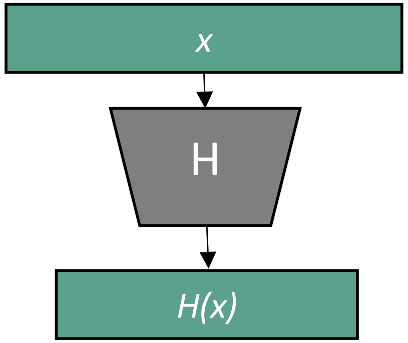
Hash Function -

Hash Function

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

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



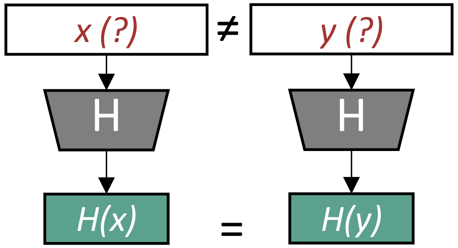
− *Attacks:*
Birthday attack

Security

Collision resistance

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

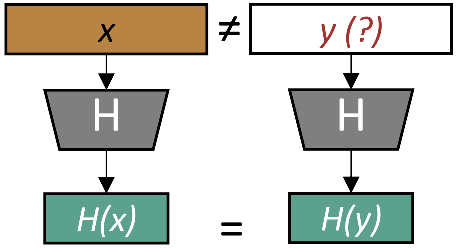
H is *collision resistant* if $\forall \mathcal{A}$ PPT, $\exists\ \varepsilon(n)$ negligible s.t.:
$\Pr[\mathrm{Hash}^{\mathrm{coll}}_{\mathcal{A},H}(n)=1] \leq \varepsilon(n)$



Second pre-image resistance

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

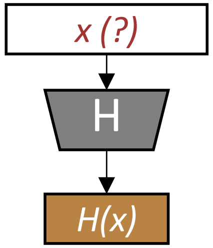
H is *second pre-image resistant* if $\forall \mathcal{A}$ PPT, $\exists\ \varepsilon(n)$ negligible s.t.:
$\Pr[\mathrm{Hash}^{\text{2nd-pre-img}}_{\mathcal{A},H}(n)=1] \leq \varepsilon(n)$



First pre-image resistance

$\mathrm{Hash}^{\text{1st-pre-img}}_{\mathcal{A},H}(n)=1$ if:
given X, $\mathcal{A}$ outputs
$x \in \{0,1\}^*$ s.t.
$\boldsymbol{H(x) = X}$
$\mathrm{Hash}^{\text{1st-pre-img}}_{\mathcal{A},H}(n)=0$, otherwise

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



one-way function

higher security ← *lower security*