

Recap :

Sec. Def. for private key enc :

(Enc, Dec) is secure

if for all poly time A ,

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

C

A

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

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

m_{i0}, m_{i1}

```
graph LR; C[C] -- "k, b" --> A[A]; A -- "m_{i0}, m_{i1}" --> C; C -- "ct_i" --> A; A -- "b'" --> C; A --- Win[wins if b = b'];
```

ct_i

b'

wins if $b = b'$

Good news : If (Enc, Dec) satisfies

[Goldwasser -
Micali 84]

above def, then no
adversary learns anything
new from the ciphertexts.

Existence of secure (Enc, Dec)



Existence of secure one way functions



$P \neq NP$

Goal of today's lecture :

Pseudorandom Functions



secure private key enc.

Pseudorandom Functions (PRFs) :

Def. 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

$$F : K \times X \rightarrow Y$$

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

$$\text{Number of keys} = 2^n$$

$$\begin{aligned} \text{Number of functions } X \rightarrow Y &= |Y|^{|X|} \\ &= 2^{n \cdot 2^n} \\ &= 2^{2^{n+1}} \end{aligned}$$

Security Game for PRFs :

C

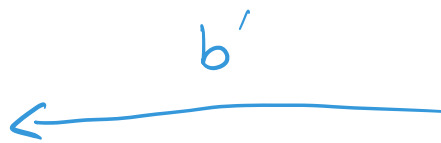
$$b \leftarrow \{0, 1\}$$

$$k \leftarrow \mathcal{K}$$

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

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

A



wins if
 $b = b'$

Fun with PRFs :

→ Extending co-domain of PRF

$$\begin{array}{ccc} \text{Given: } F: \mathcal{K} \times \mathcal{X} & \rightarrow & \mathcal{Y} \\ & \swarrow \uparrow \nearrow & \\ & \{0,1\}^n & \end{array}$$

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 $F': \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^{2n}$

assuming given PRF $F: \{0,1\}^n \times$

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

↓

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

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

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

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

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

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

Secure encryption using secure PRFs:

Goal: Encryption scheme with

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

Given: PRF $F: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$
↑
injective

Attempts:

1. $\text{Enc}(k, m) = F(k, m)$ Not sec.
 $\text{Dec}(k, ct) = F^{-1}(k, ct)$ det. enc.

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

3. $\text{Enc}(k, m; r) = (r, F(k, r) \oplus m)$
 $\text{Dec}(k, (ct_1, ct_2)) = ct_2 \oplus F(k, ct_1)$

Secure encryption, unbdd. message space:

Goal: Encryption scheme with

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

1. $\text{Enc}(k, m_1, \dots, m_t) :$

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

Not secure

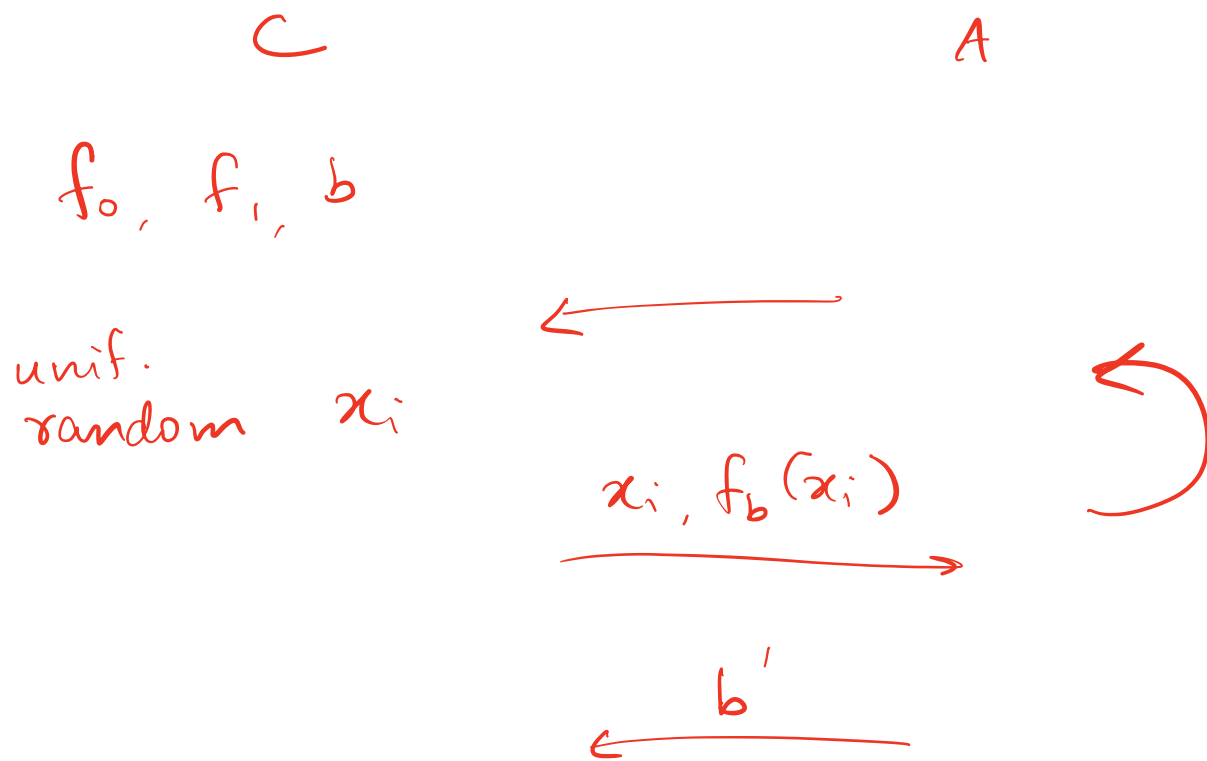
$$(m_1, m_2), (m_1, m_2 \oplus 1^n)$$

$$(\gamma, ct_2, ct_3)$$

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

$$m_1 \oplus m_2$$

A 2: Weak PRFs :



Show that weak PRFs \Rightarrow secure enc.

In Practice :

PKCS v 1.5

Variant of PKCS v 1.5 Enc. Standard:

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

$\text{Enc}(k, m):$

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

if t is not multiple of