PSEUDORANDOM FUNCTIONS

Recall: $Enc(k, m) = G(k) \oplus m$

ONE-TIME SECURE

$|k| << |m|$

In particular: $c_1 = G(k) \oplus m_1$

$c_2 = G(k) \oplus m_2$ $\quad c_1 \oplus c_2 = m_1 \oplus m_2$

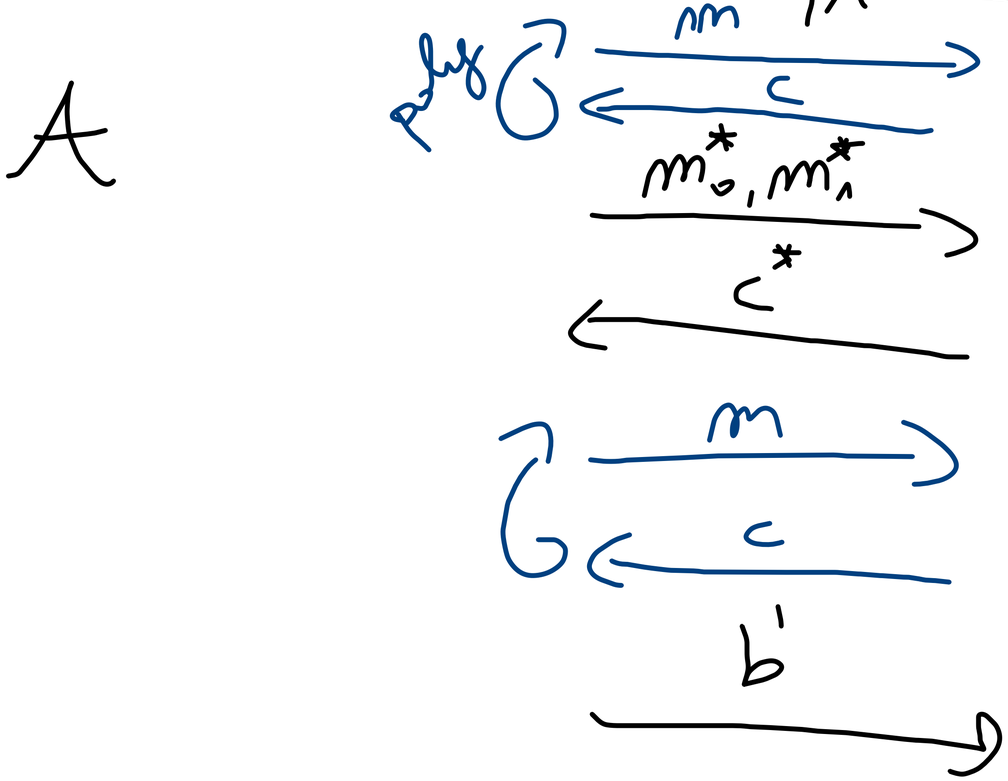
What if A knows m_1? → Chosen-Plaintext Attack.

MANY-TIME SECURITY ≡ CPA SECURITY.

Def. $\Pi = (Enc, Dec)$ is CPA secure if

$$GAME^{cpa}_{\Pi,A}(\lambda, 0) \approx_c GAME^{cpa}_{\Pi,A}(\lambda, 1)$$

$GAME^{cpa}_{\Pi,A}(\lambda, b)$



C

$k \leftarrow\$ K$

$c^* \leftarrow Enc(k, m_b^*)$

$c \leftarrow Enc(k, m)$

↳ Enc tosses coins !!!

$Enc(k, m; r)$

Next target: CPA SKE in MINICRYPT.

1) PRG ⟹ PRF ⟸ AES!

Pseudorandom function

G(k)

x	y
0…0	$
0…1	$
⋮	⋮
1…1	$

$F_k(x) = y$; $\{F\}\{F_k\}_k$

2) PRF ⇒ CPA SKE

$Enc(k, m) = (c_0, c_1)$

$c_0 = r \xleftarrow{\$} U_n$

$c_1 = F_k(r) \oplus m$

$Dec(k, (c_0, c_1)) = F_k(c_0) \oplus c_1$

How to decrypt a ransomware CTX ??

- Maybe r is PUBLIC !
- Maybe can recover r using k !