Hash Functions

Exam Stuff:

Avg 70/85
Med 74/85

#3

$$m \xmapsto{\text{Enc}} (r,\ F(k,m) \oplus r)$$
$$= (r,\ s)$$

- ask for $\text{Enc}(m)$ twice
- get $(r,\ F(k,m) \oplus r) = (r, s)$
  $(r',\ F(k,m) \oplus r') = (r', s')$

$$r \oplus s = F(k,m) = r' \oplus s'$$

#4:

$$F(k, 0110\ldots) = \text{XOR of} \quad \begin{matrix} k[1,0] & k[2,0] & k[3,0] \\ k[1,1] & k[2,1] & k[3,1] \end{matrix}$$

$$\begin{array}{rl} & F(k,\ 000\ldots0) \\ \oplus & F(k,\ 100\ldots0) \\ \hline & k[1,0] \oplus k[1,1] \end{array} \qquad \begin{matrix} k[1,0] & k[2,0] & k[3,0] \\ k[1,1] & k[2,1] & k[3,1] \end{matrix}$$

$$\begin{matrix} k[1,0] & k[2,0] & k[3,0] \\ k[1,1] & k[2,1] & k[3,1] \end{matrix}$$

$$\begin{array}{rl} & F(k,\ 011\ldots) \\ \oplus & F(k,\ 111\ldots) \\ \hline & k[1,0] \oplus k[1,1] \end{array} \qquad \begin{matrix} k[1,0] & k[2,0] & k[3,0] \\ k[1,1] & k[2,1] & k[3,1] \end{matrix}$$

$$\begin{matrix} k[1,0] & k[2,0] & k[3,0] \\ k[1,1] & k[2,1] & k[3,1] \end{matrix}$$

#5

$$m \xmapsto{\text{Enc}} (r,\ F(k,r) \oplus m)$$

$$\text{Dec}\big(k,\ (r,s)\big) = F(k,r) \oplus s = m$$

$$\text{Dec}\big(k,\ (r, s \oplus x)\big) = F(k,r) \oplus s \oplus x = m \oplus x$$

(c): for each $x = 00 0 \cdots$ to $ff 0 \cdots$

Send $(r, s \oplus x)$ to oracle

learn whether $m^* \oplus x$ has null char.

Ex: $(r, s \oplus \underbrace{c9000\cdots}) \longrightarrow$ oracle says yes

$\Rightarrow$ 1st byte of m^* is c9

Hash functions:

$$\boxed{H : \{0,1\}^* \longrightarrow \{0,1\}^n}$$

$\{0,1\}^*$: input data of any length

$\{0,1\}^n$: output fixed length

$$\begin{array}{ccc} \text{file}_1 & & \text{file}_2 \\ \downarrow & & \downarrow \\ H(\text{file}_1) & \stackrel{?}{=} & H(\text{file}_2) \end{array}$$

Idea: "$\underbrace{\text{If } H(x) = H(x') \text{ then } x = x'}_{\text{definition of 1-to-1 (injective)}}$"

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

$\{0,1\}^n$: finite # of outputs

$\{0,1\}^*$: infinite # of inputs

} injectivity is impossible

Def: x, x' are a collision if $x \neq x'$, $H(x) = H(x')$

Crypto: It's ok if collisions exist in principle as long as they are hard to find

Flavors of security

- collision resistance: given H, find any collision $x \neq x'$, $H(x) = H(x')$

$2^{n/2}$

- target-coll. resistance:
  given $H(x)$ for unknown x,
  find x' (possibly equal to x) s.t. $H(x') = H(x)$

2^n

- second-preimage resistance
  given x
  find $x' \neq x$ s.t. $H(x') = H(x)$

2^n

Cost of finding collisions

Q: How long does it take to break collision-resistance?

A: If $H: \{0,1\}^* \to \{0,1\}^n$ then need to evaluate H on $\sim 2^{n/2}$ values to get good probability of collision
(birthday bound)

Q: break second-preimage? takes $\sim 2^n$ H calls.