	Sym key	Asy key
1. Confidentiality /privacy	SKE (AES DES)	PKE (RSA, DL) LWE
2. Data Integrity / authentication.	MAC/Hash	Digital Signature (RSA, ..)
3. Non-repudiation /non-deniability	X	✓

Birthday Paradox

K persons $\longrightarrow \binom{K}{2}$ pairs

$\approx \frac{K^2}{2}$

$H : \{0,1\}^{\leq 2^{64}} \longrightarrow \{0,1\}^{256}$

Collision

$M \neq M'$

$H(M) = H(M')$

Preimage

MD5

Discrete log problem

$\langle g \rangle = G \quad |G| = p.$

$h \in G \quad$ find $x \in \{1, 2, \cdots p\}$ s.t. $g^x = h$.

Choose h randomly $\quad \mathbb{Z}_p$

$H : \mathbb{Z}_p^2 \longrightarrow G$

$(a, b) \longmapsto g^a \cdot h^b$

$g^a h^b = g^{a'} h^{b'}$

$g^{a-a'} = h^{b'-b}$

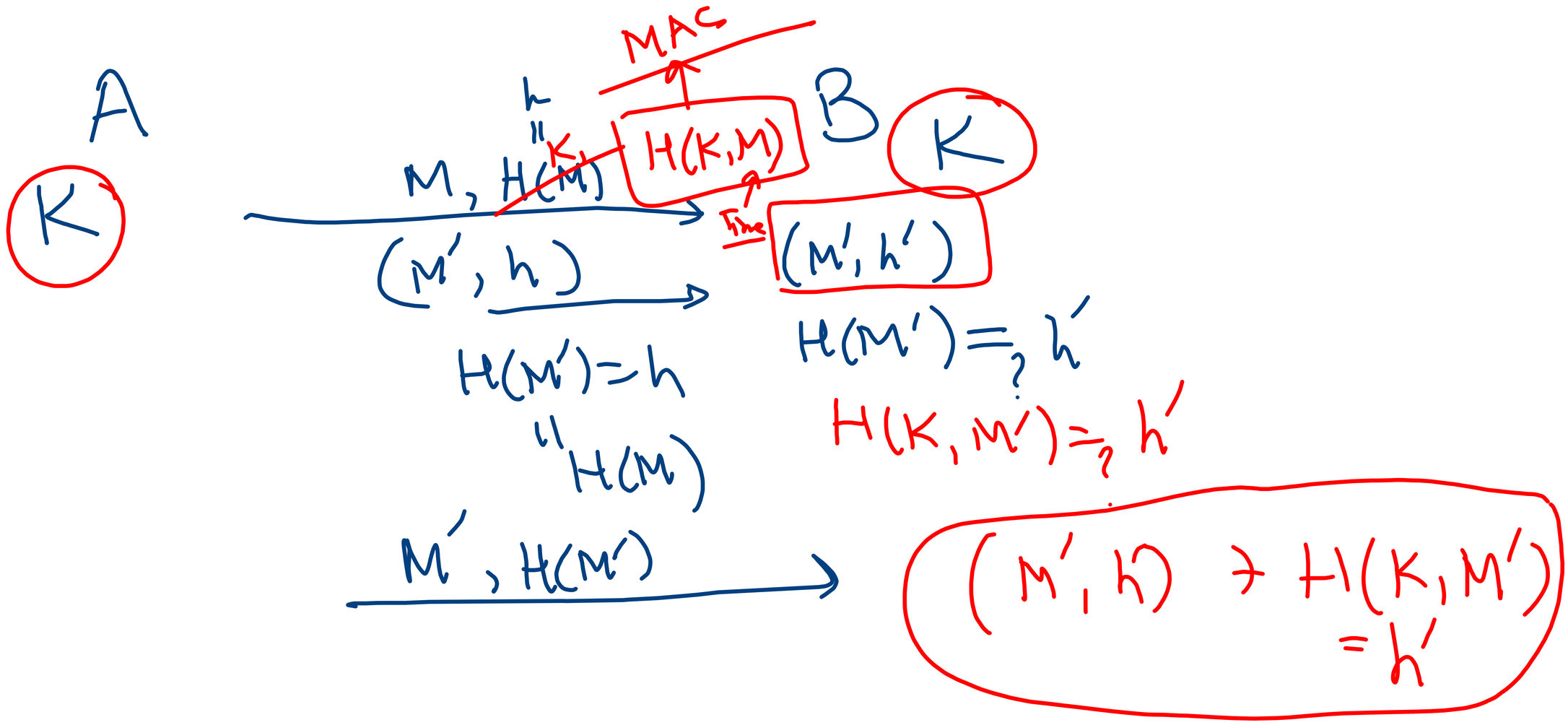
$g^x = h$

$x = (a - a') \times \left((b' - b)^{-1} \bmod p \right)$

?

Preimage

Given h from the range
Find x from the domain $H(x) = h$


A
K
M, H(M)
K
h
"
H(K,M)
MAC
B
K
Time
(M', h')
(M', h)
H(M') = h
" H(M)
M', H(M')
H(M') =? h'
H(K, M') =? h'
(M', h) ≠ H(K, M')
= h'

A

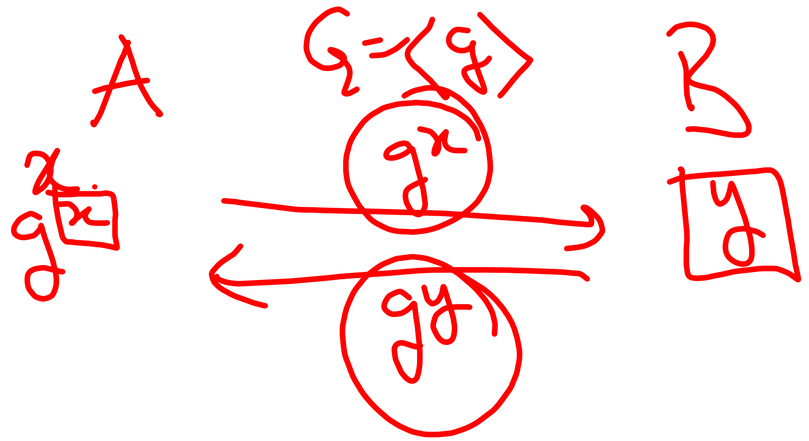
$pk \leftarrow$ B (sk)

$H(g^{xy}) \in \{0,1\}^{256}$

$Enc(pk, m) = c$ ⟶ $Dec(sk, c) = m$

Type-1 $Enc(pk, K) = c$ ⟶ $Dec(sk, c) = K$

Type-2 (DH) Key Exchange

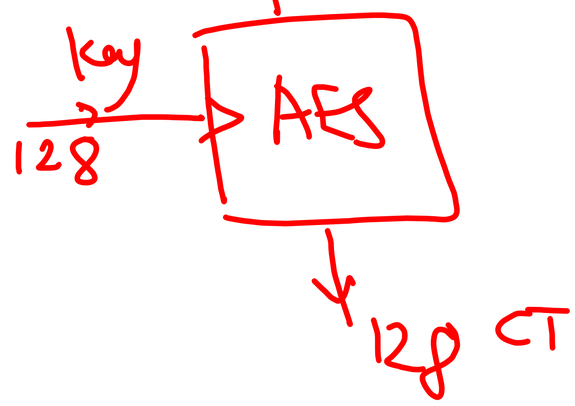


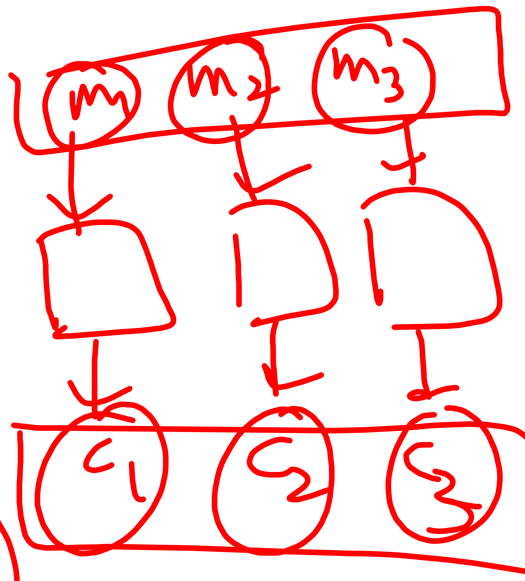
$c^* = Enc(K, m_0) / Enc(K, m_1)$

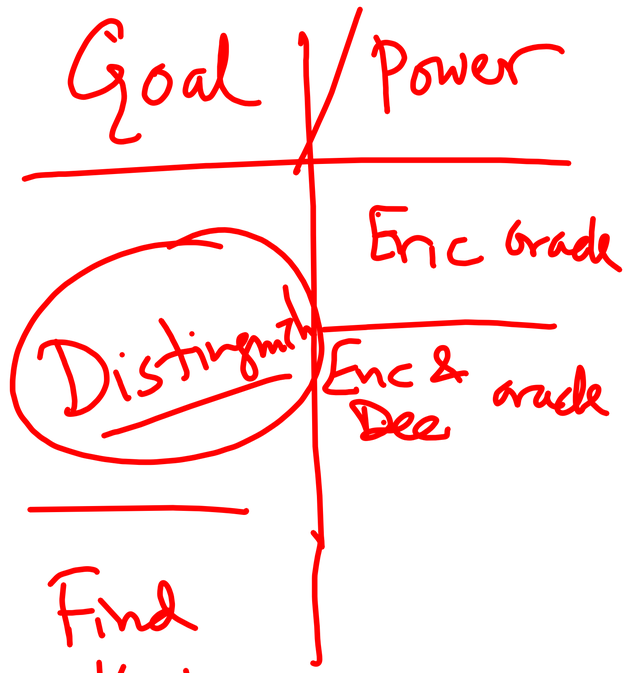
$A(c^*)$

$A(pk, c^*)$

SKE (AES/DES)







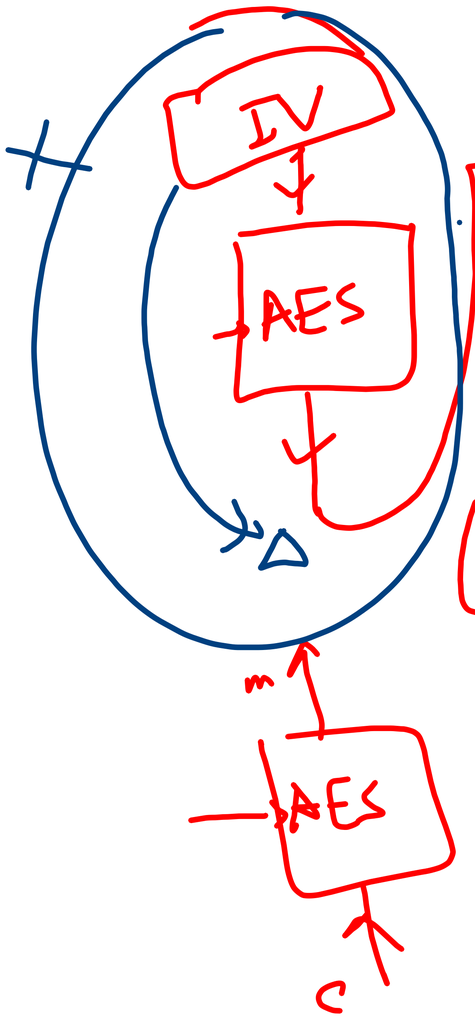
ECB ← Insecure

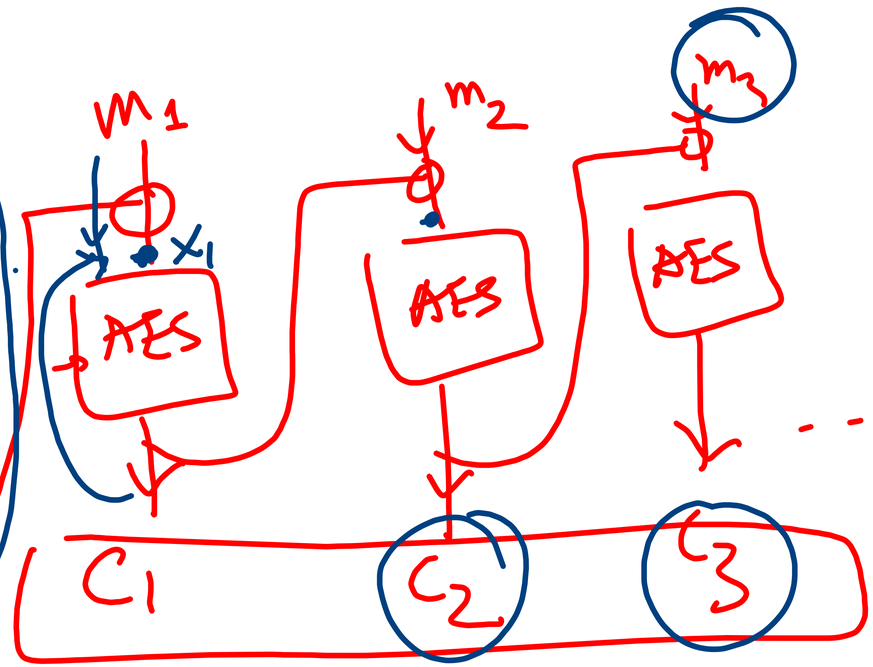
$M_0 = 0^{128}\ 0^{128}$

$M_1 = 0^{128}\ 1^{128}$

(c^*_0, c^*_1)

CBC is secure





$\Delta \oplus m_1 = x_1$

$m_1 = \Delta \oplus x_1$

$C_1^* = C_1 = C_1'$

$C_2^* = C_2 = C_2'$

C_3^*

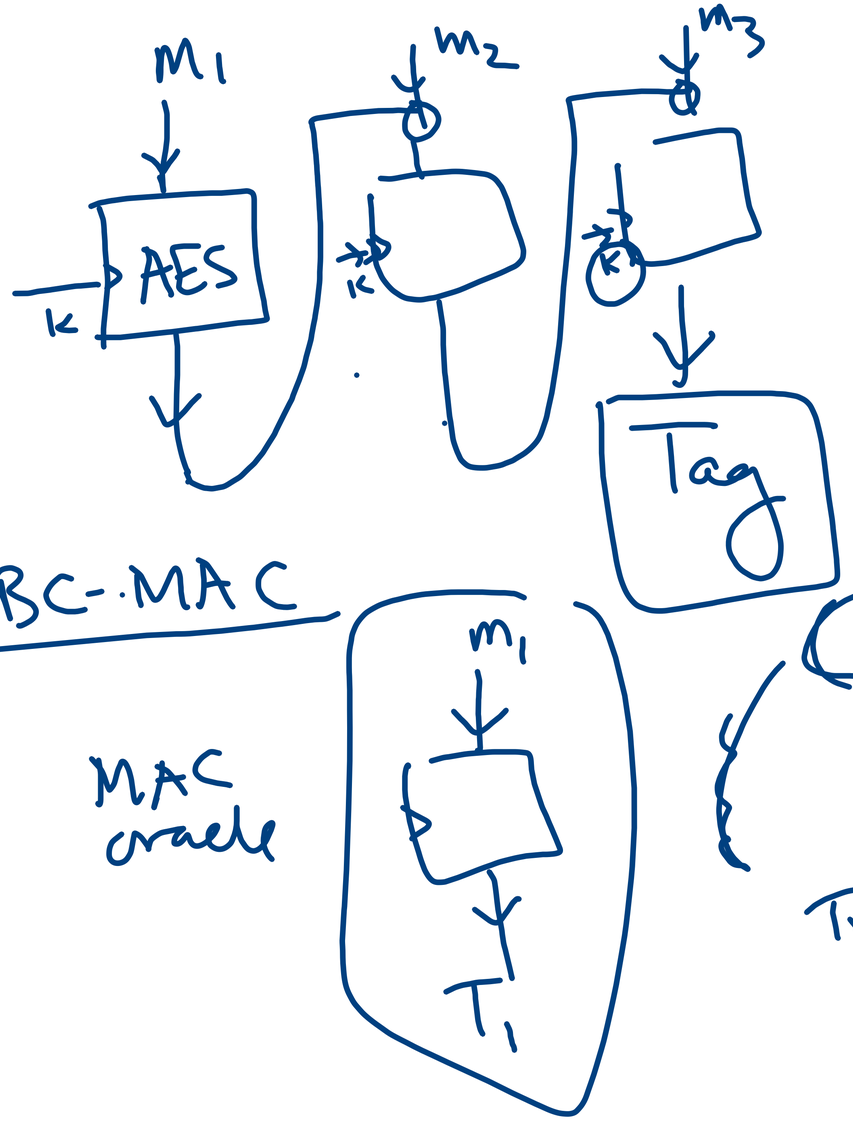
m_{10} m_{11}

M_0 0 0 1

M_1 $\begin{pmatrix} c & c_2 & c_3 \\ 0 & 1 & 0 \\ c' & c_2' & c_3' \end{pmatrix}$

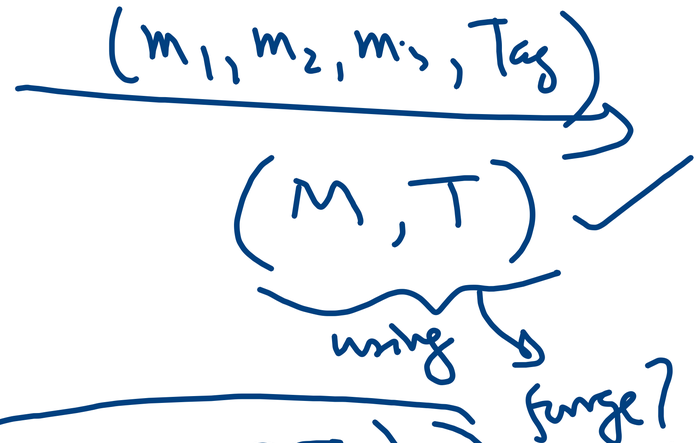
$M^* = (0\ 0\ 0) \rightarrow Enc$

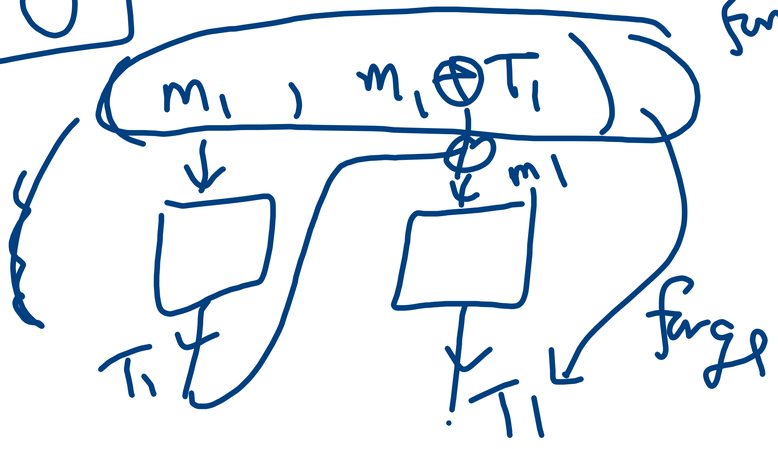
$\neq M_0, M_1$ $(c_1^*\ c_2^*\ c_3^*)$ ←



CBC-MAC

MAC oracle

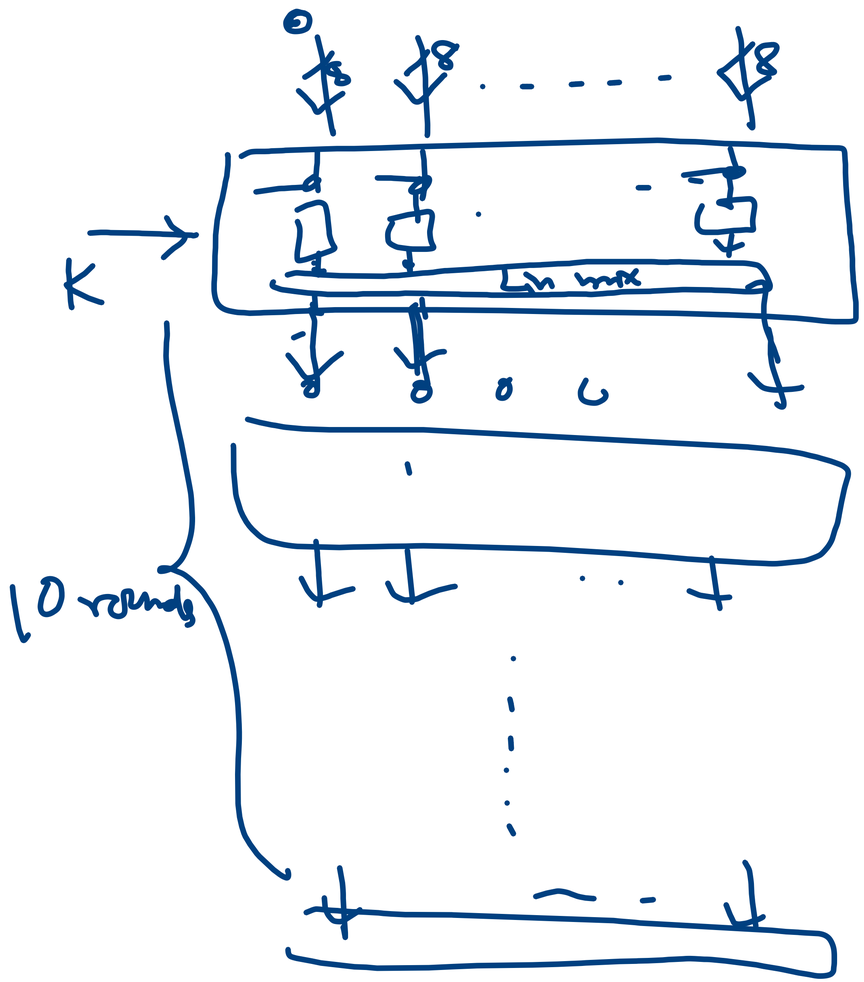


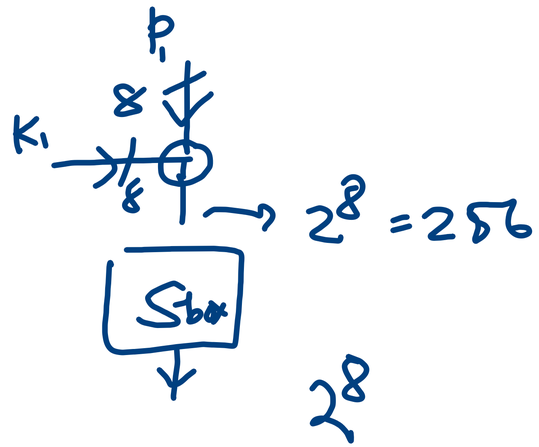


H(K, M)

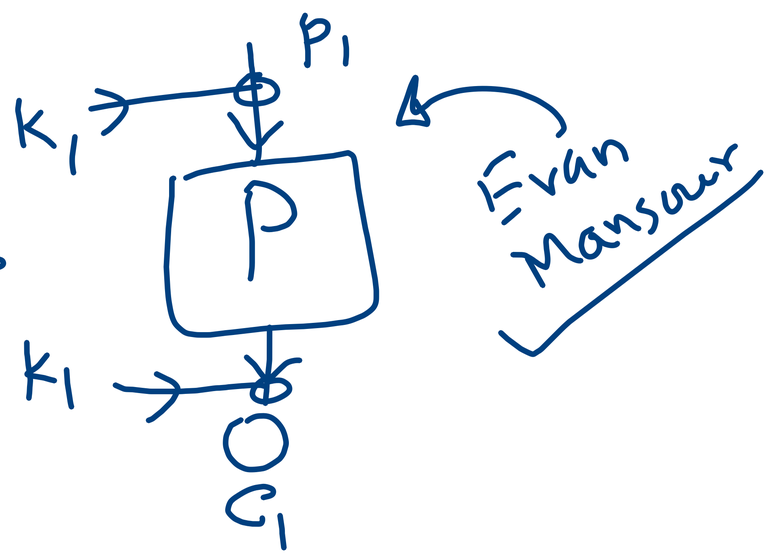
Goal	Power
forge	MAC oracle
(M^*, T^*)	(M_1, T_1) (M_2, T_2) ⋮
$M^* \neq M_1$	

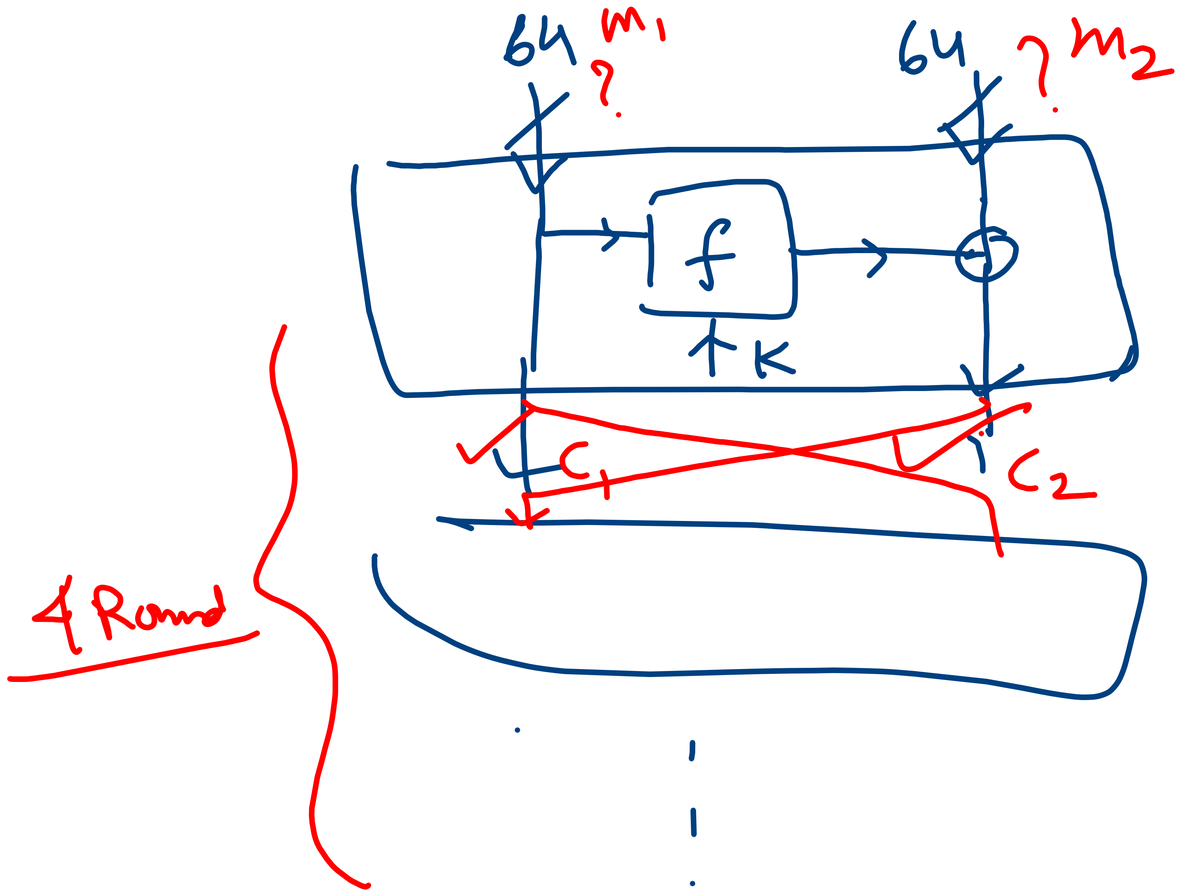
SPN

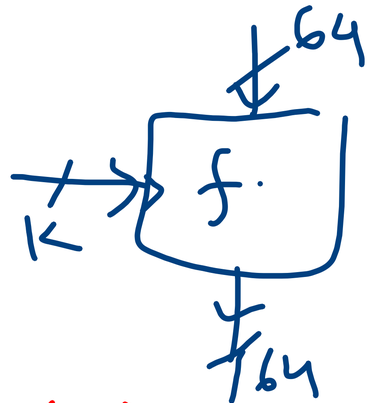




Feistel







$m_1 = C_1$

$m_2 = C_2 \oplus f_K(C_1)$

Hash function

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

$x_1, x_2, \ldots, x_q \leftarrow\$ D$

Look for Coll^n $\{H(x_1), H(x_2) \cdots, H(x_q)\}$

$\frac{q^2}{2} \approx 2^n \qquad q \approx 2^{n/2}$

Coll^n / Preimage

$y \in \{0,1\}^n$

$x_1, x_2, \cdots\cdots x_q \leftarrow\$ D$

Check if $y \in \{H(x_1) \cdots H(x_q)\}$

$q \approx 2^n$

Find a, b

$H(a,b) = g^a \cdot h^b = h'$ (given)

Hash function

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

$x_1, x_2, \ldots, x_q \leftarrow\$ D$

Look for coll^n $\{H(x_1), H(x_2) \cdots, H(x_q)\}$

$\frac{q^2}{2} \approx 2^n \qquad q \approx 2^{n/2}$

Coll^n / Preimage

$y \in \{0,1\}^n$

$x_1, x_2, \cdots\cdots x_q \leftarrow\$ D$

Check if $y \in \{H(x_1) \cdots H(x_q)\}$

$q \approx 2^n$

Find a, b

$H(a,b) = g^a \cdot h^b = h'$ (given)

$g^a \cdot h^b = h'$

$g^a = h' \cdot h^{-b}$

L_1

a_1	g^{a_1}
a_2	g^{a_2}
$\vdots$	$=$
a_q	g^{a_q}

L_2

b_1	$h' \cdot h^{-b_1}$
b_2	$h' h^{-b_2}$
$\vdots$	$\vdots$
b_q	$h' h^{-b_q}$

$q \approx \sqrt{p}$

$g^{a_i} = h' \cdot h^{-b_j}$

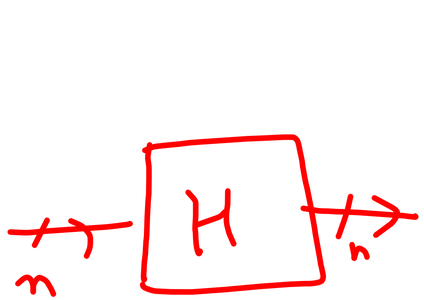
$(a_i, b_j) \mapsto h'$

Hint

L_1	L_2
x_1	y_1
x_2	y_2
x_{i_1}	$= y_{j_1}$
$\vdots$	$\vdots$
x_q	y_q

$\leftarrow$ size

$q \approx 2^{n/2}$ $\quad 2^n$

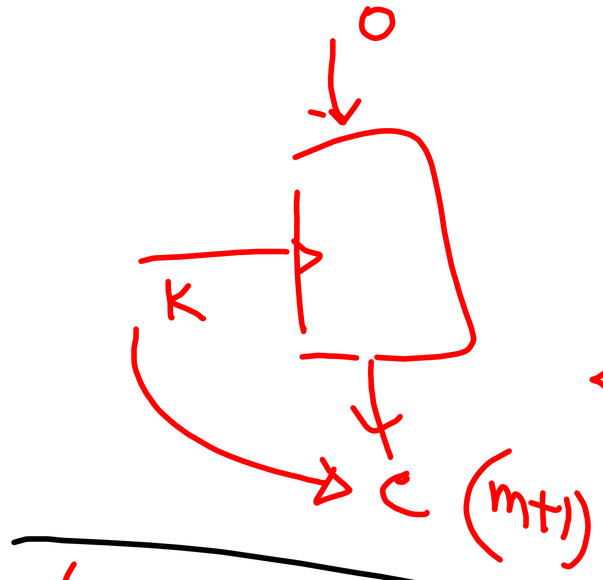


Time = q

$P(m+1) = \text{Memory}$

q

Hellman TMTO tradeoff



$(m+1)q \approx 2^n$

$mq = 2^n$