Chosen Plaintext Attacks

HW2 due
HW3 out !

~~one-time security~~

Def: Encryption scheme has CPA security (security against chosen plaintext attacks) if:

$k \leftarrow KeyGen$ CHALLENGE(m_L, m_R): ret $Enc(k, m_L)$	$\approx\approx$	$k \leftarrow KeyGen$ CHALLENGE(m_L, m_R): ret $Enc(k, m_R)$

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 $Enc(k,m) = F(k,m)$ where F is a PRP does not have CPA security

Attack: arbitrary $m_1 \neq m_2$

$C_1 = CHALLENGE(m_1, m_1)$
$C_2 = CHALLENGE(m_1, m_2)$
return $C_1 \stackrel{?}{=} C_2$

left: $C_1 = C_2 = F(k, m_1)$

right: $C_1 = F(k, m_1) \neq C_2 = F(k, m_2)$

Sanity check: If Encrypting same ptxt twice gives ctxt $\Longrightarrow$ 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 $\Rightarrow$ 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)

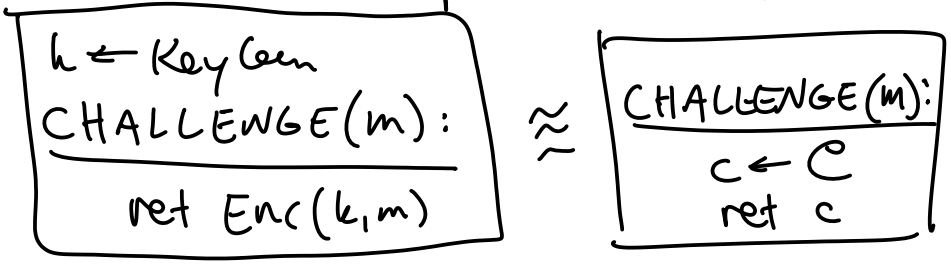
$r \leftarrow \{0,1\}^\lambda$

$x \leftarrow \{0,1\}^\lambda$

return (r, x)

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

Def: Pseudorandom ciphertexts (CPA$)



Claim: CPA$ security ⇒ CPA security