Symmetric Encryption

Tuesday, October 1, 2019 10:55 AM

- One message security
- multi-message security
- adaptive (ind-cpa)
  indistinguishability
  under chosen plaintext attack.

Syntax of encryption

(Gen, Enc, Dec)

- $k \leftarrow Gen(1^\lambda)$
- $c \leftarrow Enc_k(m)$
- $m' \leftarrow Dec_k(c)$

— Correctness: $\forall m, k \leftarrow Gen(1^\lambda)$, $m = Dec_k(Enc_k(m))$

- One message

$$\forall m_0, m_1 \quad \{k \leftarrow Gen(1^\lambda) : Enc_k(m_0)\} \approx_c \{k \leftarrow Gen(1^\lambda) : Enc_k(m_1)\}$$

Solution: one time pad

Problems $c_A = k \oplus m_A$

$c_B = k \oplus m_B$

$c_C = k \oplus$

A takes $c_A \oplus$ "Hi" $\rightarrow k$

- multi-message security $\ell = poly(\lambda)$

$$\forall m_0, m_1, \ldots m_\ell, m_0', m_1', \ldots m_\ell'$$

$$\{k \leftarrow Gen, (Enc_k(m_1), \ldots Enc_k(m_\ell))\} \approx_c \{k \leftarrow Gen, (Enc_k(m_1'), \ldots Enc_k(m_\ell'))\}$$

- to satisfy this,

Claim: Enc MUST be non-deterministic even for given k

If det., then $c_0 = c_1$

$m_0 \oplus k = c_0$

$m_1 \oplus k = c_1$

$c_0 \oplus c_1 = m_0 \oplus k \oplus k \oplus m_1$

$= m_0 \oplus m_1$

— "A" , "B" $\rightarrow (c_0, c_1)$

Proof: $m_0 = 0$ $m_1 = 1$

$m_0' = "0"$ $m_1' = "1"$ $\rightarrow (c_0', c_1')$ $c_0' \neq c_1'$

Multi-message Encryption from PRF

Assume $f: \{0,1\}^\lambda \times \{0,1\}^\lambda \rightarrow \{0,1\}^\lambda$

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

$Enc_k(m) \rightarrow r \xleftarrow{\$} \{0,1\}^\lambda$

$c = (r, m \oplus f_k(r))$

$Dec_k(c) \rightarrow$ parse c as (r, c')

$m' \leftarrow c' \oplus f_k(r)$

Claim: This scheme satisfies multi-message security

Proof: by hybrid games (for later)

IND-CPA (also known as semantic security) "adaptive"

$\forall \mathcal{A}, \{k \leftarrow Gen; m_0, m_1 \leftarrow \mathcal{A}^{Enc_k(\cdot)}(1^\lambda) : Enc_k(m_0)\}$

$\approx \{k \leftarrow Gen; m_0, m_1 \leftarrow \mathcal{A}^{Enc_k(\cdot)}(1^\lambda) : Enc_k(m_1)\}$

Success at Counterexample:

~~Attempt:~~

$Gen(1^\lambda) = k_0 \xleftarrow{\$} \{0,1\}^\lambda$, $k_1 \xleftarrow{\$} \{0,1\}^\lambda$

$Enc((k_0, k_1), m) = r \xleftarrow{\$} \{0,1\}^\lambda$

$\begin{cases} (f_{k_0}(r) \oplus m, k_1) & \text{if } m \neq k_1 \\ (k_0, k_1) & \text{if } m = k_1 \end{cases}$

Claim: If Π is many-message secure, and Π is IND-CPA secure

$\forall m_0, \dots m_l,$ $m_0', \dots m_l'$, wlog. suppose $l=1$ $\quad m_0 = m_1$, $m_0' \neq m_1'$

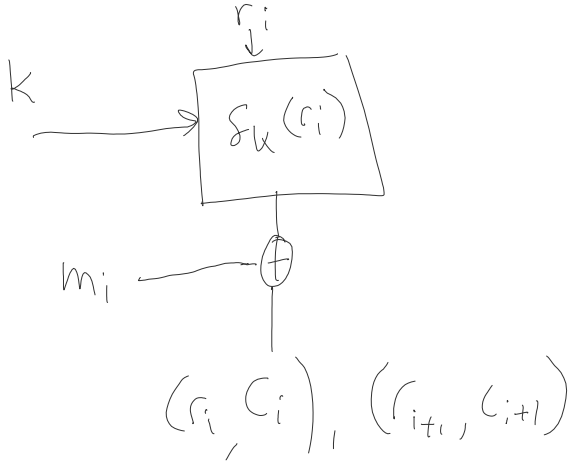
$H_0 = \{ k \xleftarrow{\$} \{0,1\}^\lambda;\ r_0 \xleftarrow{\$} \{0,1\}^\lambda, r_1 \xleftarrow{\$} \{0,1\}^\lambda : \} \approx_c H_5 = \{ k \xleftarrow{\$} \{0,1\}^\lambda, r_0' \xleftarrow{\$} \{0,1\}^\lambda, r_1 \xleftarrow{\$} \{0,1\}^\lambda : \}$

$(r_0, m_0 \oplus f_k(r_0)), (r_1, m_1 \oplus f_k(r_1)) \qquad (r_0', m_0' \oplus f_k(r_0')), (r_1', m_1' \oplus f_k(r_1'))$

$H_0 \approx_c H_1 \approx_c H_2 \approx_c H_3 \approx_c H_4 \approx_c H_5$

- H_1: replace f_k with RO
- H_2: replace RO with another pad... random ciphertext even in case $r_0 = r_1$
- H_3: replace m_0 with m_0', m_1 with m_1'
- H_4: replace RO back with f_k

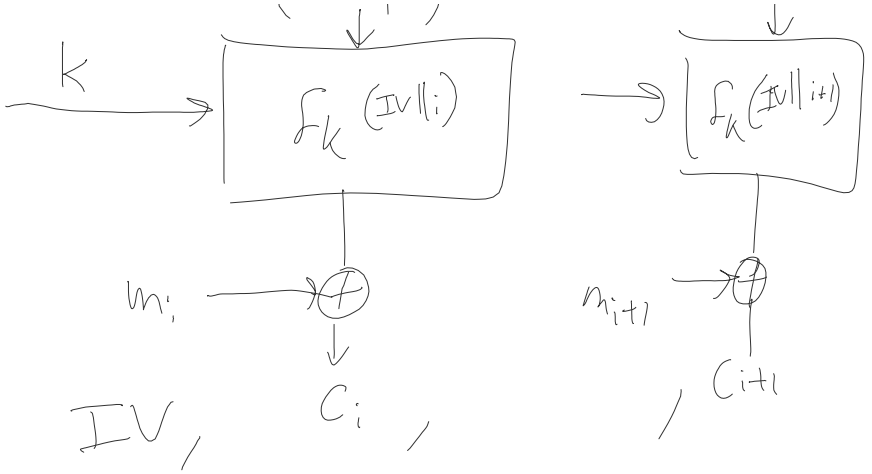
Modes of operation for ciphers



? mode

Counter mode $\boxed{IV}$ or Nonce Initialization Vector

$(IV \| i)$ $\qquad$ $(IV \| i+1)$

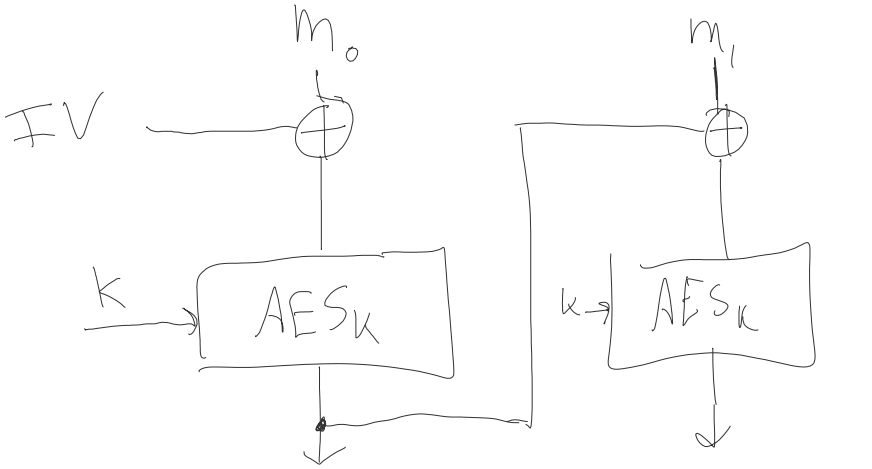


IV, C_i, /

Trapdoor pseudorandom permutation

AES $\frac{f_k(x)}{f_k^{-1}(x)}$

Cipher block chaining:

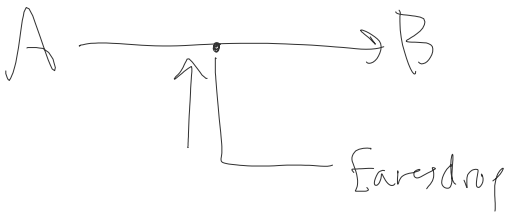


IV, C_0, C_1, C_2, ...

√ parallel decryption

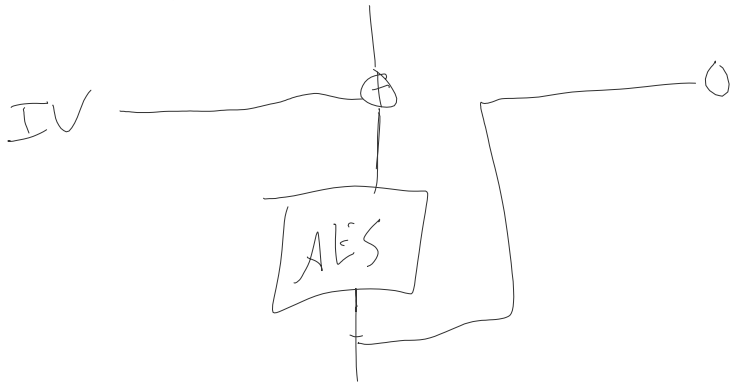
X parallel encryption

v self synchronizing



predictable

m_0 = "Content: html" m_1 = "...



$(IV, C_0, \ldots) = File$

A

$IV' = IV \oplus m_0 \oplus m_0'$

$(IV', C_1, C_0, \ldots) = File'$

m_0' : "stp put wallet.dat; Content-type"