Chosen Plaintext Attacks

HW2 due
HW3 out !

~~one-time security~~

Def: Encryption scheme has CPA security (security against <u>c</u>hosen <u>p</u>laintext <u>a</u>ttacks) if:

$$\boxed{\begin{array}{l} k \leftarrow \text{KeyGen} \\ \underline{\text{CHALLENGE}(m_L, m_R):} \\ \qquad \text{ret } \text{Enc}(k, m_L) \end{array}} \approx \boxed{\begin{array}{l} k \leftarrow \text{KeyGen} \\ \underline{\text{CHALLENGE}(m_L, m_R):} \\ \qquad \text{ret } \text{Enc}(k, m_R) \end{array}}$$

How to achieve CPA security?

Idea: use a PRP :

$$x \xrightarrow{F(k,x)} y \xrightarrow{F^{-1}(k,y)} x$$

Problem: Not CPA-secure encryption

what happens when same msg is "encrypted" twice?

Same "ciphertext" ⟹ Adv learn whether same thing encrypted twice

Claim: Scheme $\text{Enc}(k,m) = F(k,m)$ where F is a PRP does <u>not</u> have CPA security

Attack: arbitrary $m_1 \neq m_2$

left

right

$$\begin{array}{l} c_1 = \text{CHALLENGE}(m_1, m_1) \\ c_2 = \text{CHALLENGE}(m_1, m_2) \\ \text{return } c_1 \overset{?}{=} c_2 \end{array}$$

$c_1 = c_2$
$= F(k, m_1)$

$c_1 = F(k, m_1)$
$\neq c_2 = F(k, m_2)$

Sanity check: If Encrypting same ptxt twice gives ctxt ⟹ CANNOT be CPA-secure

Challenge: Encrypt m to many possible ctxts, Dec must work for all these ctxts !

Idea: encrypt 1st msg m_1 as $F(k,1) \oplus m_1$

2nd msg m_2 $F(k,2) \oplus m_2$

$\vdots$

PRF security ⇒ these look uniform, independent

but this requires keeping state (# of msgs sent / received)

Better: choose random PRF input (r)

use F(k,r) as OTP

[slides]

About the proof: Prove that this scheme has CPA sec.

Start here

```
$k \leftarrow \{0,1\}^\lambda$
CHALLENGE($m_L$, $m_R$)
    $r \leftarrow \{0,1\}^\lambda$
    $x := F(k, m_L)$
    ret $(r, x)$
```

$\approx \cdots \approx$

"half-way"

```
CHALLENGE($m_L$, $m_R$)
    $r \leftarrow \{0,1\}^\lambda$
    $x \leftarrow \{0,1\}^\lambda$
    return $(r, x)$
```

If I can get "halfway" in security proof, then I can get the whole way

Def: Pseudorandom ciphertexts (CPA$)

```
$k \leftarrow \text{KeyGen}$
CHALLENGE($m$):
    ret Enc($k,m$)
```

$$\approx$$

```
CHALLENGE($m$):
    $c \leftarrow \mathcal{C}$
    ret $c$
```

Claim: CPA$ security $\Rightarrow$ CPA security