcing a hash function



CR - Collision Resistance

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

Given a hash function $\mathbf{H}$ of $\mathbf{n}$ bits output

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