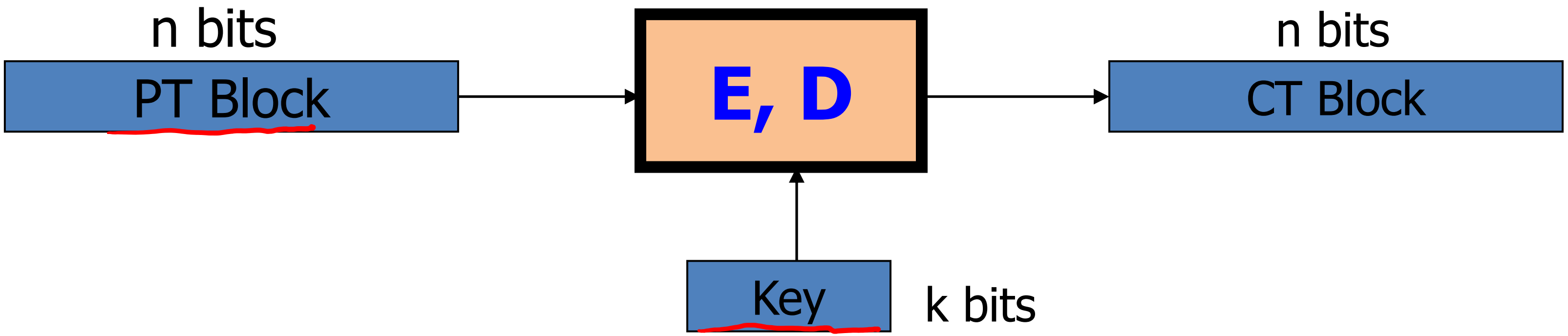
Using block ciphers

Review: PRPs and PRFs

Block ciphers: crypto work horse



Canonical examples:

1. 3DES: n= 64 bits, k = 168 bits
2. AES: n=128 bits, k = 128, 192, 256 bits

Abstractly: PRPs and PRFs

分组 流密码

序列

- Pseudo Random Function (**PRF**) defined over (K,X,Y):

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

such that exists "efficient" algorithm to evaluate F(k,x)

- Pseudo Random Permutation (**PRP**) defined over (K,X):

$$E: \ K \times X \ \rightarrow \ X$$

such that:

1. Exists "efficient" deterministic algorithm to evaluate E(k,x)
2. The function $E(\, k, \cdot \,)$ is one-to-one
3. Exists "efficient" inversion algorithm D(k,x)

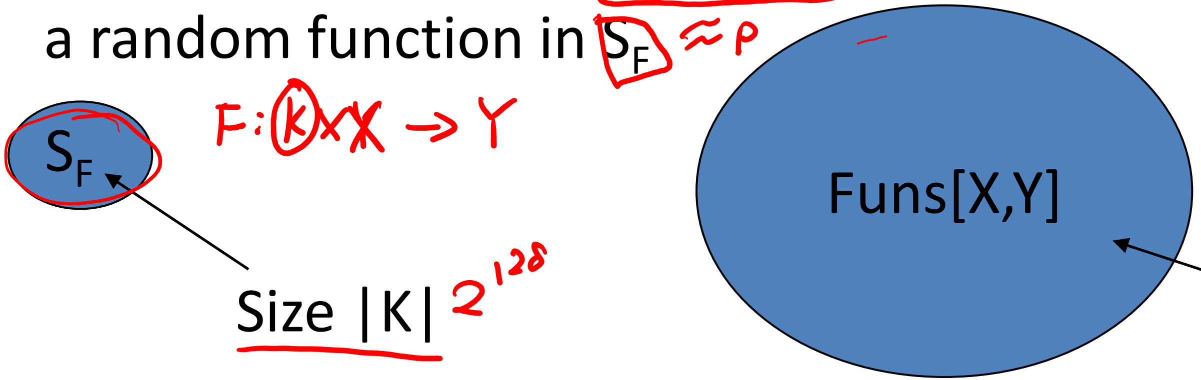
Secure PRFs

- Let $F: K \times X \rightarrow Y$ be a PRF

$$\begin{cases} \text{Funs}[X,Y]: & \text{the set of } \underline{\textbf{all}} \text{ functions from } X \text{ to } Y \\ S_F = \{\ F(k,\cdot)\ \text{ s.t. } k \in K\ \} & \subseteq \quad \text{Funs}[X,Y] \end{cases}$$

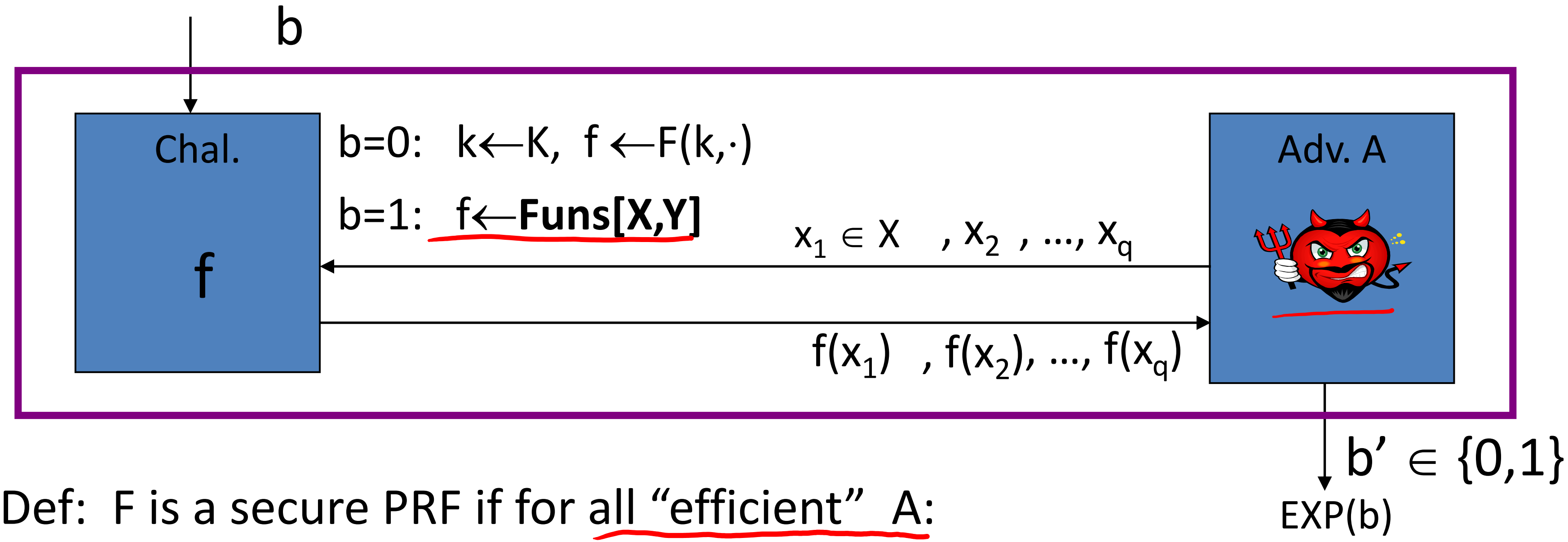
- <u>Intuition</u>: a PRF is **secure** if
  a random function in $\boxed{\text{Funs}[X,Y]}$ is indistinguishable from
  a random function in $\boxed{S_F}$ $\approx p$

AES $(2^{128})^{2^{128}}$



Secure PRF: definition

- For b=0,1 define experiment EXP(b) as:



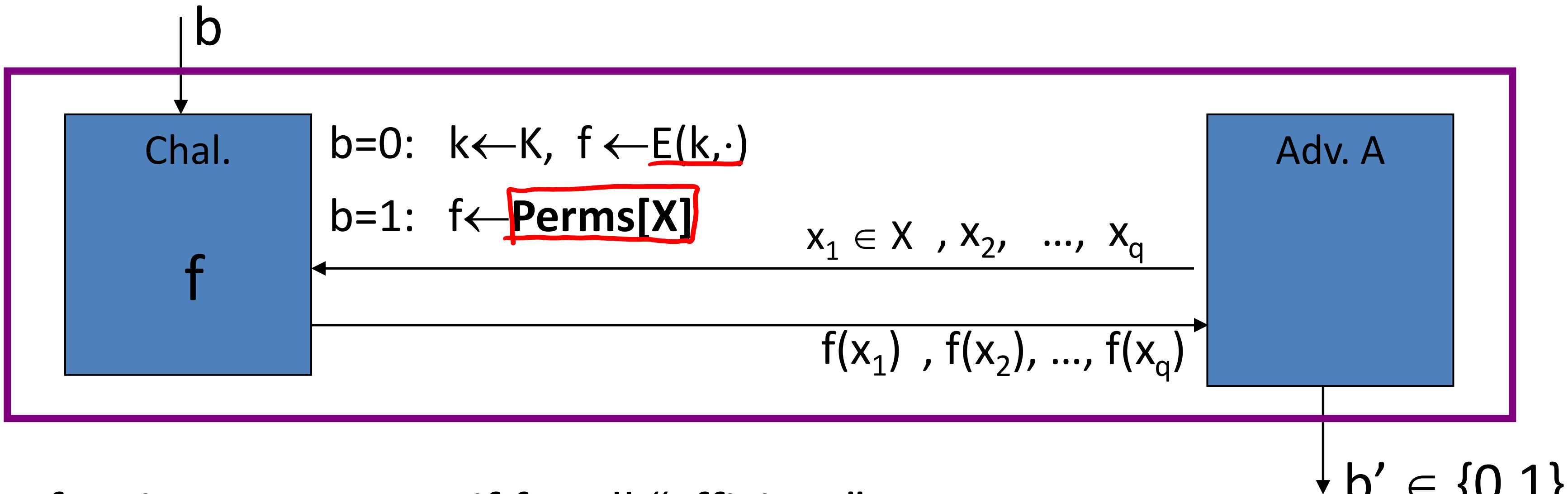
- Def: F is a secure PRF if for all "efficient" A:

$$\mathrm{Adv}_{\mathrm{PRF}}[A,F] := \left| \Pr[\mathrm{EXP}(0)=1] - \Pr[\mathrm{EXP}(1)=1] \right|$$

is "negligible."

Secure PRP (secure block cipher)

- For b=0,1 define experiment EXP(b) as:



- Def: E is a secure PRP if for all "efficient" A:

$$\text{Adv}_{\text{PRP}}[A,E] = \left| \Pr[\text{EXP}(0)=1] - \Pr[\text{EXP}(1)=1] \right|$$

is "negligible."

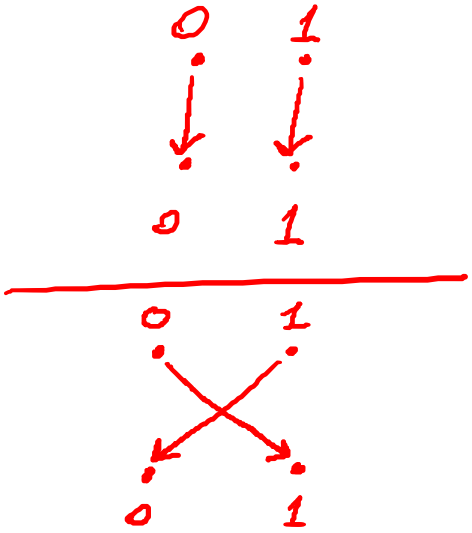
Let $X = \{0,1\}$. Perms[X] contains two functions

Consider the following PRP:

key space $K=\{0,1\}$, input space $X = \{0,1\}$,

PRP defined as:

$$E(k,x) = x \oplus k$$



Is this a secure PRP?

- ○ Yes
- ○ No
- ○ It depends
- ○

Example secure PRPs

ZUC 序列 → 4G. LTE.

- PRPs believed to be secure: 3DES, AES, IDEA, SM4…

↳ WAPI / WIFI.

AES-128: $K \times X \rightarrow X$ where $K = X = \{0,1\}^{128}$

Effi. A.

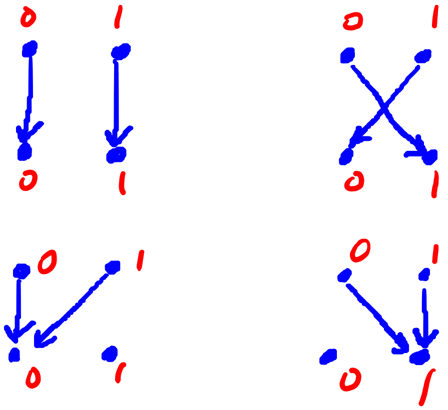
- An example concrete assumption about AES:

All 2^{80}–time algs. A have $\mathrm{Adv}_{\mathrm{PRP}}[A, \mathbf{AES}] < 2^{-40}$

Consider the 1-bit PRP from the previous question: $\boxed{E(k,x) = x \oplus k}$

Is it a secure PRF?

Note that $\boxed{\text{Funs}[X,X]}$ contains four functions



- ○ Yes
- ○ No
- ○ It depends
- ○

Attacker A: $f(0)$. $f(1)$

(1) query $f(\cdot)$ at $x=0$ and $x=1$

(2) if $f(0) = f(1)$ output "1", else "0"

$\text{Adv}_{\text{PRF}}[A,E] = |0-½| = ½$

PRF Switching Lemma

Any secure PRP is also a secure PRF, if $|X|$ is sufficiently large.

<u>Lemma</u>: Let E be a PRP over (K,X)

Then for any q-query adversary A:

$$\big|\ \cancel{\mathrm{Adv}_{\mathrm{PRF}}[A,E]} - \mathrm{Adv}_{\mathrm{PRP}}[A,E]\ \big| < q^2 / 2|X|$$

neg. neg. neg.

$\Rightarrow$ Suppose $|X|$ is large so that $q^2 / 2|X|$ is "negligible"

Then $\mathrm{Adv}_{\mathrm{PRP}}[A,E]$ "negligible" $\Rightarrow$ $\mathrm{Adv}_{\mathrm{PRF}}[A,E]$ "negligible"

Final note

PRP

- Suggestion:
  - don't think about the inner-workings of AES and 3DES.

- We assume both are secure PRPs and will see how to use them

End of Segment

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)

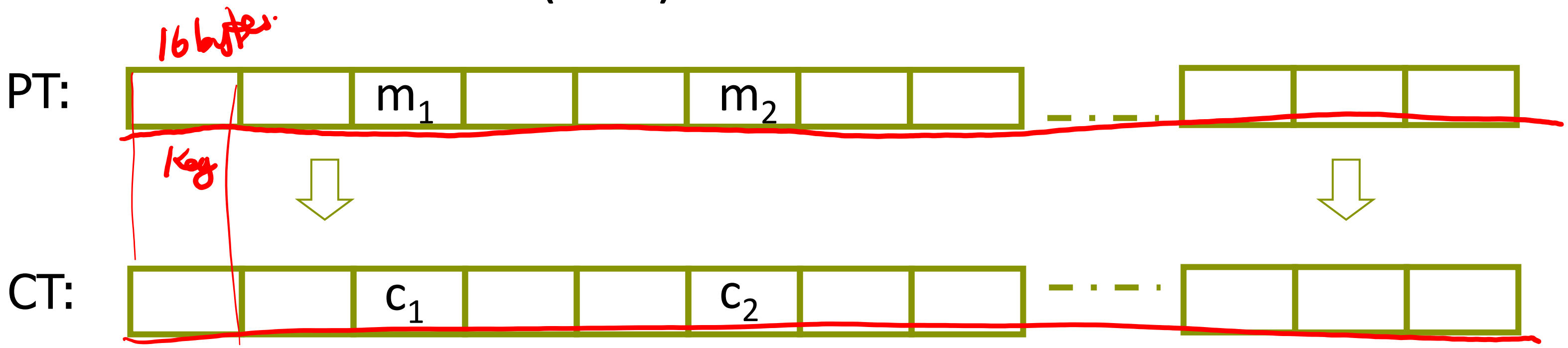
2. Adversary's goal:

   Learn info about PT from CT (semantic security)

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

Incorrect use of a PRP

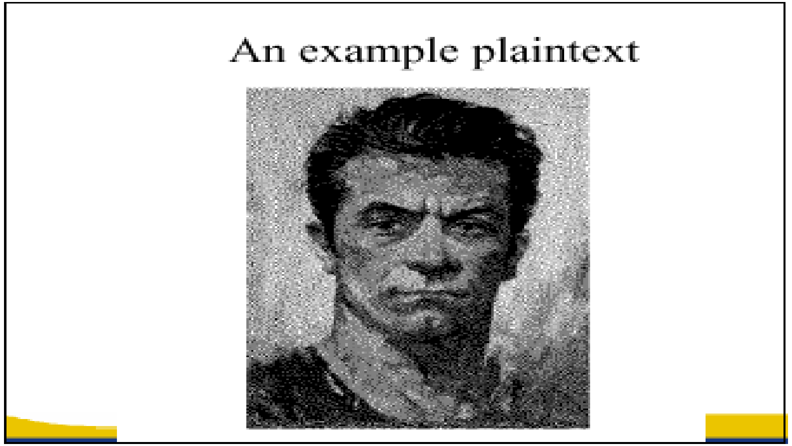
Electronic Code Book (ECB):

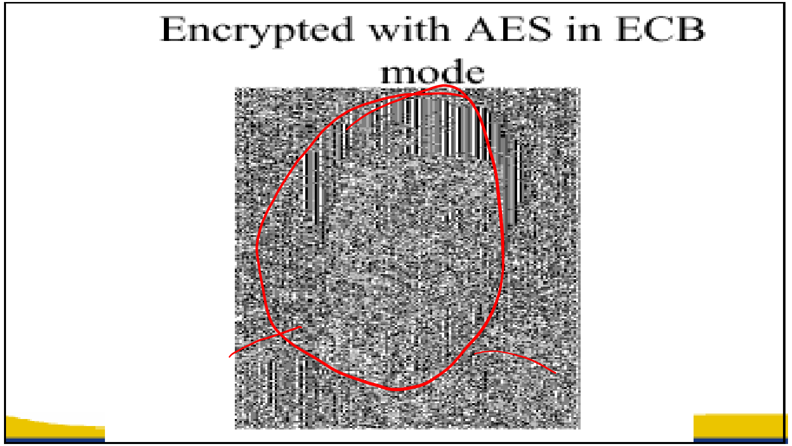


Problem:

– if $m_1 = m_2$ then $c_1 = c_2$

In pictures

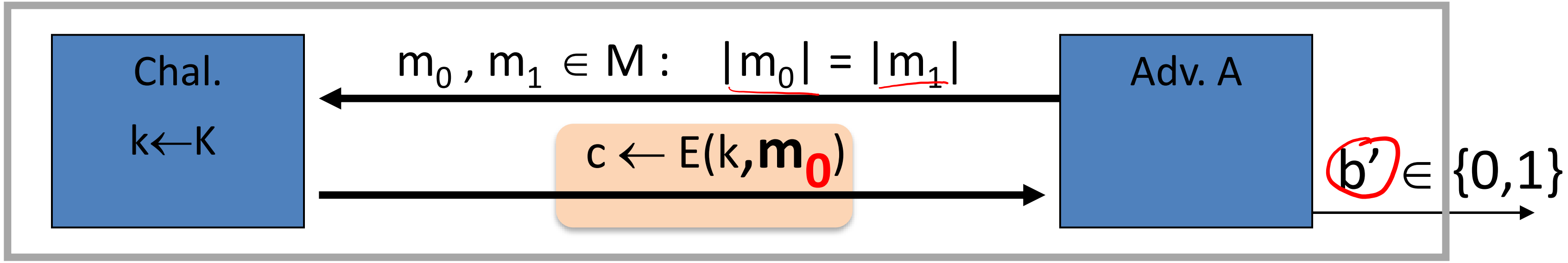




(courtesy B. Preneel)

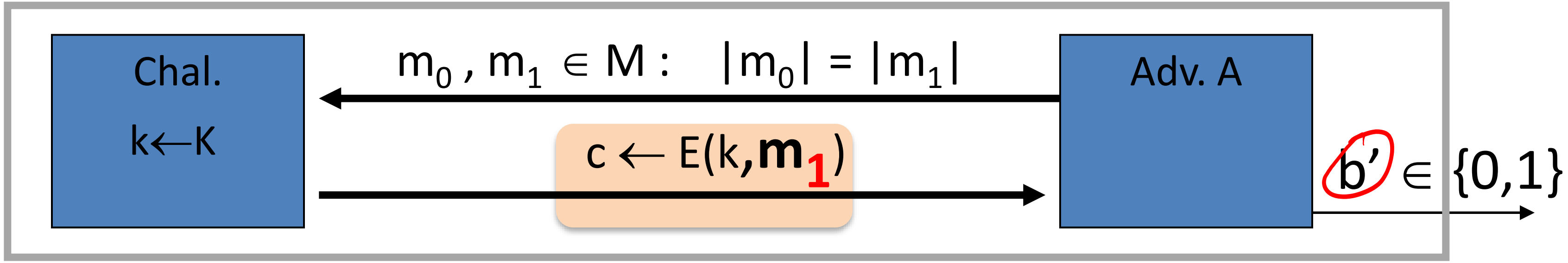
Semantic Security (one-time key)

EXP(0):



one time key $\Rightarrow$ adversary sees only one ciphertext

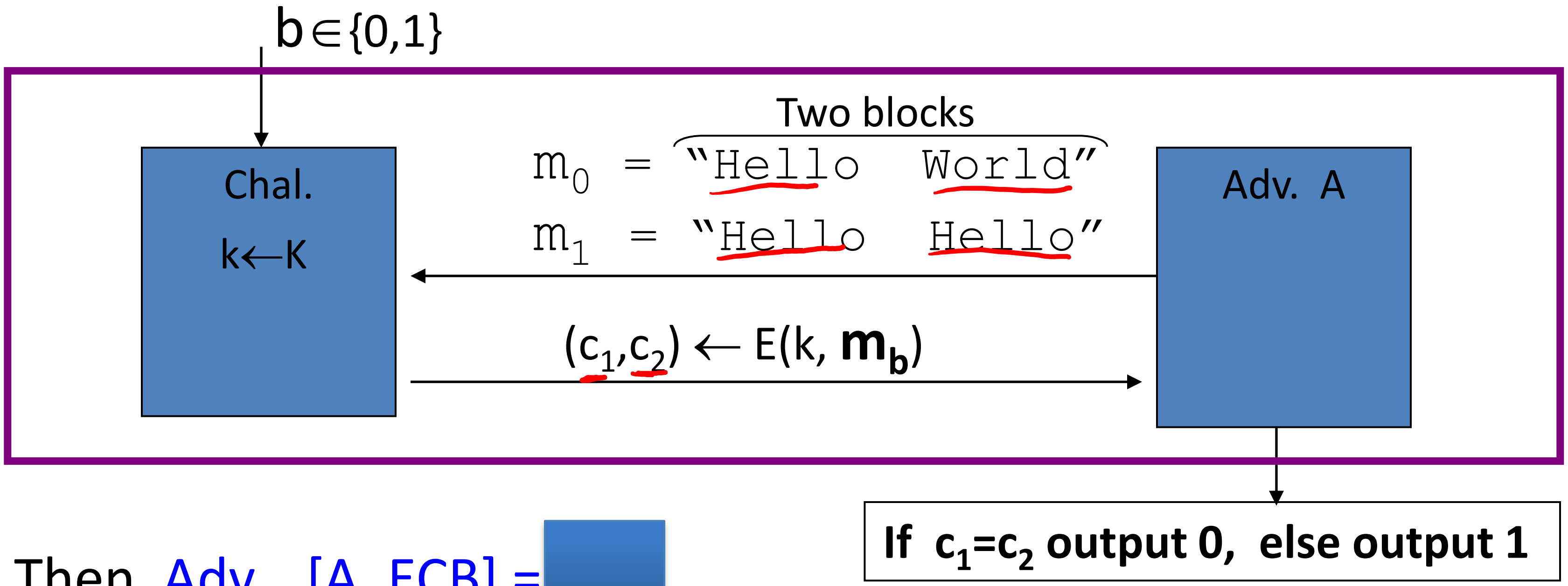
EXP(1):



$\text{Adv}_{SS}[A,\text{OTP}] = \Big|\ \Pr[\ \mathbf{EXP(0)}=1\ ] - \Pr[\ \mathbf{EXP(1)}=1\ ]\ \Big|$ 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 : $\mathcal{K} \times \{0,1\}^n \longrightarrow \{0,1\}^n$

(e.g. n=128)

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

	m[0]	m[1]	…	m[L]
⊕	ctr.			
	F(k,0)	**F(k,1)**	…	**F(k,L)**
	c[0]	c[1]	…	c[L]

⇒ 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}

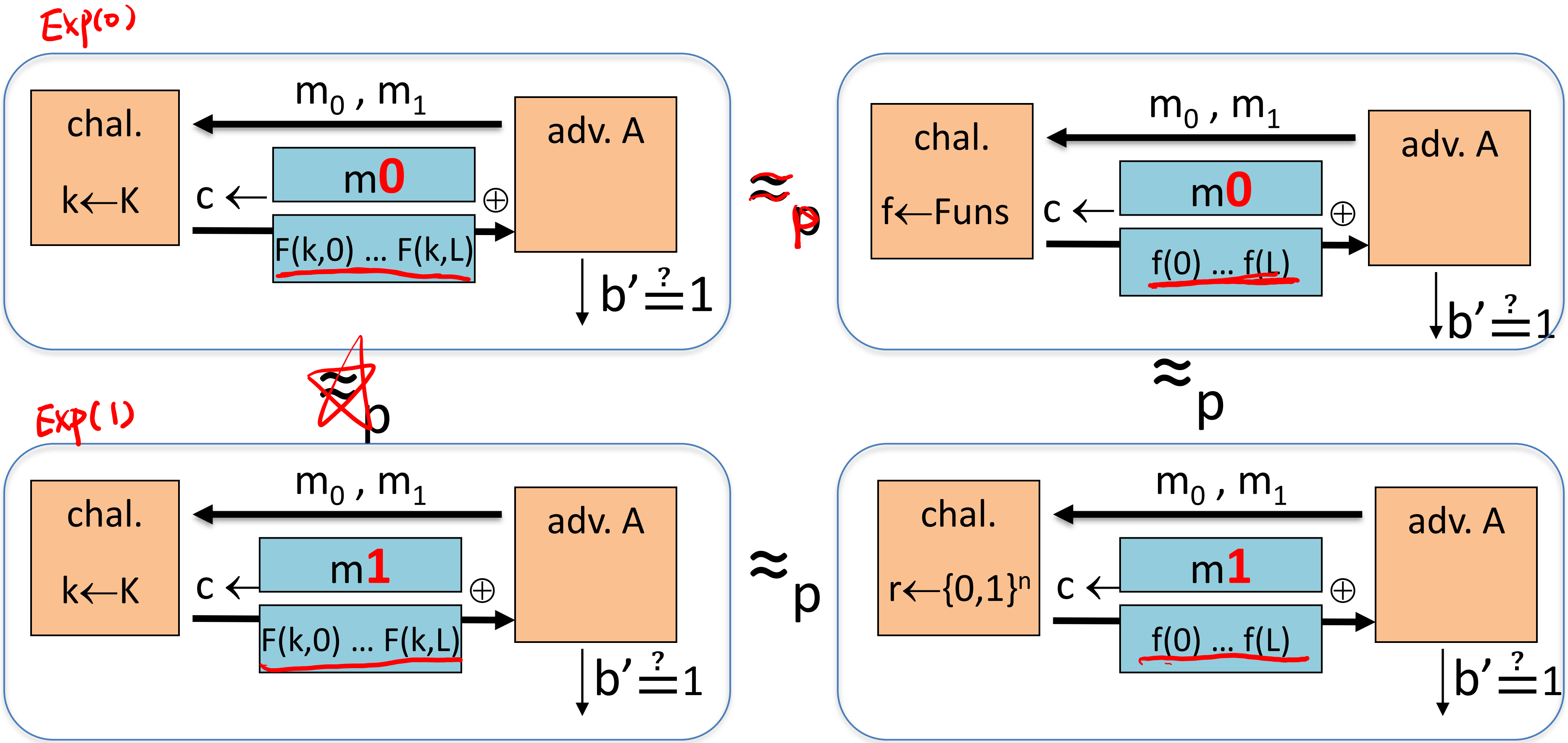
there exists a n eff. PRF adversary B s.t.:

$$\mathrm{Adv}_{SS}[A, E_{DETCTR}] = 2 \cdot \mathrm{Adv}_{PRF}[B, F] \approx \text{neg.}$$

$\mathrm{Adv}_{PRF}[B, F]$ is negligible (since F is a secure PRF)

Hence, $\mathrm{Adv}_{SS}[A, E_{DETCTR}]$ must be negligible.

Proof



Exp(0)
chal.
k←K
m0 , m1
adv. A
m0
c ←
⊕
F(k,0) … F(k,L)
b' ≟ 1
≈p
chal.
f←Funs
m0 , m1
adv. A
m0
c ←
⊕
f(0) … f(L)
b' ≟ 1
≈p
Exp(1)
≈p
chal.
k←K
m0 , m1
adv. A
m1
c ←
⊕
F(k,0) … F(k,L)
b' ≟ 1
≈p
chal.
r←{0,1}^n
m0 , m1
adv. A
m1
c ←
⊕
f(0) … f(L)
b' ≟ 1

End of Segment

Using block ciphers

Security for many-time key

<u>Example applications</u>:

1. File systems: Same AES key used to encrypt many files.
2. IPsec: Same AES key used to encrypt many packets.

Semantic Security for many-time key

Key used more than once $\Rightarrow$ adv. sees many CTs with same key

Adversary's power: chosen-plaintext attack (CPA)

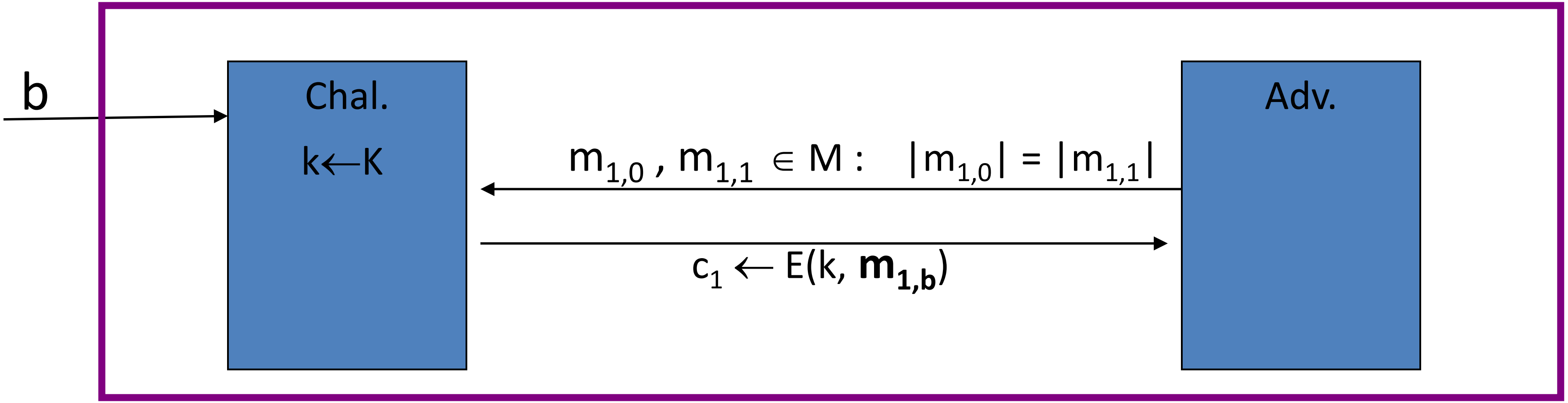
- Can obtain the encryption of arbitrary messages of his choice

(conservative modeling of real life)

Adversary's goal: Break sematic security

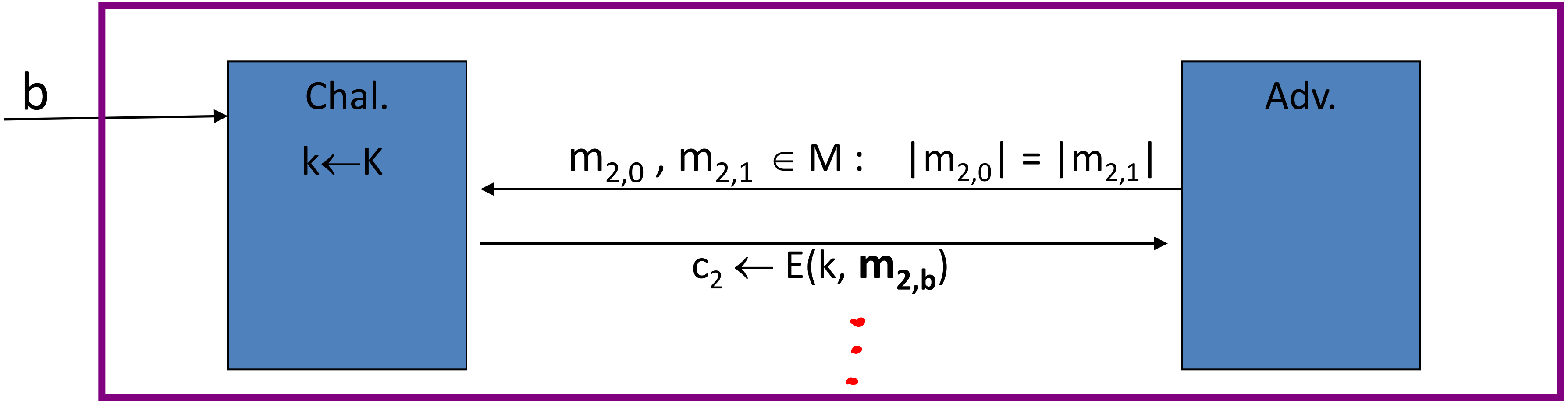
Semantic Security for many-time key

$\mathbb{E}$ = (E,D) a cipher defined over (K,M,C). For b=0,1 define EXP(b) as:



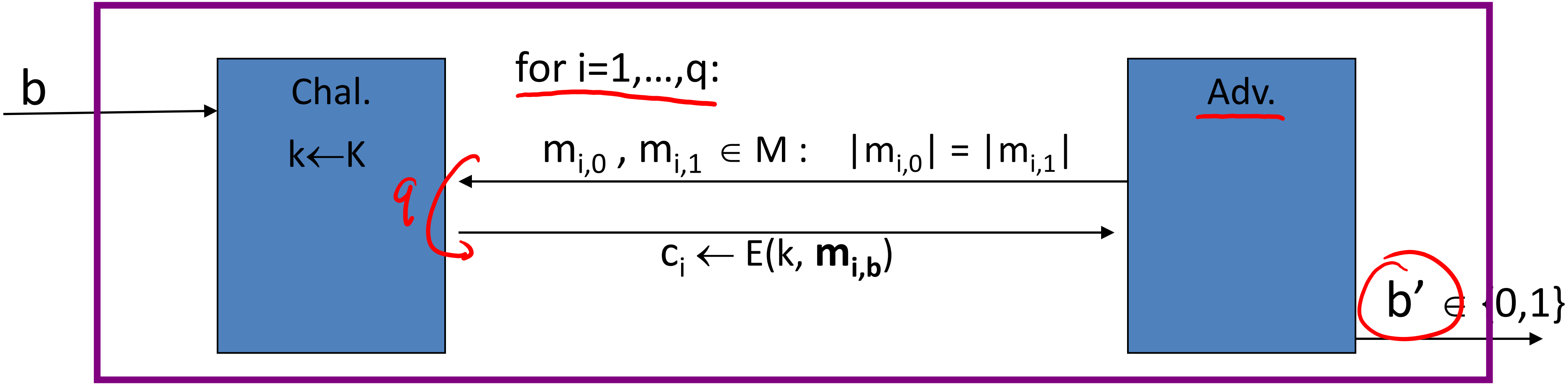
Semantic Security for many-time key

$\mathbb{E}$ = (E,D) a cipher defined over (K,M,C). For b=0,1 define EXP(b) as:



Semantic Security for many-time key (CPA security)

$\mathbb{E}$ = (E,D) a cipher defined over (K,M,C). For b=0,1 define EXP(b) as:



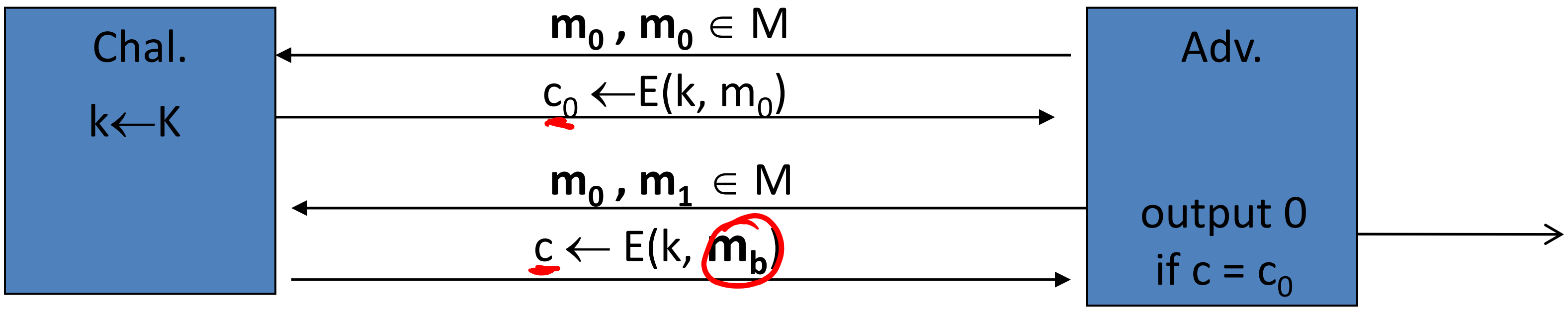
if adv. wants $c = E(k, m)$ it queries with $m_{j,0} = m_{j,1} = m$

Def: $\mathbb{E}$ is sem. sec. under CPA if for all "efficient" A:

$$\text{Adv}_{\text{CPA}}[A,\mathbb{E}] = \big|\Pr[\text{EXP}(0)=1] - \Pr[\text{EXP}(1)=1]\big|$$ is "negligible."

Ciphers insecure under CPA

Suppose E(k,m) always outputs same ciphertext for msg m.   Then:

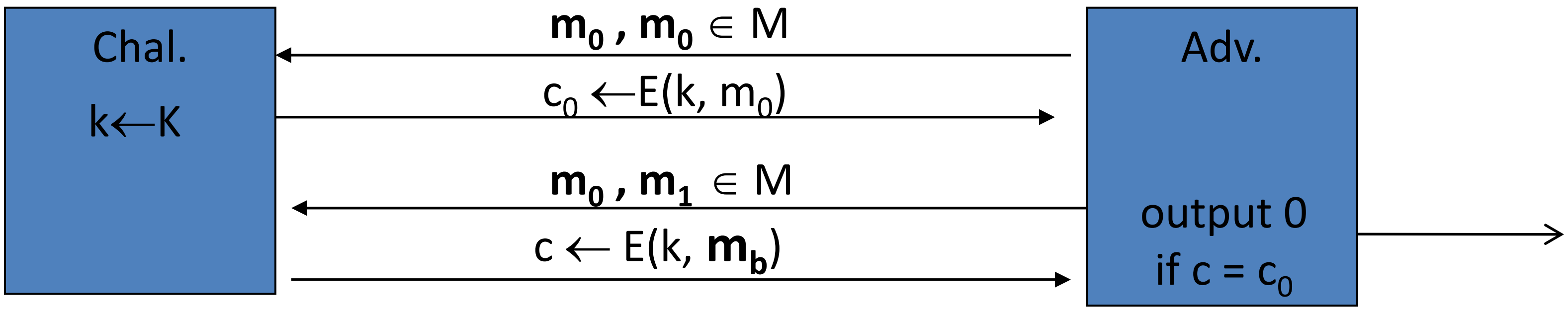


So what?   an attacker can learn that two encrypted files are the same, two encrypted packets are the same, etc.

- Leads to significant attacks when message space M is small

Ciphers insecure under CPA

Suppose E(k,m) always outputs same ciphertext for msg m. Then:

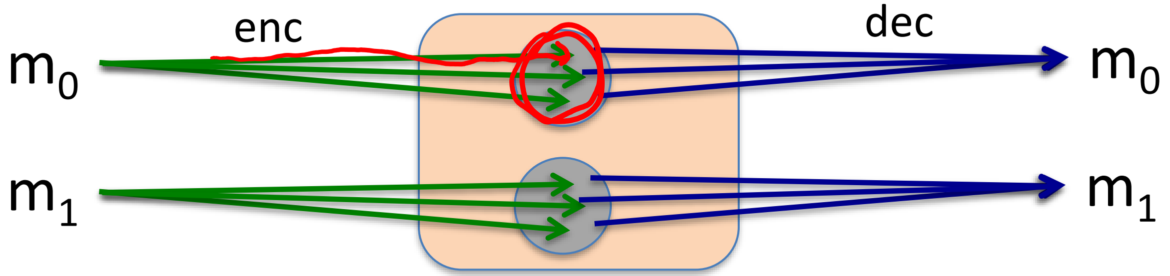


If secret key is to be used multiple times $\Rightarrow$ CPA

given the same plaintext message twice,
encryption must produce different outputs.

Solution 1: randomized encryption

- E(k,m) is a randomized algorithm:



⇒ encrypting same msg twice gives different ciphertexts (w.h.p)

⇒ ciphertext must be longer than plaintext

Roughly speaking: CT-size = PT-size + "# random bits"

Let $F: K \times R \longrightarrow M$ be a secure PRF.

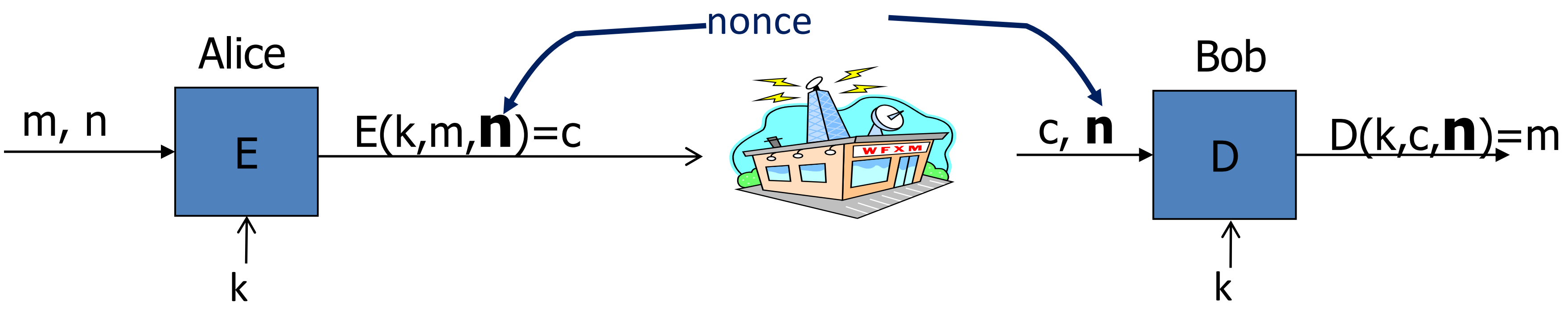
$\approx_p (r, F(r) \oplus m)$

For $m \in M$ define $E(k,m) = [\, r \xleftarrow{R} R,$ output $(r, F(k,r) \oplus m) \,]$

Is E semantically secure under CPA?

- Yes, whenever F is a secure PRF
- No, there is always a CPA attack on this system
- Yes, but only if R is large enough so r never repeats (w.h.p)
- It depends on what F is used

Solution 2: nonce-based Encryption



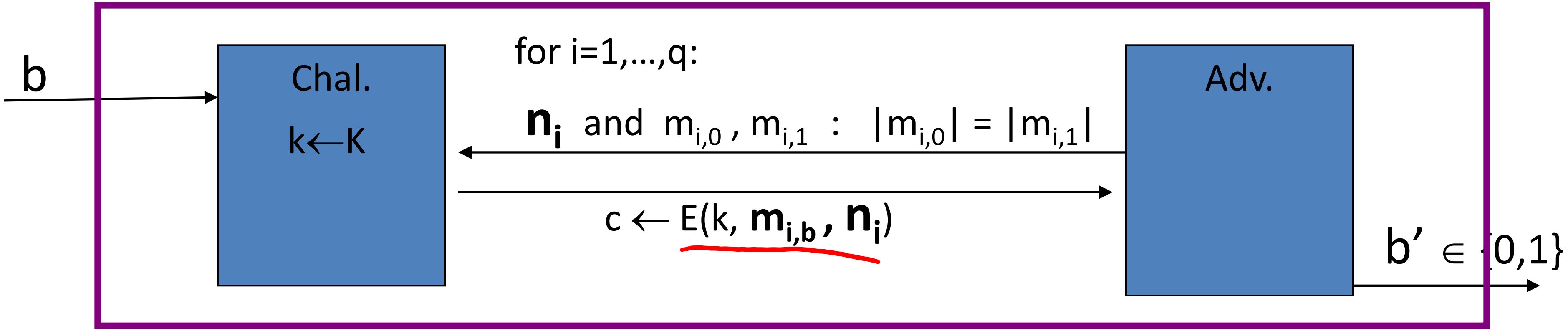
- nonce n: a value that changes from msg to msg.
  (k,n) pair <u>never</u> used more than once

- <u>method 1</u>: nonce is a **counter** (e.g. packet counter)
  - used when encryptor keeps state from msg to msg
  - if decryptor has same state, need not send nonce with CT

- <u>method 2</u>: encryptor chooses a **random nonce**, $n \leftarrow \mathcal{N}$

CPA security for nonce-based encryption

System should be secure when nonces are chosen adversarially.



All nonces $\{n_1, \ldots, n_q\}$ must be distinct.

Def: nonce-based $\mathbb{E}$ is sem. sec. under CPA if for all "efficient" A:

$$\text{Adv}_{\text{nCPA}}[A,\mathbb{E}] = \left| \Pr[\text{EXP}(0)=1] - \Pr[\text{EXP}(1)=1] \right|$$ is "negligible."

Let $F: K \times R \longrightarrow M$ be a secure PRF. Let $r = 0$ initially.

For $m \in M$ define $E(k,m) = [\ \underline{r{+}{+}},\ \text{output}\ (r, \underline{F(k,r)} \oplus m)\ ]$

$\approx_p \ (r, \underline{F(r) \oplus m})$

(r, r')

Is E CPA secure nonce-based encryption?

- ○ Yes, whenever F is a secure PRF
- ○ No, there is always a nonce-based CPA attack on this system
- ○ <u>Yes, but only if R is large enough so r never repeats</u>
- ○ It depends on what F is used

End of Segment

Using block ciphers

Modes of operation: many time key (CBC)

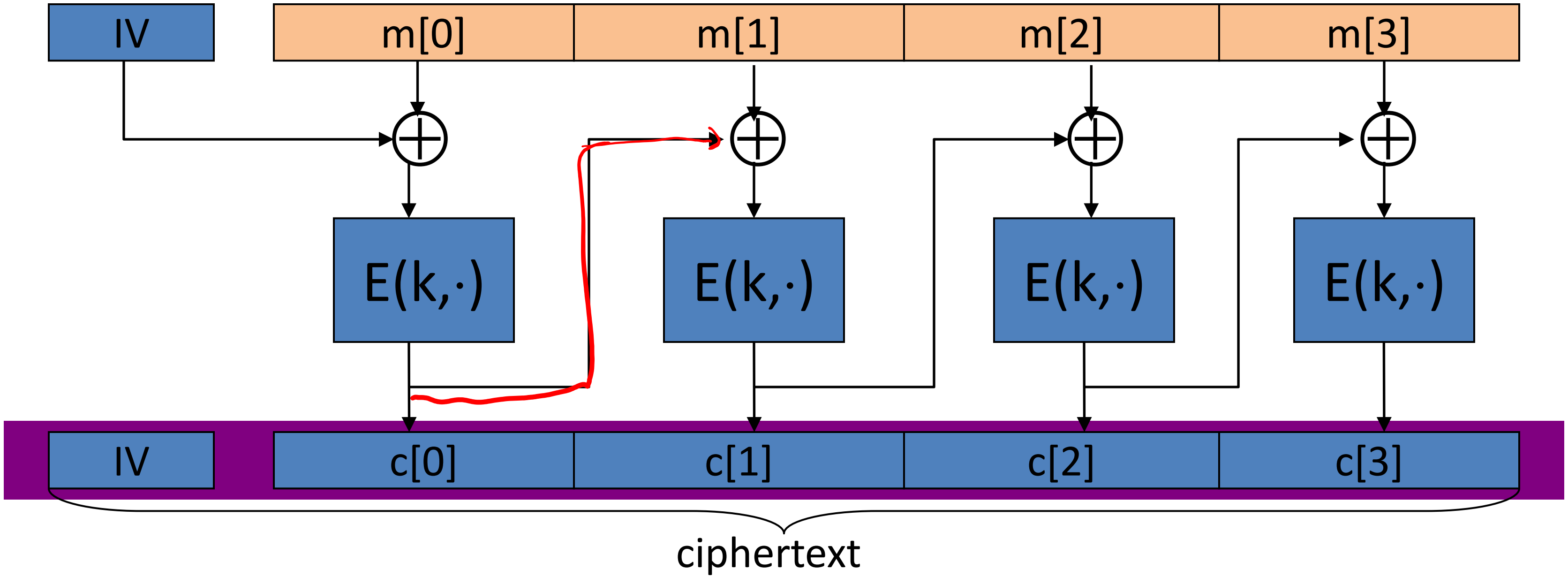
<u>Example applications</u>:

1. File systems: Same AES key used to encrypt many files.
2. IPsec: Same AES key used to encrypt many packets.

Construction 1: CBC with random IV

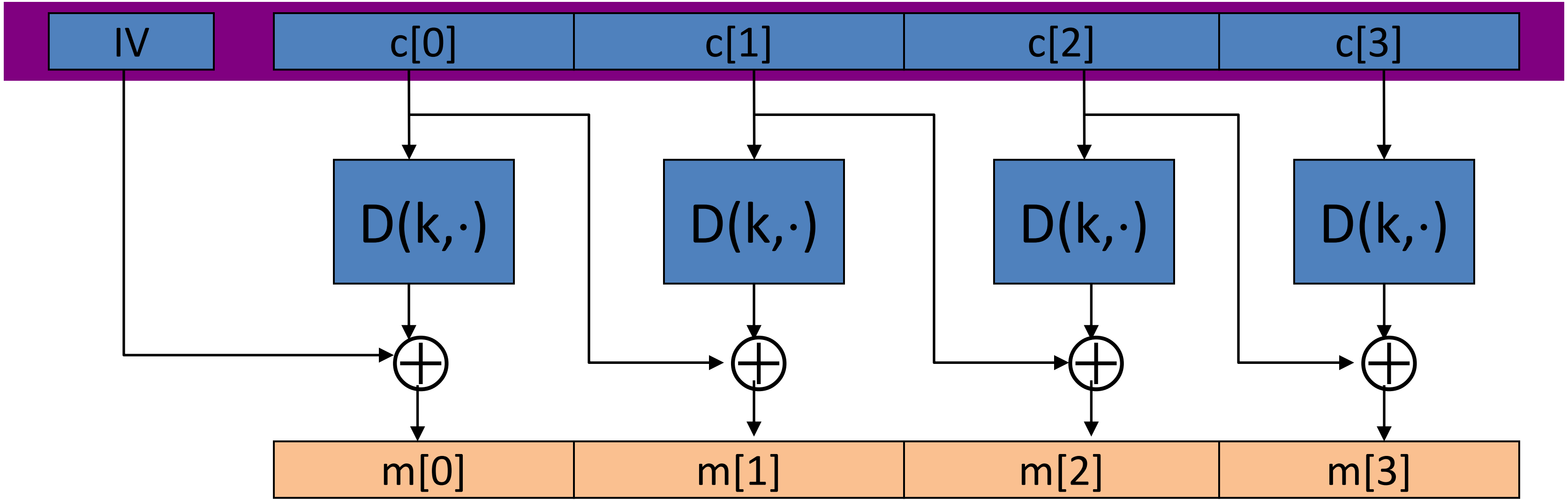
Let (E,D) be a PRP. $E_{CBC}(k,m)$: choose **random** IV∈X and do:

$E: \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ $IV \in \{0,1\}^n$



Decryption circuit

In symbols: $c[0] = E\big(k, IV \oplus m[0]\big) \Rightarrow m[0] =$



CBC: CPA Analysis

CBC Theorem: For any L>0,

If E is a secure PRP over (K,X) then

E_{CBC} is a sem. sec. under CPA over (K, X^{L}, X^{L+1}).

In particular, for a q-query adversary A attacking E_{CBC}

there exists a PRP adversary B s.t.:

$$\underbrace{\mathrm{Adv}_{\mathrm{CPA}}[A, E_{\mathrm{CBC}}]}_{\text{neg.}} \leq \underbrace{2\cdot\mathrm{Adv}_{\mathrm{PRP}}[B, E]}_{\text{neg.}} + \mathbf{2\, q^2 L^2 / |X|}$$

Note: CBC is only secure as long as $\mathbf{q^2L^2 \ll |X|}$

An example

$$\text{Adv}_{\text{CPA}}[A, E_{\text{CBC}}] \le 2\cdot\text{PRP Adv}[B, E] + \mathbf{2\,q^2\,L^2 / |X|}$$

q = # messages encrypted with k , L = length of max message

Suppose we want $\text{Adv}_{\text{CPA}}[A, E_{\text{CBC}}] \le 1/2^{32}$ $\Leftarrow$ $q^2\,L^2 / |X| < 1/2^{32}$

- AES: $|X| = 2^{128}$ $\Rightarrow$ $q\,L < 2^{48}$

  So, after 2^{48} AES blocks, must change key

- 3DES: $|X| = 2^{64}$ $\Rightarrow$ $q\,L < 2^{16}$

Warning: an attack on CBC with rand. IV

CBC where attacker can predict the IV is not CPA-secure !!

Suppose given $c \longleftarrow E_{CBC}(k,m)$ can predict IV for next message

Chal.

$k \leftarrow K$

Adv.

predict IV

$\mathbf{0} \in X$

$c_1 \leftarrow [\,IV_1,\ E(k, 0 \oplus IV_1)\,]$

$m_0 = IV \oplus IV_1, \quad m_1 \neq m_0$

$c \leftarrow [\,IV,\ E(k,$

$c \leftarrow [\,IV,\ E(k, m_1 \oplus IV)\,]$

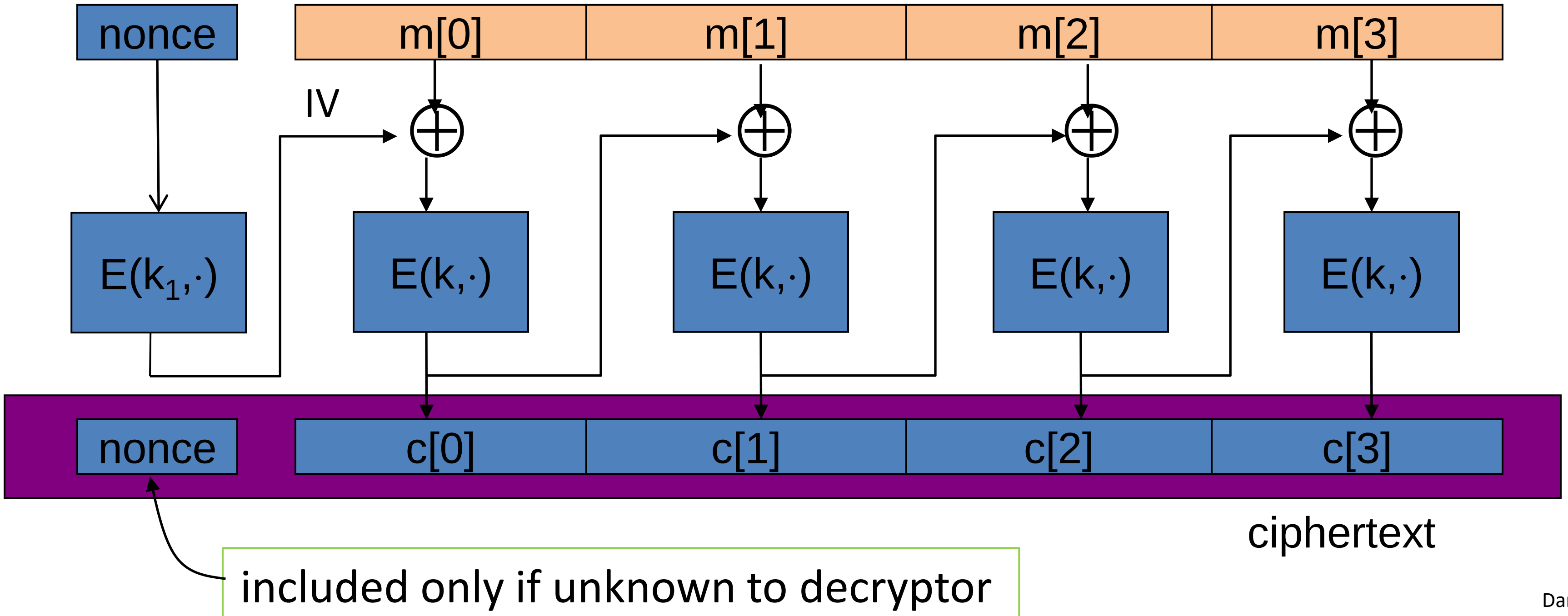
output 0 if $c[1] = c_1[1]$

Bug in SSL/TLS 1.0: IV for record #i is last CT block of record #(i-1)

Construction 1': nonce-based CBC

- Cipher block chaining with <u>unique</u> nonce: key = (k,k_1)

  unique nonce means: (key, n) pair is used for only one message



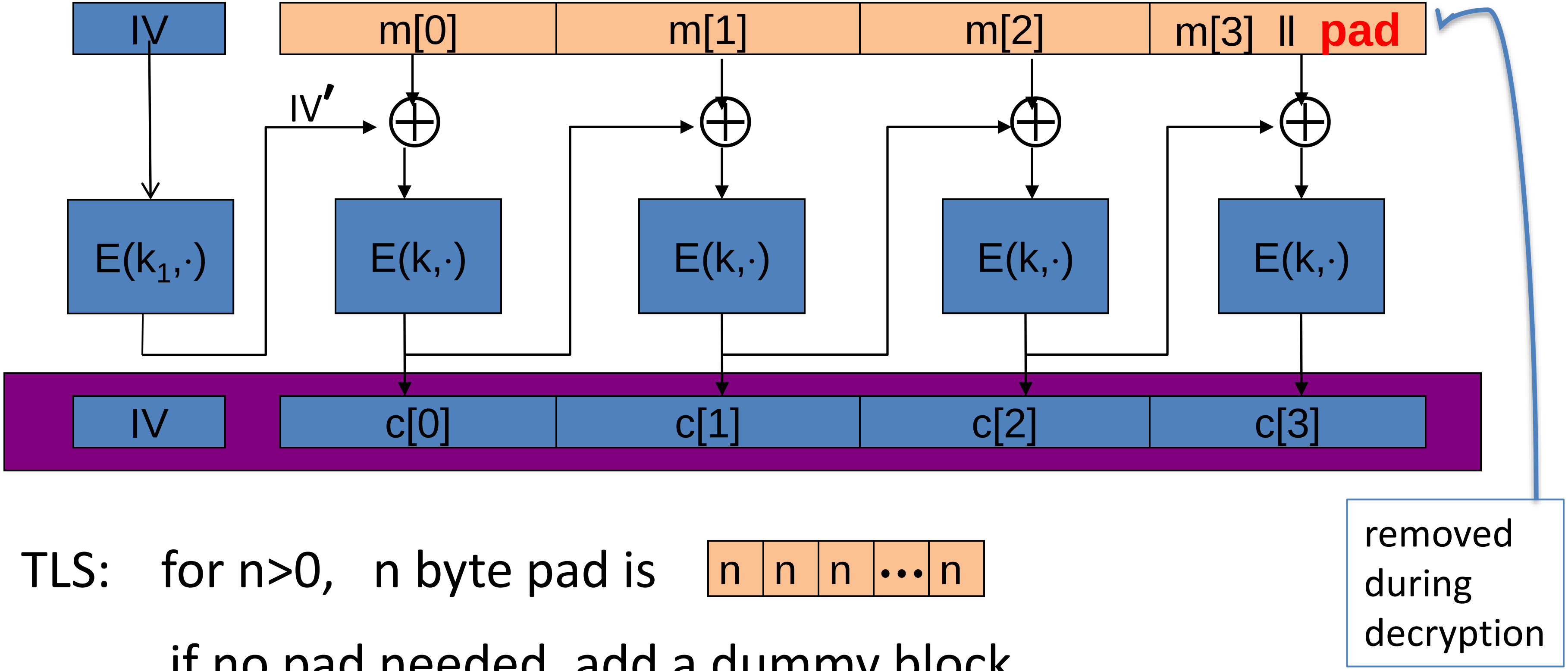
An example Crypto API   (OpenSSL)

```
void AES_cbc_encrypt(
        const unsigned char *in,
        unsigned char *out,
        size_t length,
        const AES_KEY *key,
        unsigned char *ivec,          ⟵   user supplies IV
        AES_ENCRYPT or AES_DECRYPT);
```

otherwise, no CPA security

When nonce is non random need to encrypt it before use

A CBC technicality: padding



TLS: for n>0, n byte pad is | n | n | n | ••• | n |

if no pad needed, add a dummy block

End of Segment

Using block ciphers

Modes of operation: many time key (CTR)

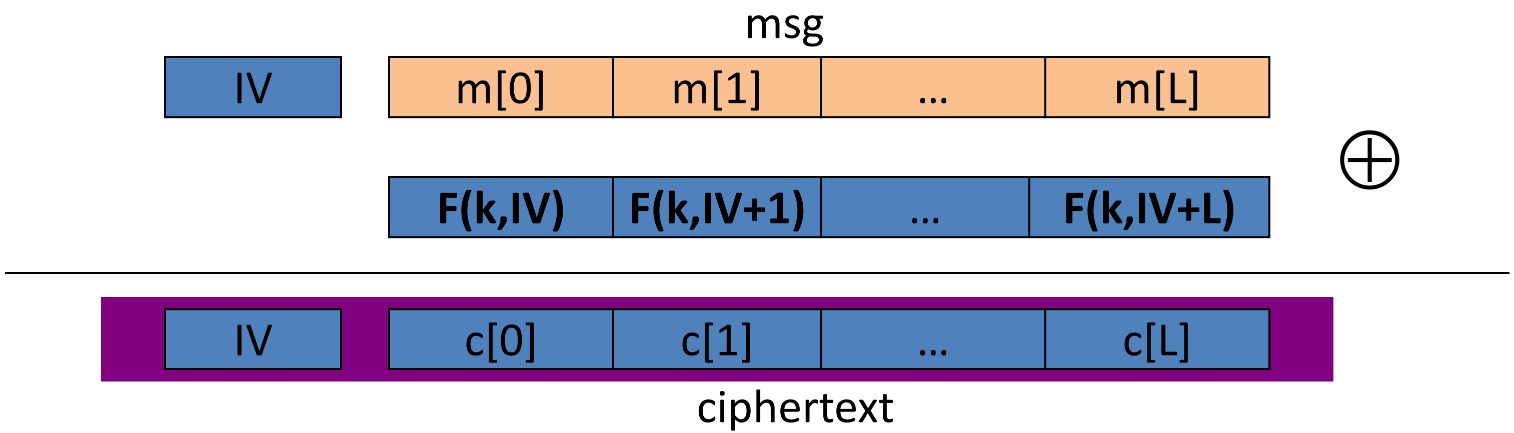
<u>Example applications</u>:

1. File systems: Same AES key used to encrypt many files.
2. IPsec: Same AES key used to encrypt many packets.

Construction 2: rand ctr-mode

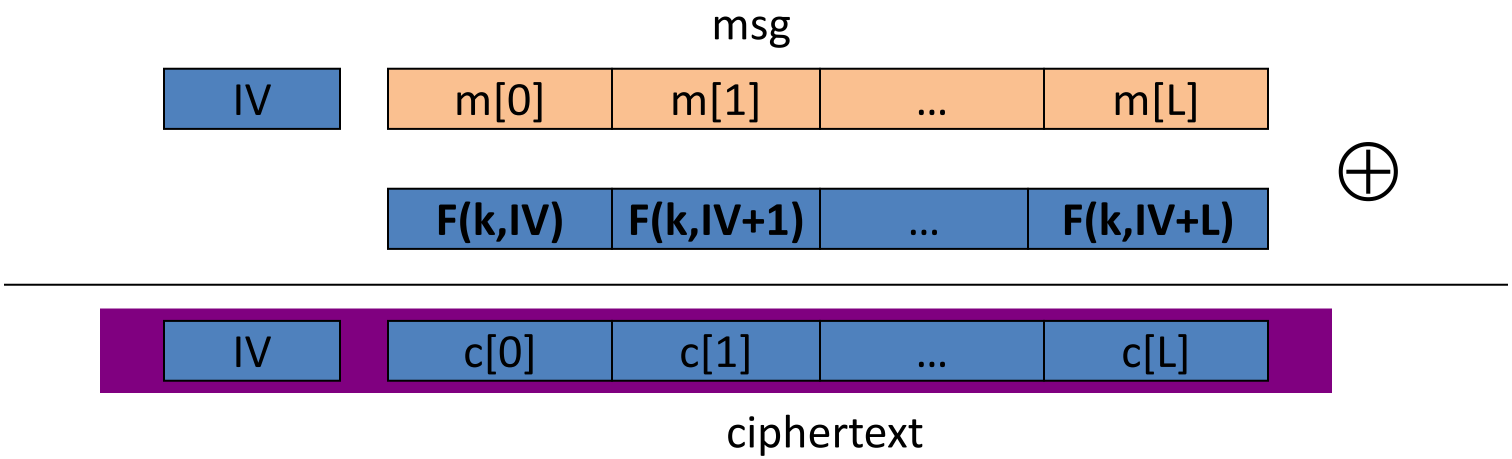
Let $F: K \times \{0,1\}^n \longrightarrow \{0,1\}^n$ be a secure PRF.

$E(k,m)$: choose a random $IV \in \{0,1\}^n$ and do:

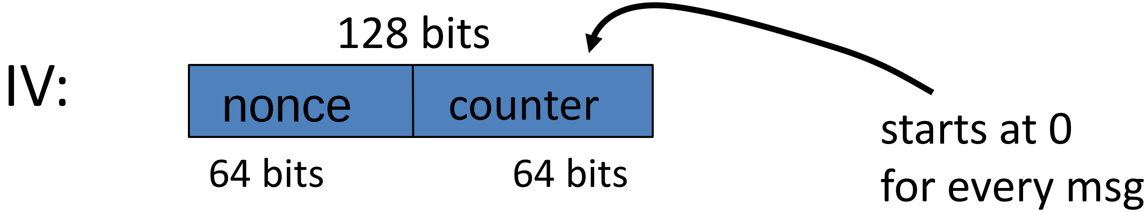


note: parallelizable (unlike CBC)

Construction 2’: nonce ctr-mode



To ensure F(k,x) is never used more than once, choose IV as:



rand ctr-mode (rand. IV): CPA analysis

- <u>Counter-mode Theorem</u>: For any L>0,

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

  E_{CTR} is a sem. sec. under CPA over (K,X^L,X^{L+1}).

  In particular, for a q-query adversary A attacking E_{CTR}

  there exists a PRF adversary B s.t.:

$$\mathrm{Adv}_{CPA}[A, E_{CTR}] \leq 2\cdot\mathrm{Adv}_{PRF}[B, F] + \mathbf{2\, q^2\, L \,/\, |X|}$$

<u>Note</u>: ctr-mode only secure as long as $q^2L \ll |X|$. Better than CBC !

An example

$$\mathrm{Adv}_{\mathrm{CPA}}[A, E_{\mathrm{CTR}}] \le 2\cdot\mathrm{Adv}_{\mathrm{PRF}}[B, E] + \mathbf{2\,q^2\,L\,/\,|X|}$$

q = # messages encrypted with k , L = length of max message

Suppose we want $\mathrm{Adv}_{\mathrm{CPA}}[A, E_{\mathrm{CTR}}] \le 1/2^{32}$ $\Leftarrow$ $q^2 L / |X| < 1/ 2^{32}$

- AES: $|X| = 2^{128}$ $\Rightarrow$ $q\, L^{1/2} < 2^{48}$

So, after 2^{32} CTs each of len 2^{32}, must change key

(total of 2^{64} AES blocks)

Comparison: ctr vs. CBC

	CBC	ctr mode
uses	PRP	PRF
parallel processing	No	Yes
Security of rand. enc.	$q^2 L^2 \ll \|X\|$	$q^2 L \ll \|X\|$
dummy padding block	Yes	No
1 byte msgs (nonce-based)	16x expansion	no expansion

(for CBC, dummy padding block can be solved using ciphertext stealing)

Summary

- PRPs and PRFs: a useful abstraction of block ciphers.

- We examined two security notions: (security against eavesdropping)
  1. Semantic security against one-time CPA.
  2. Semantic security against many-time CPA.

  Note: neither mode ensures data integrity.

- Stated security results summarized in the following table:

Power / Goal	**one-time key**	**Many-time key (CPA)**	**CPA and integrity**
Sem. Sec.	steam-ciphers det. ctr-mode	rand CBC rand ctr-mode	later

Further reading

- A concrete security treatment of symmetric encryption: Analysis of the DES modes of operation, M. Bellare, A. Desai, E. Jokipii and P. Rogaway, FOCS 1997

- Nonce-Based Symmetric Encryption, P. Rogaway, FSE 2004

End of Segment