

# Hash Functions

Exam Stuff:

Avg 70/85  
Med 74/85

#3

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

- ask for  $\text{Enc}(m)$  twice

$$\begin{aligned} \text{get } (r, F(k, m) \oplus r) &= (r, s) \\ (r', F(k, m) \oplus r') &= (r', s') \end{aligned}$$

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

#4:

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

$$\begin{aligned} &F(k, 000 \dots 0) \\ \oplus &F(k, 100 \dots 0) \\ \hline &k[1,0] \oplus k[1,1] \end{aligned}$$

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

$$\begin{aligned} &F(k, 011 \dots) \\ \oplus &F(k, 111 \dots) \\ \hline &k[1,0] \oplus k[1,1] \end{aligned}$$

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

#5

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

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

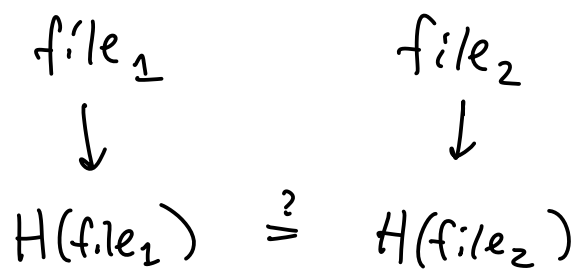
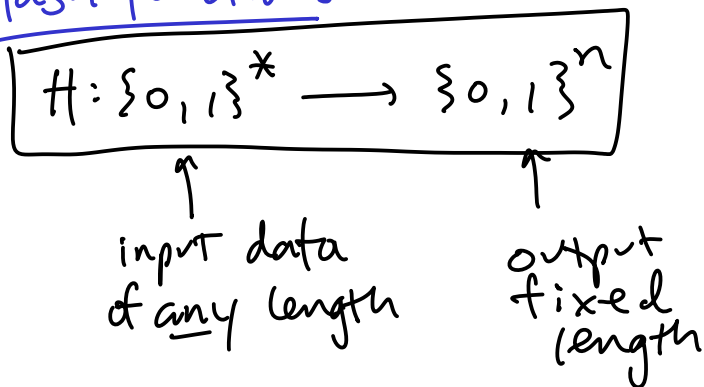
$$\text{Dec}(k, (r, \underline{s \oplus x})) = F(k, r) \oplus \underline{s \oplus x} = m \oplus x$$

(c): for each  $x = \emptyset \emptyset \emptyset \dots$   
to  $f f \emptyset \dots$

Send  $(r, s \oplus x)$  to oracle  
learn whether  $m^* \oplus x$  has null char.

Ex:  $(r, S \oplus \underline{c9\emptyset\emptyset\emptyset\dots}) \rightarrow$  oracle says yes  
 $\Rightarrow$  1<sup>st</sup> byte of  $m^*$  is c9

## Hash functions:



Idea: "If  $H(x) = H(x')$  then  $x = x'$ "  
definition of 1-to-1 (injective)

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

↑ infinite # of inputs      ↑ finite # of outputs

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