Using block ciphers

Modes of operation: one time key

example: encrypted email, new key for every message.

Using PRPs and PRFs

Goal: build "secure" encryption from a secure PRP (e.g. AES).

This segment: **one-time keys**

1. Adversary's power:

   Adv sees only one ciphertext (one-time key)

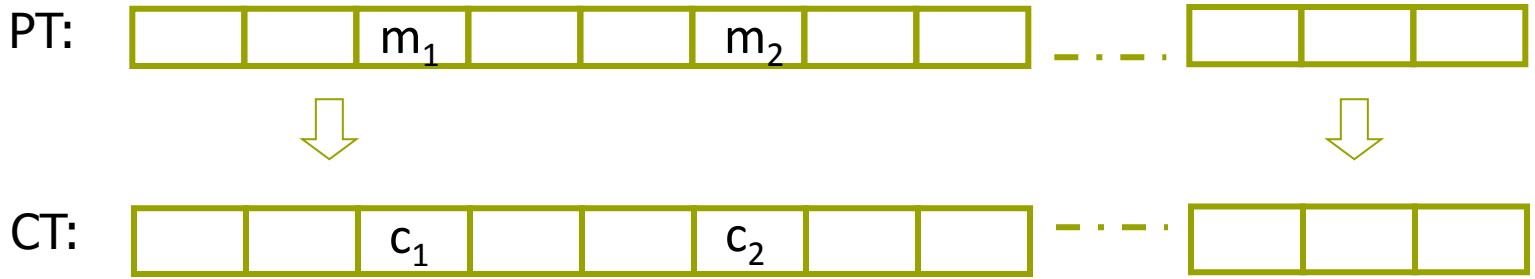
3. Adversary's goal:

   Learn info about PT from CT (semantic security)

Next segment: many-time keys (a.k.a chosen-plaintext security)

Incorrect use of a PRP

Electronic Code Book (ECB):



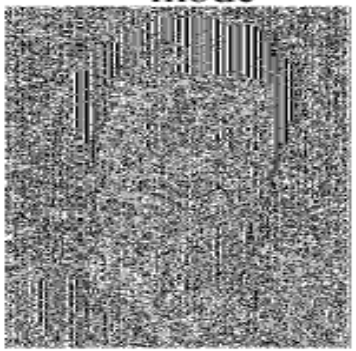
<u>Problem</u>:

– if $m_1=m_2$ then $c_1=c_2$

In pictures

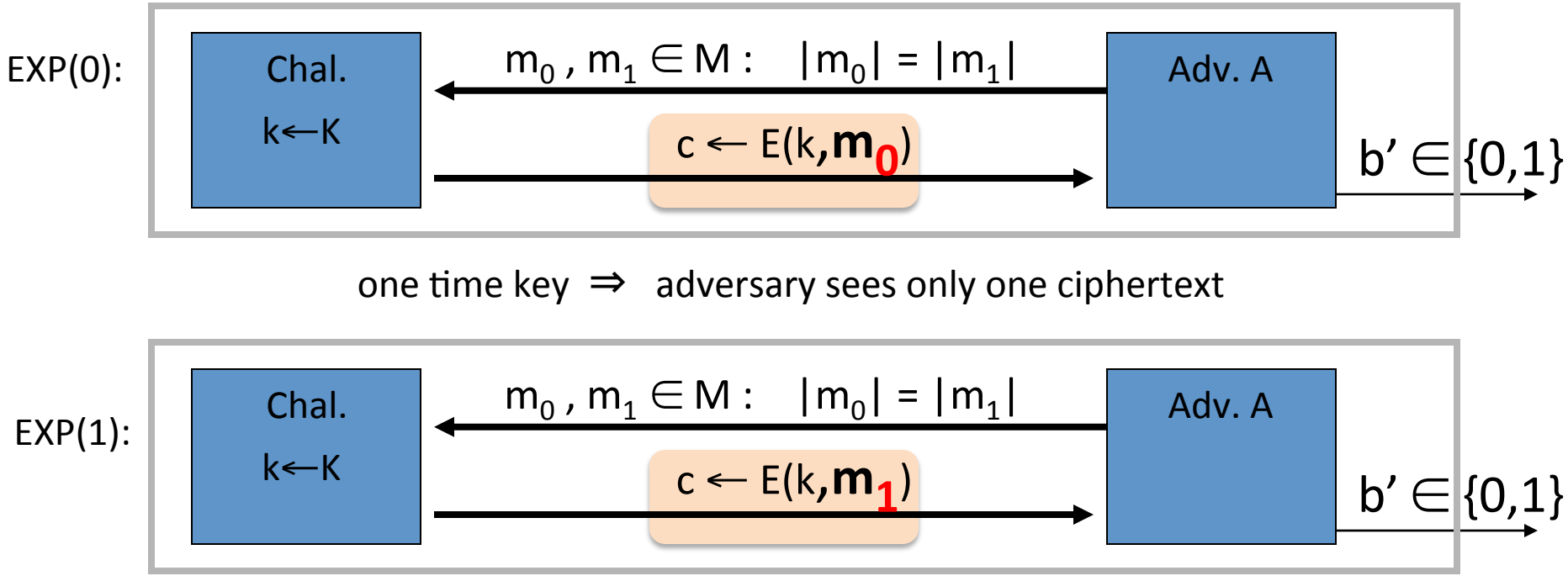
An example plaintext

Encrypted with AES in ECB mode



(courtesy B. Preneel)

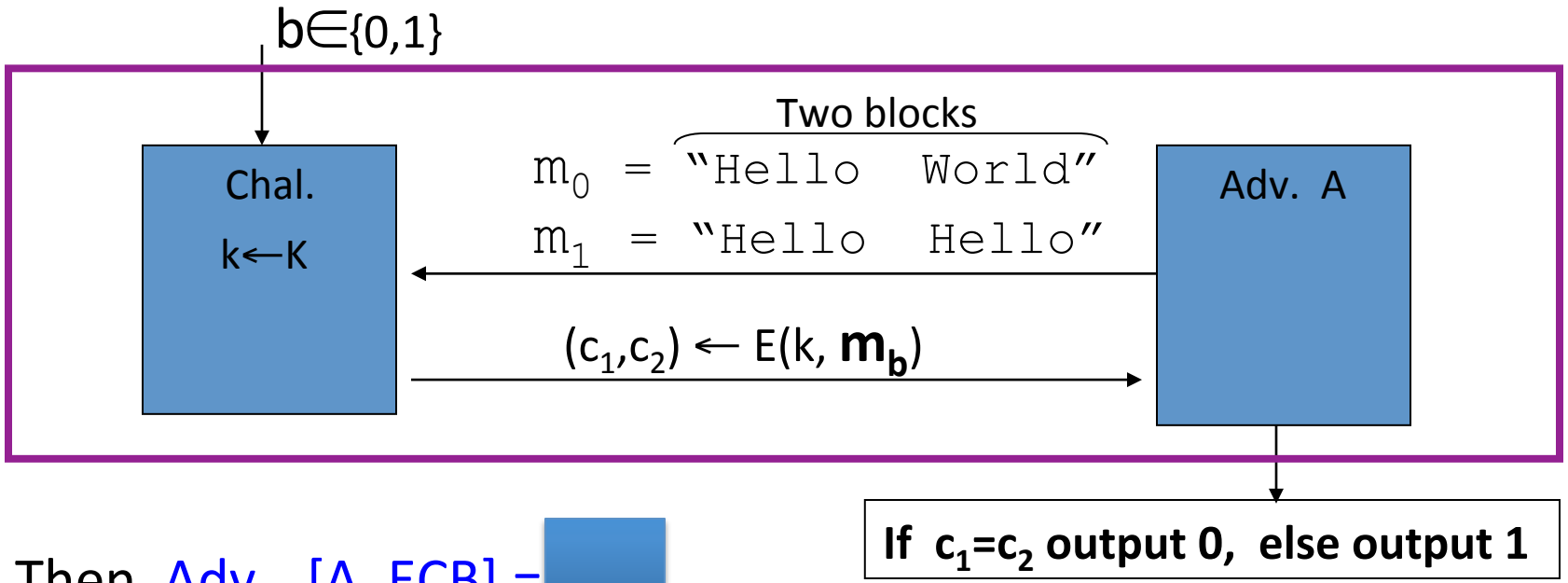
Semantic Security (one-time key)



$Adv_{SS}[A,OTP] = \left| \Pr[\ \mathbf{EXP(0)}=1\ ] - \Pr[\ \mathbf{EXP(1)}=1\ ] \right|$ should be "neg."

ECB is not Semantically Secure

ECB is not semantically secure for messages that contain more than one block.



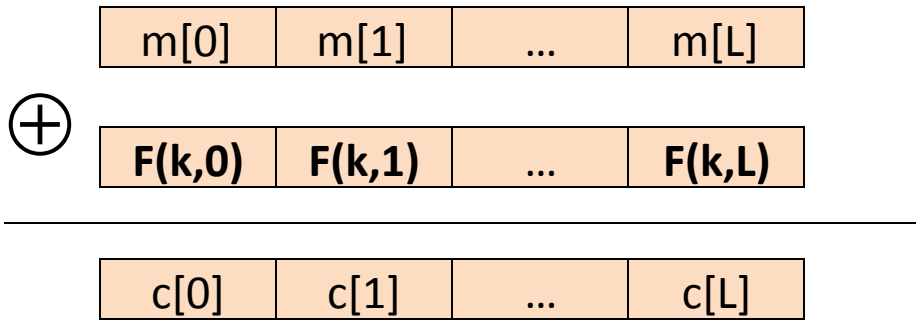
Then $Adv_{SS}[A, ECB] =$

Secure Construction I

Deterministic counter mode from a PRF F : $\mathcal{K} \times \{0,1\}^n \rightarrow \{0,1\}^n$

(e.g. $n = 128$)

- $E_{DETCTR}(k, m)$ =



⇒ Stream cipher built from a PRF (e.g. AES, 3DES)

Det. counter-mode security

Theorem: For any L>0,

If F is a secure PRF over (K,X,X) then

E_{DETCTR} is sem. sec. cipher over (K, X^L, X^L).

In particular, for any eff. adversary A attacking E_{DETCTR}

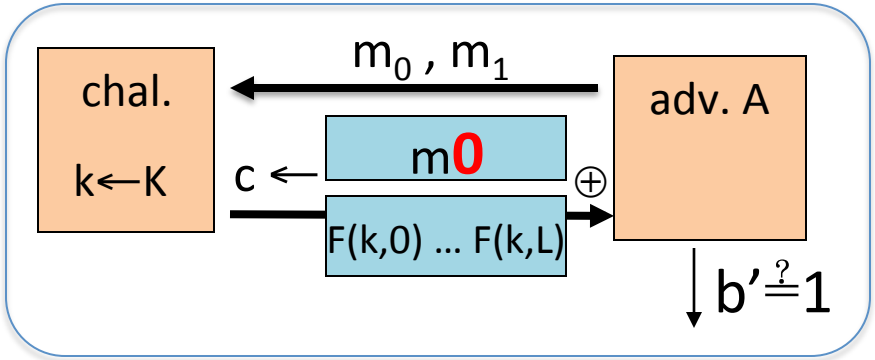
there exists a n eff. PRF adversary B s.t.:

$$Adv_{SS}[A, E_{DETCTR}] = 2 \cdot Adv_{PRF}[B, F]$$

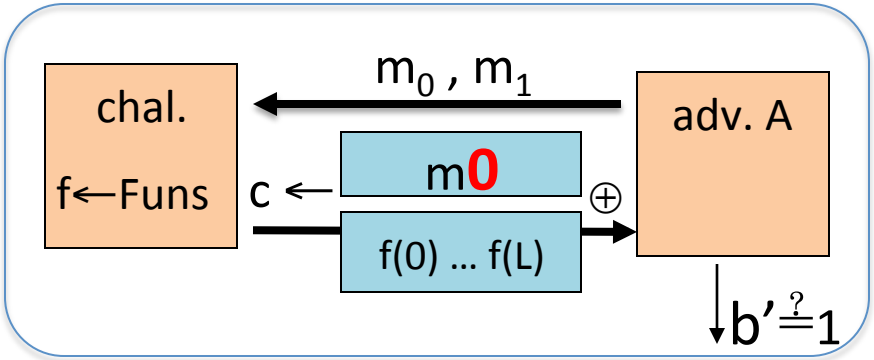
$Adv_{PRF}[B, F]$ is negligible (since F is a secure PRF)

Hence, $Adv_{SS}[A, E_{DETCTR}]$ must be negligible.

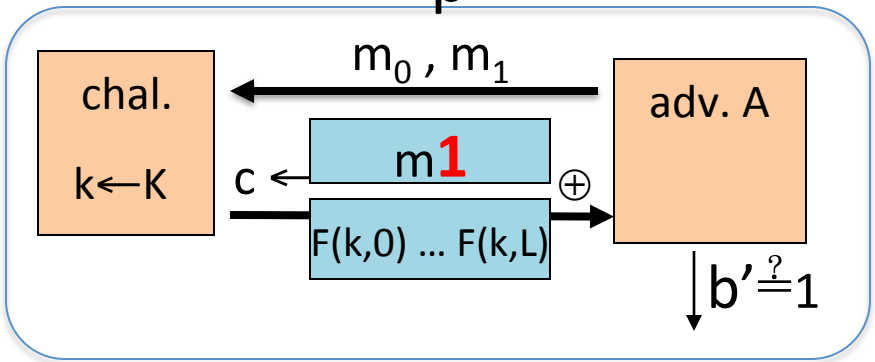
Proof



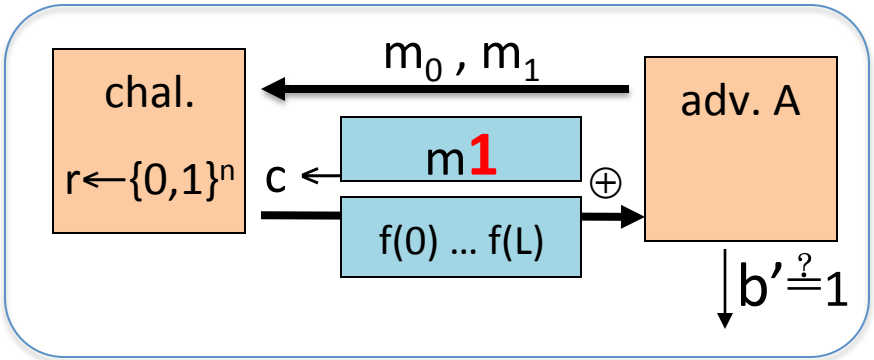
$\approx_p$



$\approx_p$



$\approx_p$



End of Segment