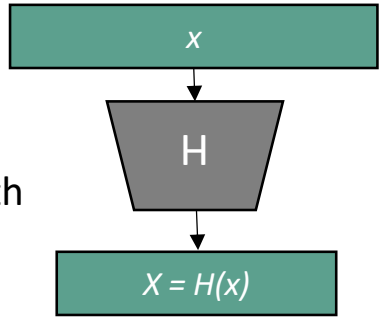
Cryptographic Hash Function

$H: \{0,1\}^* \rightarrow \{0,1\}^{l(n)}$

- arbitrary input length, fixed output length
- deterministic
- "easy" to compute, "difficult" to invert



Attacks:

Birthday attack

$l(n) = poly(n)$, with n the security parameter
$\{0,1\}^*$: sequence on bits, regardless its size
s.t.: such that
$\mathcal{A}$: adversary

Security

Collision resistance

$\text{Hash}^{\text{coll}}_{\mathcal{A},H}(n)=1$ if
$\mathcal{A}$ outputs $x,y \in \{0,1\}^*$ s.t.
$\boldsymbol{x \neq y}$ **and** $\boldsymbol{H(x) = H(y)}$
$\text{Hash}^{\text{coll}}_{\mathcal{A},H}(n)=0$, otherwise

H is *collision resistant* if
$\forall \mathcal{A}$ PPT, $\exists\ \varepsilon(n)$ negligible s.t.:
$\Pr[\text{Hash}^{\text{coll}}_{\mathcal{A},H}(n)=1] \leq \varepsilon(n)$

Second pre-image resistance

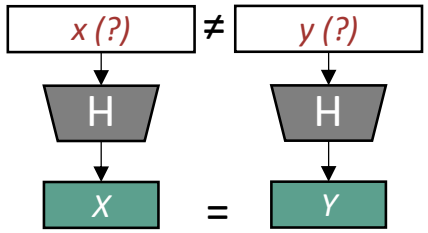
$\text{Hash}^{\text{2nd-pre-img}}_{\mathcal{A},H}(n)=1$ if
given $x \leftarrow^R \{0,1\}^*$,
$\mathcal{A}$ outputs $y \in \{0,1\}^*$ s.t.
$\boldsymbol{x \neq y}$ **and** $\boldsymbol{H(x) = H(y)}$
$\text{Hash}^{\text{2nd-pre-img}}_{\mathcal{A},H}(n)=0$, otherwise

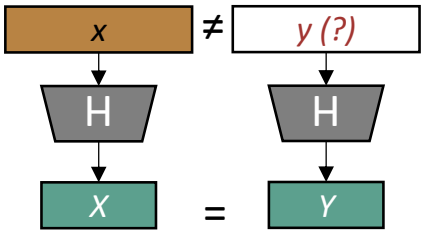
H is *second pre-image resistant* if
$\forall \mathcal{A}$ PPT, $\exists\ \varepsilon(n)$ negligible s.t.:
$\Pr[\text{Hash}^{\text{2nd-pre-img}}_{\mathcal{A},H}(n)=1] \leq \varepsilon(n)$

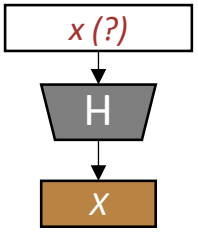
First pre-image resistance

$\text{Hash}^{\text{1st-pre-img}}_{\mathcal{A},H}(n)=1$ if
given $\mathbf{X} = H(x')$, $x' \leftarrow^R \{0,1\}^*$,
$\mathcal{A}$ outputs $x \in \{0,1\}^*$ s.t.
$\boldsymbol{H(x) = X}$
$\text{Hash}^{\text{1st-pre-img}}_{\mathcal{A},H}(n)=0$, otherwise

H is *first pre-image resistant* if
$\forall \mathcal{A}$ PPT, $\exists\ \varepsilon(n)$ negligible s.t.:
$\Pr[\text{Hash}^{\text{1st-pre-img}}_{\mathcal{A},H}(n)=1] \leq \varepsilon(n)$







one-way function

higher security ← → lower security