Recap :

Sec. Def. for private key enc :

(Enc, Dec) is secure

if for all poly time A,

$\Pr[A \text{ wins many-time sec. game}] \leq 1/2 + \ldots$

C $\qquad\qquad\qquad\qquad$ A

$k \leftarrow \mathcal{K}, \; b \leftarrow \{0,1\}$

$\xleftarrow{\quad m_{i0},\; m_{i1} \quad}$

$ct_i \leftarrow Enc(k, m_{ib})$

$\xrightarrow{\quad ct_i \quad}$

$\xleftarrow{\quad b' \quad}$

wins if $b = b'$

[Goldwasser - Micali 84]

Good news: If (Enc, Dec) satisfies above def, then no adversary learns anything new from the ciphertexts.

Existence of secure (Enc, Dec)

$\Downarrow$

Existence of secure one way functions

$\Downarrow$

$P \neq NP$

Goal of today's lecture :

Pseudorandom Functions

$\downarrow$

secure private key enc.

Pseudorandom Functions (PRFs) :

Det. keyed function s.t.

F_k (for random k) behaves like

a truly random function.

Why PRFs are good starting point for building secure encryption ?

Theory : OWFs $\Rightarrow$ PRFs

$\therefore$ Existence of OWFs is necessary and sufficient for existence of sec. enc.

Practice : Good candidate PRFs, extensively cryptanalysed.

AES

Motivating scenario : WiFi protocols

$$F : \mathcal{K} \times \mathcal{X} \rightarrow \mathcal{Y}$$

$$\mathcal{K} = \mathcal{X} = \mathcal{Y} = \{0,1\}^n$$

Number of keys $= 2^n$

Number of functions $\mathcal{X} \rightarrow \mathcal{Y}$ $= |\mathcal{Y}|^{|\mathcal{X}|}$

$= 2^{n2^n}$

Security Game for PRFs :

$\underline{C}$ $\qquad\qquad\qquad\qquad$ $\underline{A}$

$b \leftarrow \{0,1\}$

$k \leftarrow \mathcal{K}$

$f_0(\cdot) \equiv F(k, \cdot)$

$f_1(\cdot)$: unif. random function

$$\xleftarrow{\quad x_i \quad}$$

$$\xrightarrow{\quad f_b(x_i) \quad}$$

poly

$$\xleftarrow{\quad b' \quad}$$

wins if $b = b'$

Fun with PRFs :

→ Extending co-domain of PRF

Given : $F : \mathcal{K} \times \mathcal{X} \rightarrow \mathcal{Y}$

$\{0,1\}^n$

Construct : $F' : \mathcal{K} \times \mathcal{X} \rightarrow \{0,1\}^{2n}$

using F.

Candidate 1 :

$$F'(k, x) = F(k, x), F(k, x \oplus 1^n)$$

Candidate 2:

$$F'(k,x) = F(k,x),\ F(k, F(k,x))$$

A1: Construct a provably sec. PRF $F' : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{2n}$, assuming given PRF $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$.

C3: $F'(k,x) = F(k,x),$

$F(k, x) \oplus k$ X

C4: $F'(k,x) = F(k,x),$?

$F(k \oplus F(k,x), x)$

C5: $F'(k,x) = F(k,x),\ F(k, x \oplus F(k,x))$ X

Secure encryption using secure PRFs:

Goal: Encryption scheme with

$\mathcal{K} = \mathcal{M} = \{0,1\}^n$

Given: PRF $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$

injective

Attempts:

1. $\mathrm{Enc}(k, m) = F(k, m)$ Not sec.

$\mathrm{Dec}(k, ct) = F^{-1}(k, ct)$ det. enc.

2. $\mathrm{Enc}(k, m; r) = (r \oplus F(k, m), r)$

$\mathrm{Dec}(k, ct)$

3. $\mathrm{Enc}(k, m; r) = (r, F(k, r) \oplus m)$

$\mathrm{Dec}(k, (ct_1, ct_2)) = ct_2 \oplus F(k, ct_1)$

Secure encryption, unbdd. message space:

Goal: Encryption scheme with

$$\mathcal{M} = \{0,1\}^{tn}$$

1. $Enc(k, m_1 \ldots m_t)$:

$$(r, m_1 \oplus F(k,r), m_2 \oplus F(k,r), \ldots, m_t \oplus F(k,r))$$

Not secure

$$(m_1, m_2), (m_1, m_2 \oplus 1^n)$$

$$\longleftarrow$$

$$(r, ct_2, ct_3)$$

$$\longrightarrow$$

$$ct_2 \oplus ct_3 \stackrel{?}{=} m_1 \oplus m_2$$

A 2: Weak PRFs :

C　　　　　　　　　　A

f_0, f_1, b

$\longleftarrow$

unif. random x_i

$\xrightarrow{x_i,\ f_b(x_i)}$

$\xleftarrow{b'}$

Show that weak PRFs $\Rightarrow$ secure enc.

In Practice :

PKCS v 1.5

Variant of PKCS v 1.5 Enc. Standard:

Uses $F : \{0,1\}^{128} \times \{0,1\}^{128} \longrightarrow \{0,1\}^{128}$

in bytes

$Enc(k, m)$:

$m = m_1 \, m_2 \, \cdots \, m_t$

if t is not multiple of