

# Computational complexity



- Given  $H$  and  $m$ , computing  $x$  is **easy** (polynomial or linear)
- Given  $H$  and  $x$ , computing  $m$  is **hard** (exponential)

➔  $H$  is **not invertible**

# Preimage resistance and collision resistance



## **PR - Preimage Resistance (a.k.a One Way)**

- ➡ given  $H$  and  $x$ , hard to find  $m$   
e.g. password storage

## **2PR - Second Preimage Resistance (a.k.a Weak Collision Resistance)**

- ➡ given  $H$ ,  $m$  and  $x$ , hard to find  $m'$  such that  $H(m) = H(m') = x$   
e.g. virus identification

## **CR - Collision Resistance (a.k.a Strong Collision Resistance)**

- ➡ given  $H$ , hard to find  $m$  and  $m'$  such that  $H(m) = H(m') = x$   
e.g. digital signatures

**CR → 2PR and CR → PR**