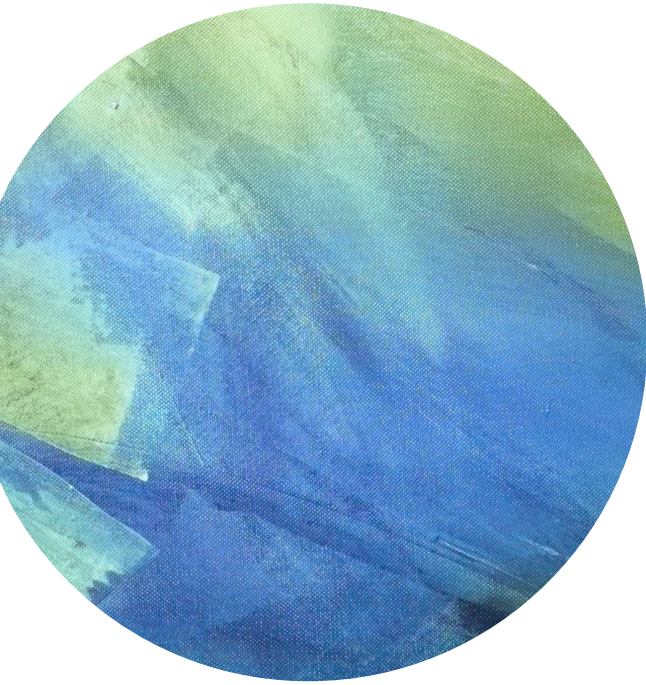
The background of the slide is an abstract composition of broad, textured brushstrokes. The color palette is dominated by various shades of green and blue, ranging from light, almost white-green to deep, dark blues. The strokes are layered and overlapping, creating a sense of depth and movement. The overall effect is reminiscent of an impressionistic or expressionist painting. A white horizontal band is positioned in the lower third of the image, containing the text 'Lecture 5'.

Lecture 5



# Outline



Block Ciphers, PRF,  
PRP



Modes of Operation  
for Block Ciphers



# Administrative Details

- Scribe volunteer

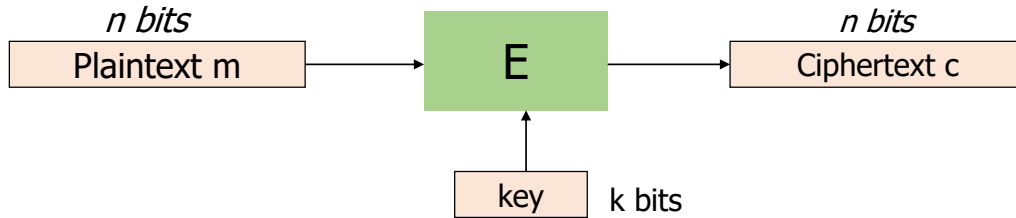
*Meghan*

# Block Ciphers

# Block Ciphers

Stream Ciphers:  $E(k, m)$

$$G(k) \oplus m$$



Examples:

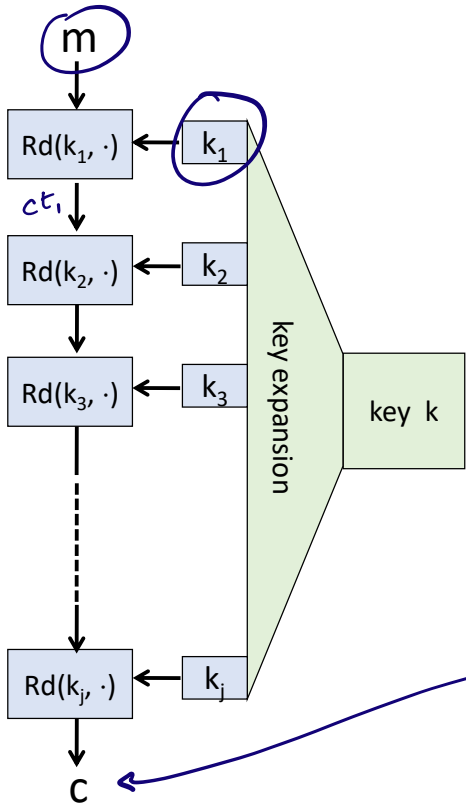
1. DES:  $n = 64$  bits,  $k = 56$  bits

*x Deprecated*

2. 3DES:  $n = 64$  bits,  $k = 168$  bits

3. AES:  $n = 128$  bits,  $k = 128, 192, 256$  bits





Examples:


1. DES:  $k = 56$  bits,  $j = 16$ , each  $k_j = 48$  bits
2. 3DES:  $k = 168$  bits,  $j = 16$ , each  $k_j = 48$  bits
3. AES:  $k = 128/192/256$  bits,  $j = 10$ , each  $k_j = 128$  bits

$$E(k, m)$$

$$D(k, c)$$

# Defining Security for Block Ciphers

↳ "indistinguishable from a random function"

- A pseudorandom function (PRF) is a function from  $(\mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C})$   
s.t.  $F(k, m)$  is efficiently computable for every  $k$  and  $m$   


key    msg    c
- A pseudorandom permutation (PRP) is a function from  $(\mathcal{K} \times \mathcal{X} \rightarrow \mathcal{X})$   
s.t.  $F(k, m)$  is efficiently computable for every  $k$  and  $m$ , and  
 $F(k, \cdot)$  has domain = image and is one-to-one, and  
 $F^{-1}(k, y)$  is efficiently computable for every  $k$  and  $y$   
where  $F^{-1}(k, F(k, x)) = x$

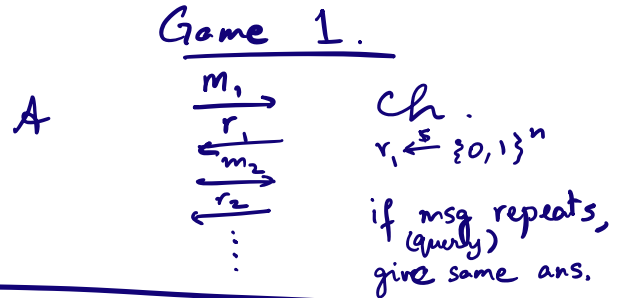
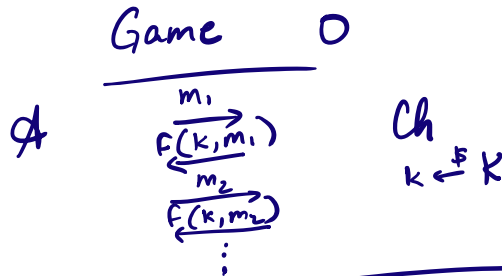
AES, DES are PRPs. In AES,  $|\mathcal{X}| = 2^{128}$  and in DES,  $|\mathcal{X}| = 2^{64}$ .

Permutation:  $\{1, 2, 3 \dots N\} \rightarrow \{1, 2, \dots, N\}$ .  $1 \rightarrow 2$      $3 \rightarrow 4$      $\dots$      $N-1 \rightarrow N$   
 $2 \rightarrow 3$      $4 \rightarrow 5$      $\dots$      $N \rightarrow 1$

# Defining Security for Block Ciphers

$$\text{PRF}_k : \{0,1\}^m \rightarrow \{0,1\}^n$$

- A **pseudorandom function (PRF)** is a function from  $\mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$  s.t.  $F(k, m)$  is efficiently computable for every  $k$  and  $m$  and is indistinguishable from a “random” function for a “random” choice of key



$$|\Pr[\mathcal{A} = 1 \mid \text{Game 0}] - \Pr[\mathcal{A} = 1 \mid \text{Game 1}]| = \text{negl}$$



Can we build a PRF from a PRG?

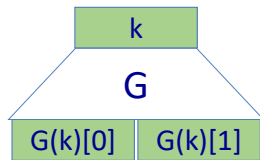
AES( $k, m$ )

$$\{0,1\}^n \rightarrow \{0,1\}^{2^n}$$

Let  $G: \{0,1\}^n \rightarrow \{0,1\}^{2^n}$  be a secure PRG

Define 1-bit PRF  $F: K \times \{0,1\} \rightarrow K$  as

$$F(k, x \in \{0,1\}) = G(k)[x]$$



$F(k, 0)$  = first half of the bits of  $G(k)$   
 $F(k, 1)$  = second half of the bits of  $G(k)$

H.W. Prove that  $F$  is a secure PRF.

(Link to proof on webpage for tree construction)

# Question 1

Let  $F: K \times X \rightarrow X$  be a secure PRP.

Is  $F$  a secure PRF?

1. Always
2. Never
3. Depends on  $F$

## Question 2

Let  $F: K \times X \rightarrow \{0,1\}^{128}$  be a secure PRF.

Is the following  $F'$  a secure PRF?

$$F'(k, x) = \begin{cases} 1^{128} & \text{if } x=0 \\ F(k,x) & \text{otherwise} \end{cases}$$

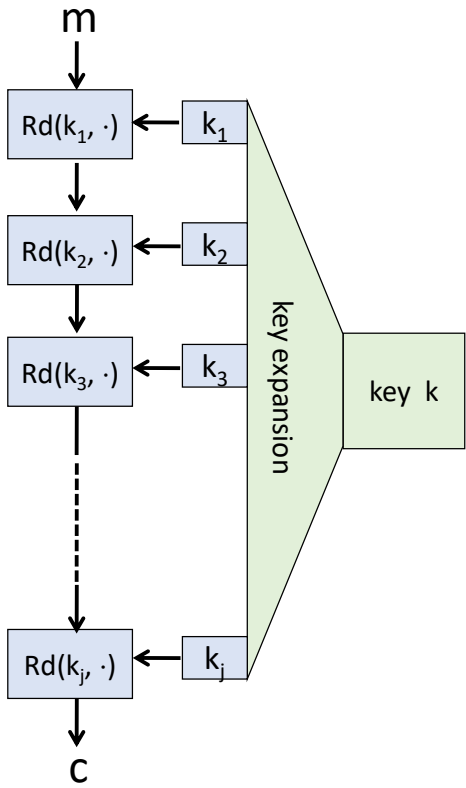
1. Yes
2. No
3. Depends on  $F$

## Question 3

Let  $F: K \times X \rightarrow \{0,1\}^{128}$  be a secure PRF.

Can you build a PRG  $G: K \rightarrow \{0,1\}^{4096}$  from  $F$ ?

DES

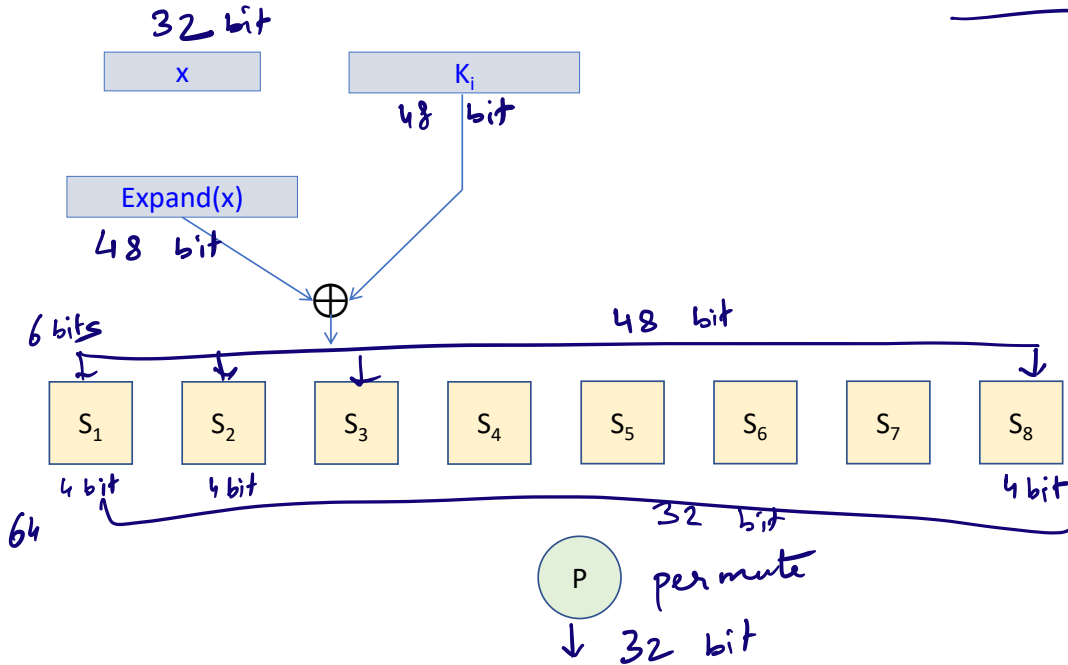


Examples:

- 1. DES:  $k = 56$  bits,  $j = 16$ , each  $k_j = 48$  bits
- 2. 3DES:  $k = 168$  bits,  $j = 16$ , each  $k_j = 48$  bits
- 3. AES:  $k = 128/192/256$  bits,  $j = 10$ , each  $k_j = 128$  bits

Each function  $f_i$  is:

PRF

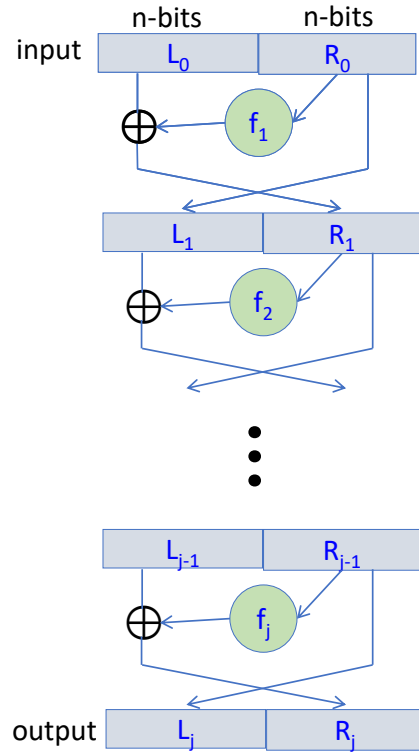


## Inversion.

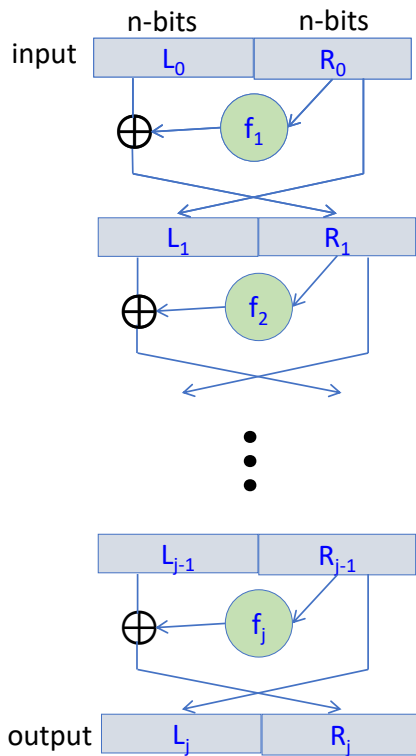
Each round  $Rd_i$ : Feistel Network

Given functions  $f_1, \dots, f_j : \{0,1\}^n \rightarrow \{0,1\}^n$

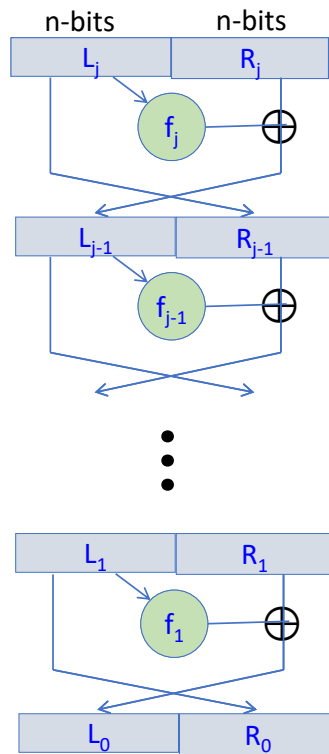
Build an invertible function  $F : \{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$







inverse





# Modes of Operation for Block Ciphers

*or, How to use Block Ciphers*

# One-time Key

128-bit

$$\mathcal{K} \times \mathcal{M} \rightarrow \mathcal{M}.$$

- Goal: build “secure” encryption from a secure PRP (e.g. AES)
- Recall: what is semantic (or CPA/chosen plaintext attack) security

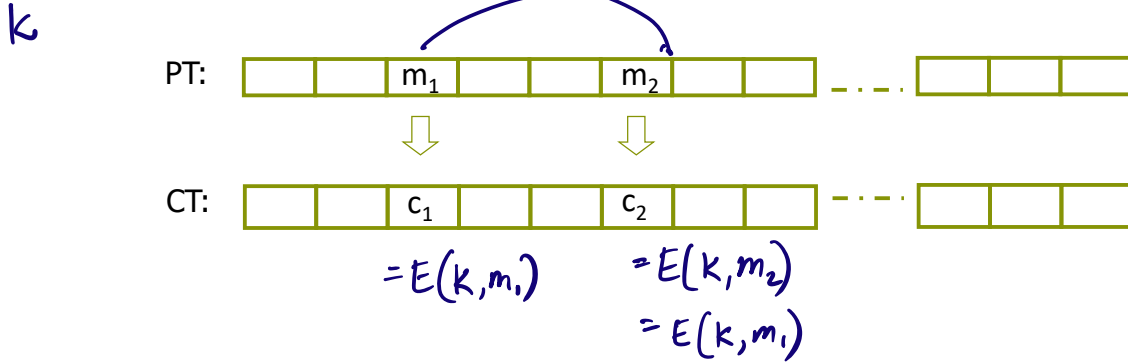
$$\neq m_0, m_1$$

$$\left\{ E(k, m_0) \right\}_{k \leftarrow \mathcal{K}} \not\sim_c \left\{ E(k, m_1) \right\}_{k \leftarrow \mathcal{K}}$$

- ECB mode (electronic code book):  $E(k, m) = \text{PRP}(k, m)$

# Incorrect Use of Block Ciphers

Electronic Code Book (ECB) should not be applied to multiple blocks



## Problem:

- if  $m_1 = m_2$  then  $c_1 = c_2$
- not semantically secure for messages that contain two blocks

# One-time key, but many blocks

Deterministic counter mode from a PRF  $F : \mathcal{K} \times \{0,1\}^n \rightarrow \{0,1\}^n$  ( $n = 128$ )

$$\bullet E_{\text{DETCTR}}(k, m) =$$

m[0]	m[1]	...	m[L]
$\oplus$			
F(k,0)	F(k,1)	...	F(k,L)
c[0]	c[1]	...	c[L]

$\Rightarrow$  Stream cipher built from a PRF (e.g. AES, 3DES)

# One-time Keys

Theorem: For any  $L > 0$ ,

If  $F$  is a secure PRF over  $(\mathcal{K}, \mathcal{X}, \mathcal{X})$  then

$E_{\text{DETCTR}}$  is semantically secure cipher over  $(\mathcal{K}, \mathcal{X}^L, \mathcal{X}^L)$

- example: encrypted email, new key for every message.

# Many-time Keys

## Example applications:

- 1. File systems: Same AES key used to encrypt many files.
- 2. Ipvsec (used in VPN): Same AES key used to encrypt many packets.

## Defining Security:

Recall: one-time security  $\forall m_0, m_1 \in \{0,1\}^{28}$   
 $\{E(k, m_0)\}_{k \leftarrow \mathcal{K}} \approx_c \{E(k, m_1)\}_{k \leftarrow \mathcal{K}}$

Many-time Security  $\forall \vec{m}_0 = (m_0^1, m_0^2, \dots, m_0^n)$  s.t.  $\vec{m}_0 \neq \vec{m}_1$   
 $\vec{m}_1 = (m_1^1, m_1^2, \dots, m_1^n)$   
(No deterministic function can satisfy)  
 $\{E(k, m_0^1), E(k, m_0^2), \dots, E(k, m_0^n)\}_{k \leftarrow \mathcal{K}} \approx_c \{E(k, m_1^1), E(k, m_1^2), \dots, E(k, m_1^n)\}_{k \leftarrow \mathcal{K}}$



# Many-time Keys

If secret key is to be used multiple times  $\Rightarrow$   
given the same plaintext message twice, encryption must produce different outputs.

Solutions?

Deterministic function  $(k, m)$  won't work!

- \* randomize
- \* nonce
- \* counter  $\neq$  chaining.

# Many-time Keys : Solution 1 - PRF

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

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

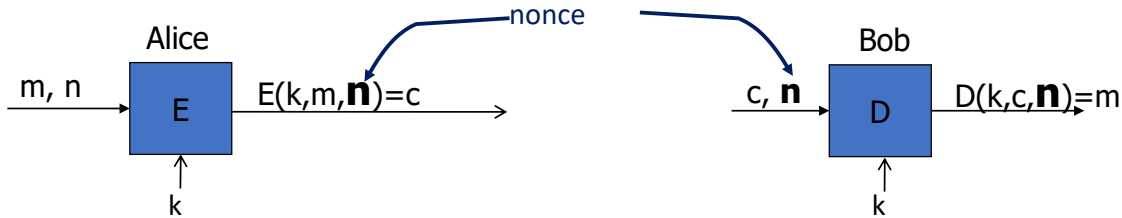
Is  $E$  semantically secure under CPA?

$$\left( \begin{array}{ccc} r_0^1, m_0^1 & r_0^2, m_0^2 & r_0^n, m_0^n \\ \oplus F(k, r_0^1) & \oplus F(k, r_0^2) & \oplus F(k, r_0^n) \end{array} \right)$$

$$\left( \begin{array}{ccc} r_0^1, m_1^1 & r_0^2, m_1^2 & r_0^n, m_1^n \\ \oplus F(k, r_0^1) & \oplus F(k, r_0^2) & \dots \end{array} \right)$$

$$\begin{aligned} &\approx_c \left( \begin{array}{ccc} r_0^1, m_0^1 & m_0^2 & \dots \\ \oplus \text{random}_1 & \oplus \text{random}_2 & \dots \end{array} \right) \\ &= \text{OTP} \\ &\approx_c \left( \begin{array}{ccc} m_1^1 & m_1^2 & \dots \\ \oplus \text{random}_1 & \oplus \text{random}_2 & \dots \end{array} \right) \end{aligned}$$

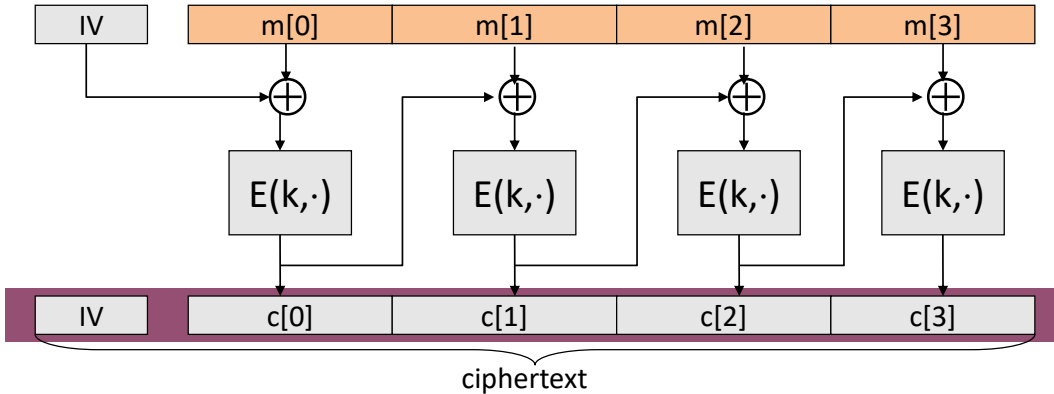
# Solution 2: nonce-based Encryption



- nonce  $n$ : a value that changes from msg to msg.  
( $k, n$ ) pair never used more than once
- method 1: nonce is a **counter** (e.g. packet counter) [SSL, IPsec]
  - used when encryptor keeps state from msg to msg
  - if decryptor has same state, need not send nonce with CT
- method 2: nonce is **random** [File Encryption]

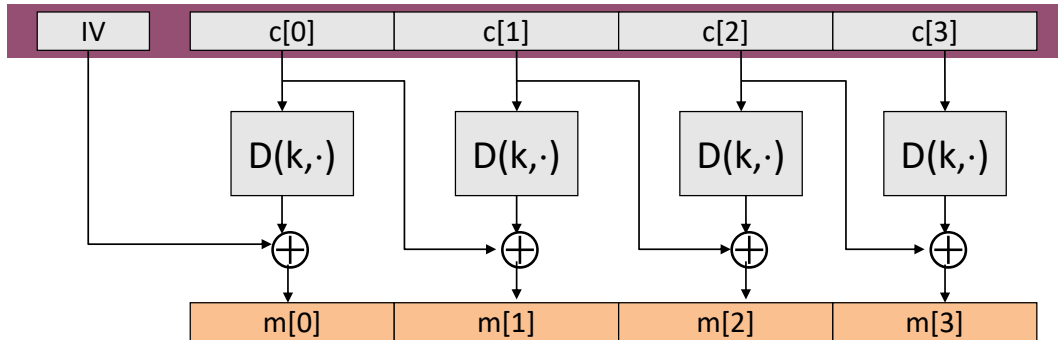
# CBC (Cipher Block Chaining) mode

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



# Decryption Circuit

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



# CPA Security of CBC

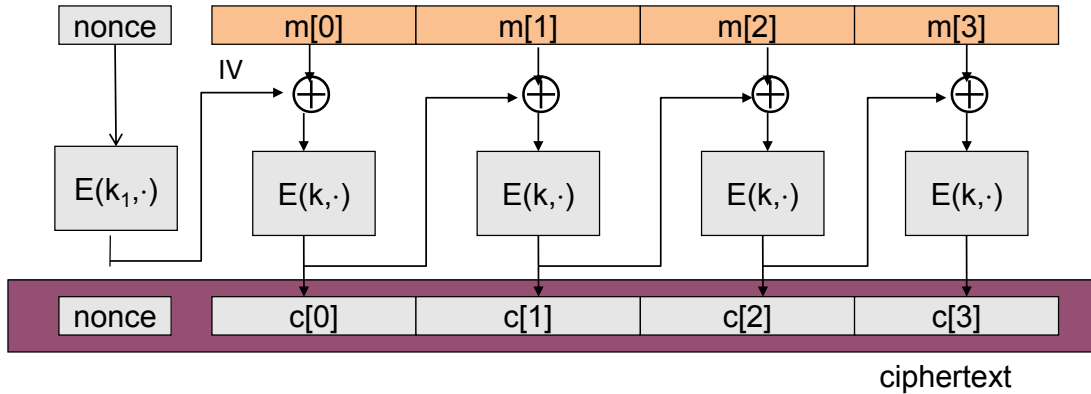
- CBC Theorem: For small enough  $L > 0$ ,  
If  $E$  is a secure PRP over  $(K, X)$  then  
 $E_{\text{CBC}}$  is CPA-secure over  $(K, X^L, X^{L+1})$ .
- In particular, security error in CBC =  $(2 \times \text{sec. error in PRP}) + (q^2 L^2 / |X|)$
- What if IV was predictable? Is it still CPA-secure?

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

What happens if adversary can predict IV

# CBC (Cipher Block Chaining) mode: Version 2

- Cipher block chaining with unique nonce: key = (k,k<sub>1</sub>)  
unique nonce means: (key, n) pair is used for only one message

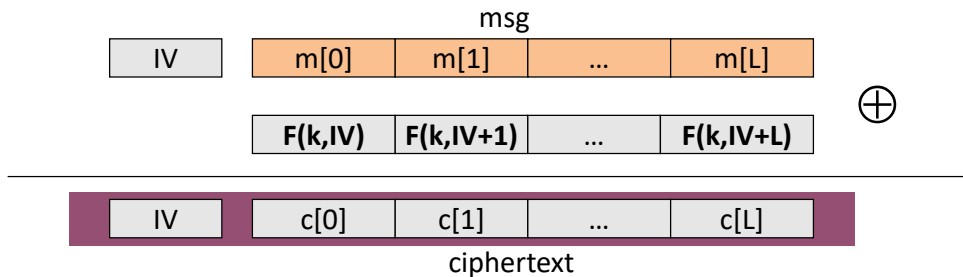




# Rand-ctr mode

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

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



(1) Can use PRF instead of PRP and (2) is parallelizable.

# Summary

- Modes of operation of block-ciphers

$\{m\}$

