Hash Function

2021年4月7日 19:21

SHA - 0,1,2,3. = secure hash algo.

Hash functions

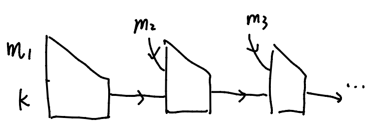
- key public
- $H: \{0,1\}^* \longrightarrow \{0,1\}^n$

Goal:

1. one - way
2. collision - resistant
3. $x \to h(x) \approx$ random

Davies - Meyer

$$h(x,y) = P_x(y) \oplus y$$



Collision - resistance

$$H = \{ h_k : \{0,1\}^{\ell} \to \{0,1\}^n \}_{n \in N,\ \ell > n,\ (\ell \text{ can be } *)} \quad , \ \forall \text{ n.u.p.p.t} \ , \ \exists \text{ negl. } \varepsilon(n).$$

$$\Pr_k \left[Adv(1^n, k) \to x_1, x_2 \in \{0,1\}^{\ell} \text{ s.t. } h_k(x_1) = h_k(x_2),\ x_1 \neq x_2 \right] < \varepsilon(n)$$

Remark: We define by prob. over k instead of a single hash function, because Adv may just store collision pairs.

Collision Resistant $\to$ OWF

if not OW, $x \to h(x) \to y$. $x \neq y$ with non-negl. Prob.

Collision - Resistance from Discrete - log.

$G, k, q, h = g^a, a \leftarrow$ random Assumption: find a is difficult

$|G| = p$ (eg. $G = \mathbb{Z}_q^*$, $q = 2p+1$)

$$h_k : \mathbb{Z}_p \times \mathbb{Z}_p \to G$$

$$x, y \mapsto g^x \cdot h^y$$

Proof. Suppose $Adv \to (x_1, y_1)\ (x_2, y_2)$

$$g^{x_1} h^{y_1} = g^{x_2} h^{y_2} \Rightarrow g^{\frac{x_1 - x_2}{y_2 - y_1}} = h = g^a \Rightarrow \text{find } a$$

Hence collision - resistant

Commitment from Hash functions.

- relax def. of binding:

$$\Pr_{info} \left[Adv(1^n, info) \longrightarrow m_1, m_2, r_1, r_2, \text{ s.t. } m_1 \neq m_2 \ \& \ Commit(m_1, r_1) = Commit(m_2, r_2) \right] < \varepsilon(n)$$

- hiding.

$$Commit(m_1, r_1) \approx_c Commit(m_2, r_2)$$

"Random Oracle"

CR $\Rightarrow$ binding. Trivial.

SHA 2.

$h(x_1)$ $h(x_2)$