$L_{A,B,C} = \{(a,b) : A = g^a \quad B = g^b \quad C = g^{a(3+b)}$ $A = g^a \; A^{(3+b)}$ $A^3 \cdot A^b$

$L'_{A',B',C'} = \{(a',b') : A' = g^{a'} \; B' = g^{b'} \; C' = A^{(b')}\}$

$C' = (C/A^3)$ $k_a \xleftarrow{\$} Z_p$ $k_b \xleftarrow{\$} Z_p$

$\varphi_{A,B,C}(a',b')$

such that $L_{A,B,C'}(a',b')$ holds

where:

$A' = A$ $\quad a = a' \; b = b'$

$B' = B$

$C' = C/A^3$

$A' = g^{a'} \Rightarrow A = g^a$

$B' = g^{b'} \Rightarrow B = g^b$

$C' = A'^{b'} \Rightarrow C' = A^b$

$C/A^3 = A^b$

$C = A^{3+b}$

$C = g^{a(3+b)}$

Symmetric Encryption:

$k \xleftarrow{\$} K$

Alice(k, m)

$c \leftarrow Enc_k(m)$

Bob(k)

c →

$A(c) \rightarrow m^*$

$m' \leftarrow Dec_k(c)$

↑ same key

Definition:

A scheme for symmetric encryption is:

$(\quad , \quad , Dec)$

(Gen, Enc, Dec)

$k \leftarrow Gen(1^\lambda)$ $\quad k \in K$ ← key space

$m \in M$ ← message space

$c \leftarrow Enc_k(m)$ $\quad c \in C$ ← ciphertext space

$m' \leftarrow Dec_k(c)$

Satisfying properties:

Correctness:

$$\forall m, Pr[k \leftarrow Gen; c \leftarrow Enc_k(m); Dec_k(c) = m] = 1$$

(One-time) Perfect Secrecy

$$\forall m_1, m_2 \quad \{k \leftarrow Gen(1^\lambda) : Enc_k(m_1)\} \approx \{k \leftarrow Gen(1^\lambda) : Enc_k(m_2)\}$$

(Shannon secrecy)

$$\forall_{m', c_1} D : Pr[k \leftarrow Gen, m \in D; m = m' \mid Enc_k(m) = c] = Pr[m \in D; m = m']$$

One time pad:

$Gen(1^\lambda)$: $k \xleftarrow{\$} \{0,1\}^\lambda$

$Enc_k(m)$: $m \in \{0,1\}^\lambda$ $\quad c = m \oplus k$

$Dec_k(c)$: $m = k \oplus c$

Correctness

$k \oplus c = k \oplus (k \oplus m)$

Alice → m_1, m_2

$c_1 = Enc_k(m_1)$

$c_2 = Enc_k(m_2)$

Bob → "oh yeah, m_1"

$k \leftarrow m_1 \oplus c$

$A(c_1, c_2, m_1)$

$k \leftarrow m_1 \oplus c$

$m_2 \leftarrow c \oplus k$

Multi-message secrecy:

$\forall\ m_1, m_2, \ldots m_{q(\lambda)}, m'_1, m'_2, \ldots m'_{q(\lambda)}$. (for some $q = \text{poly}(\lambda)$)

$$\{K \leftarrow Gen(1^\lambda) : (Enc_K(m_1), Enc_K(m_2), \ldots Enc_K(m_{q(\lambda)}))\}$$
$$\approx \{K \leftarrow Gen(1^\lambda) : (Enc_K(m'_1), \ldots Enc_K(m'_{q(\lambda)}))\}$$

Semantic Security: (IND-CPA1, IND-CPA2, IND-CCA)

$$Pr\left[k \xleftarrow{\$} K,\ m_0, m_1 \leftarrow A^{Enc_K(\cdot)}(1^\lambda),\ b \xleftarrow{\$} \{0,1\},\ b' \leftarrow A_2^{Enc_K(\cdot)}(Enc_K(m_b));\ b = b'\right] = \frac{1}{2} + negl(\lambda)$$

Construction of Multi message security: using PRF $f_K(x)$

Assume $f_K(x)$ is a PRF

$Gen(1^\lambda)$: $K \xleftarrow{\$} \{0,1\}^\lambda$

$Enc_K(m)$: $r \xleftarrow{\$} \{0,1\}^\lambda$

output $(r, m \oplus f_K(r)) = c$

$Dec_K(c = (r, c'))$: $m = f_K(r) \oplus c'$

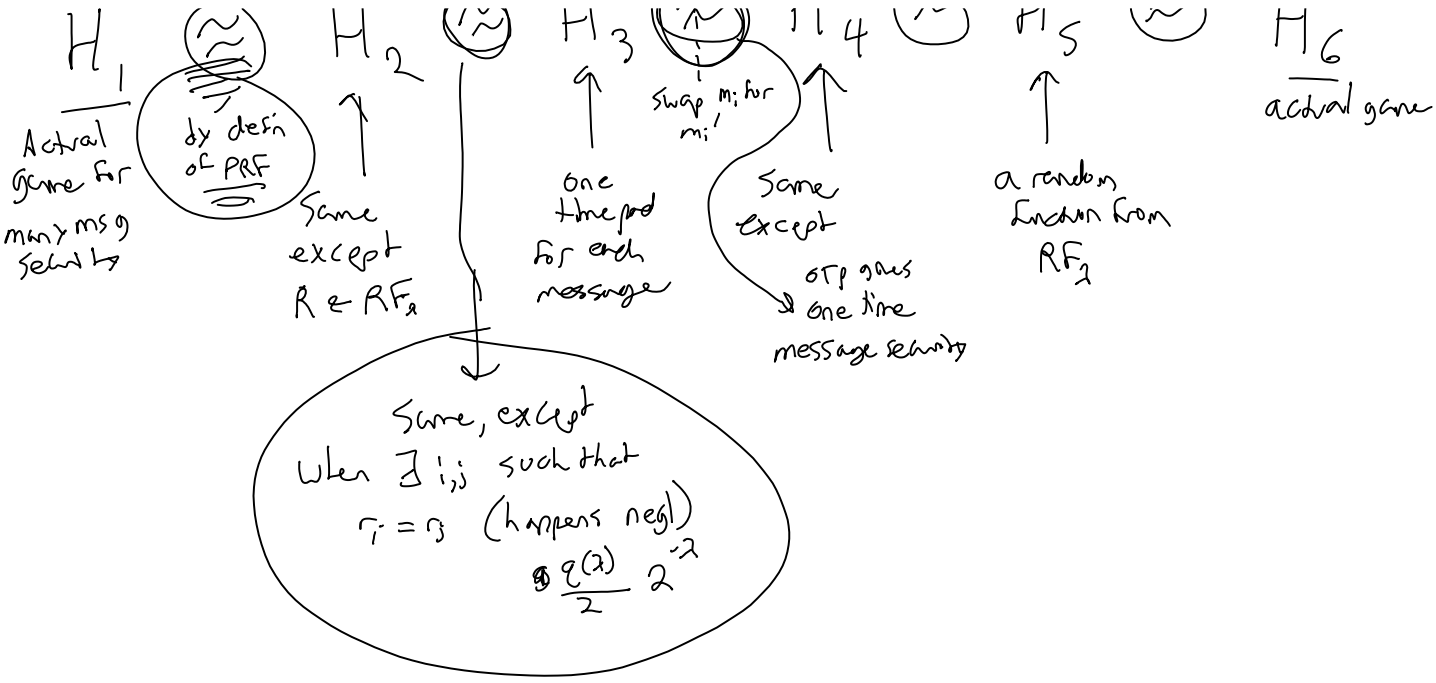
output m'

Prove this satisfies many message security:

Approach: Hybrid games

$$\underbrace{\{K \leftarrow Gen : (Enc_K(m_1), \ldots Enc_K(m_q))\}}_{H_1} \approx \underbrace{\{K \leftarrow Gen : (Enc_K(m'), Enc_K(m'q))\}}_{H_6}$$

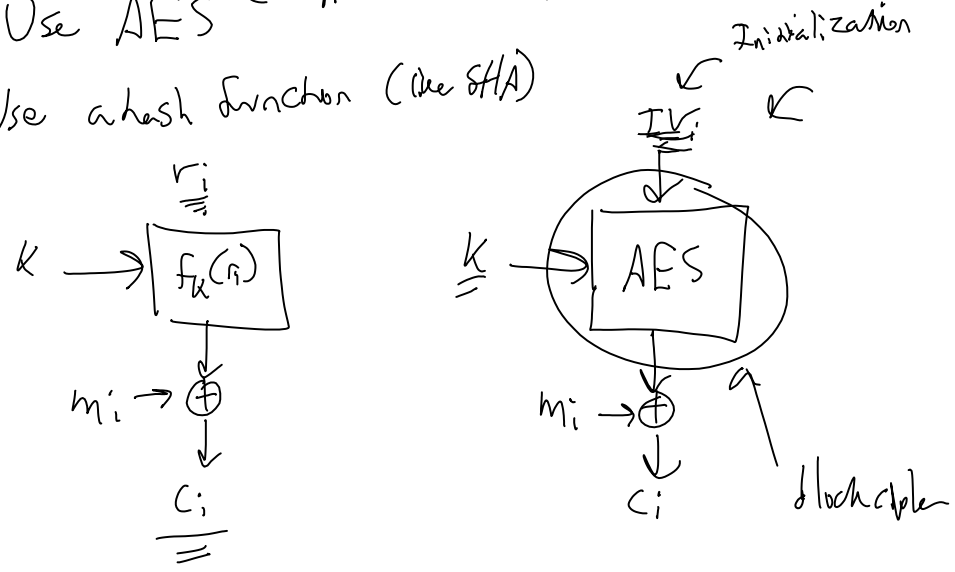
Hybrid games



Block Ciphers and modes of operation

Where do we get a PRF:

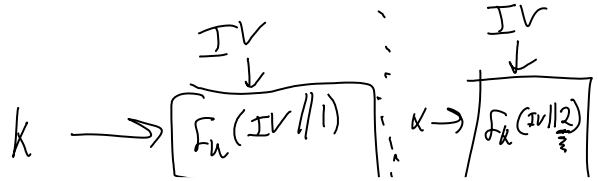
- Construction from last time
- Use AES ← Advanced Encryption Standard
- Use a hash function (like SHA)

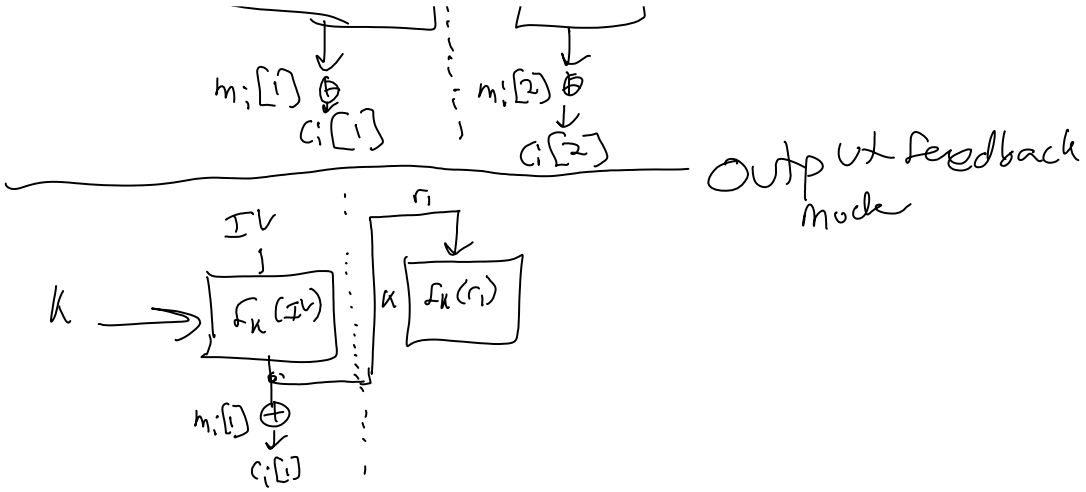


How to evaluate block ciphers:

- Statistical cryptanalysis

Counter mode
CTR




$m_i[1]$
$c_i[1]$
$m_i[2]$
$c_i[2]$
Output feedback mode
IV
r_1
K
$f_K(IV)$
K
$f_K(r_1)$
$m_i[1]$
$c_i[1]$