CSCI 1510

- Substitution-Permutation Network (continued)
- Feistel Network
- Data Encryption Standard (DES)
- Block Cipher Modes of Operation

Block Cipher

$F: \{0,1\}^n \times \{0,1\}^l \rightarrow \{0,1\}^l$

n: key length

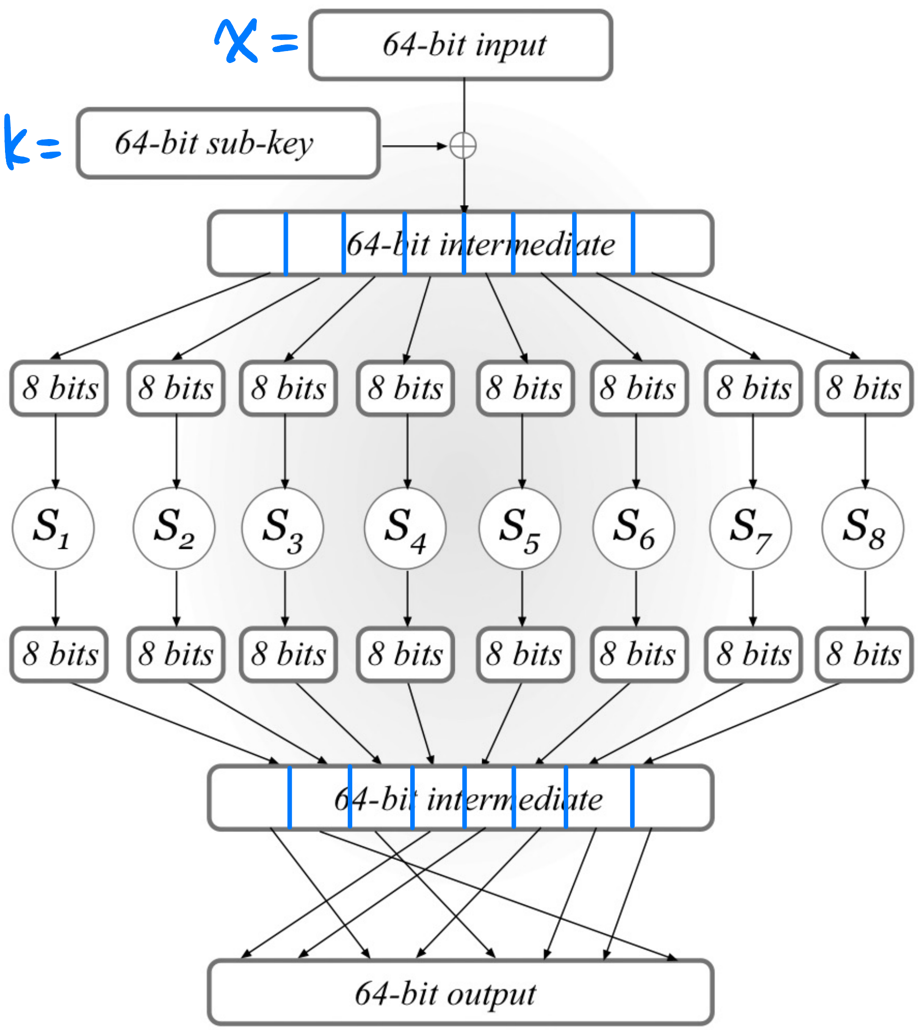
l: block length

$F_k(\cdot)$: permutation / bijective $\{0,1\}^l \rightarrow \{0,1\}^l$

$F_k^{-1}(\cdot)$: efficiently computable given k.

Assumed to be a pseudorandom permutation (PRP).

Substitution-Permutation Network (SPN)



A single round of SPN

"Confusion-Diffusion Paradigm"

Step 1: Key Mixing

$x := x \oplus k$

Step 2: Substitution (Confusion Step)

$S_i : \{0,1\}^8 \rightarrow \{0,1\}^8$ (S-box)

Public permutation / one-to-one map

1-bit change of input

→ at least 2-bit change of output

Step 3: Permutation (Diffusion Step)

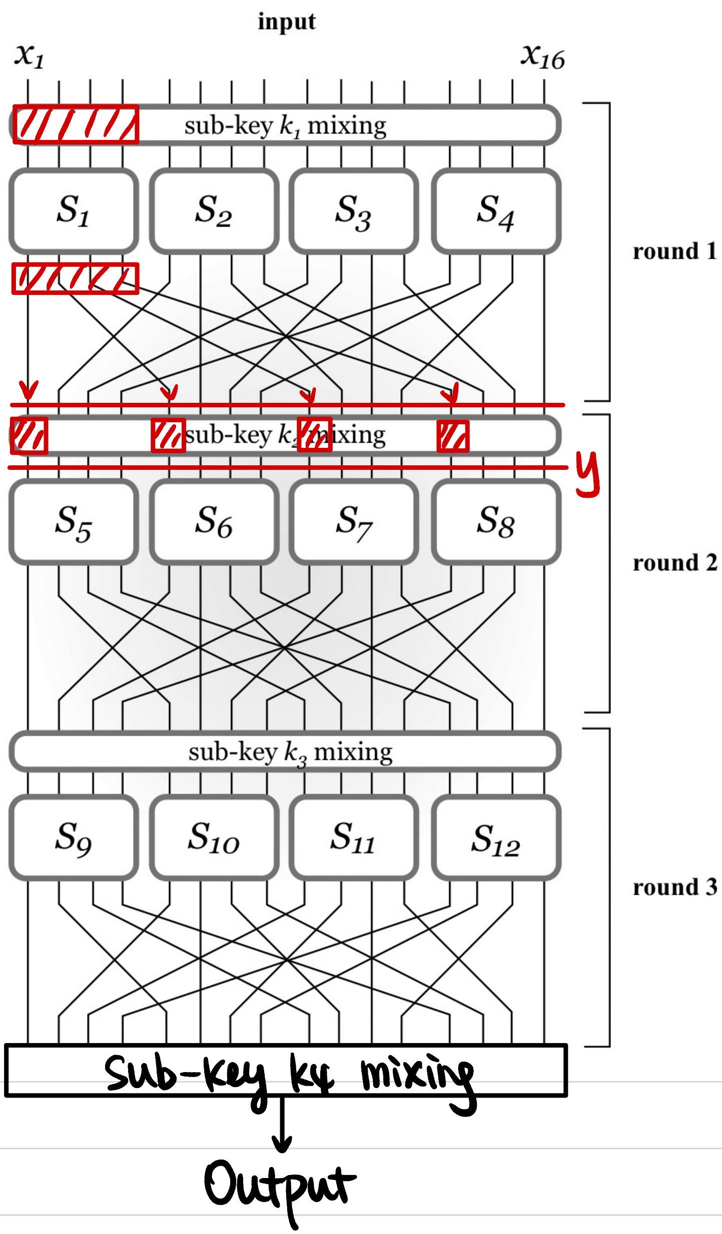
$P : [64] \rightarrow [64]$

Public mixing permutation

↓

affect input to multiple S-boxes next round

Attacks on Reduced-Round SPN



1-round SPN without final key mixing?

C $\xleftarrow{x}$ A

$\xrightarrow{y}$

$\Rightarrow k_1$

1-round SPN with final key mixing?

C $\xleftarrow{x}$ A

$\xrightarrow{y}$

$\xleftarrow{x'}$

$\xrightarrow{y'}$

brute force search on $k_1 \Rightarrow k_2$ $O(2^{16})$

brute force search on each block of k_1

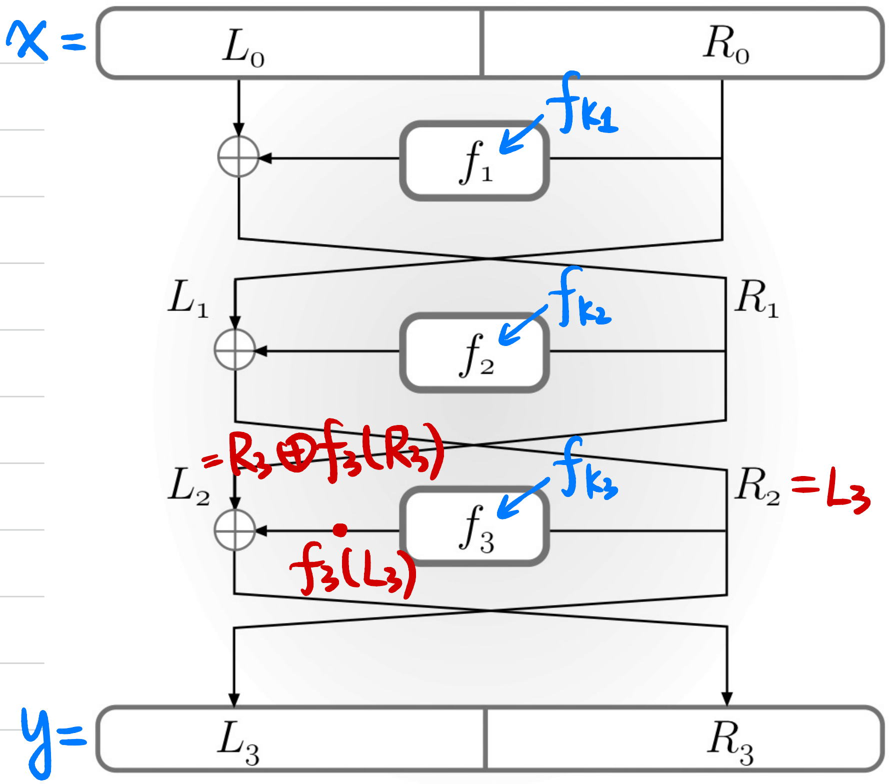
$O(2^4 \cdot 4)$

Why do we need a final key mixing step?

$\Rightarrow$ $(r-1)$-round

Can we do r-round key mixing, then r-round substitution, then r-round permutation? $\Rightarrow$ 1-round

Feistel Network



3-round Feistel Network

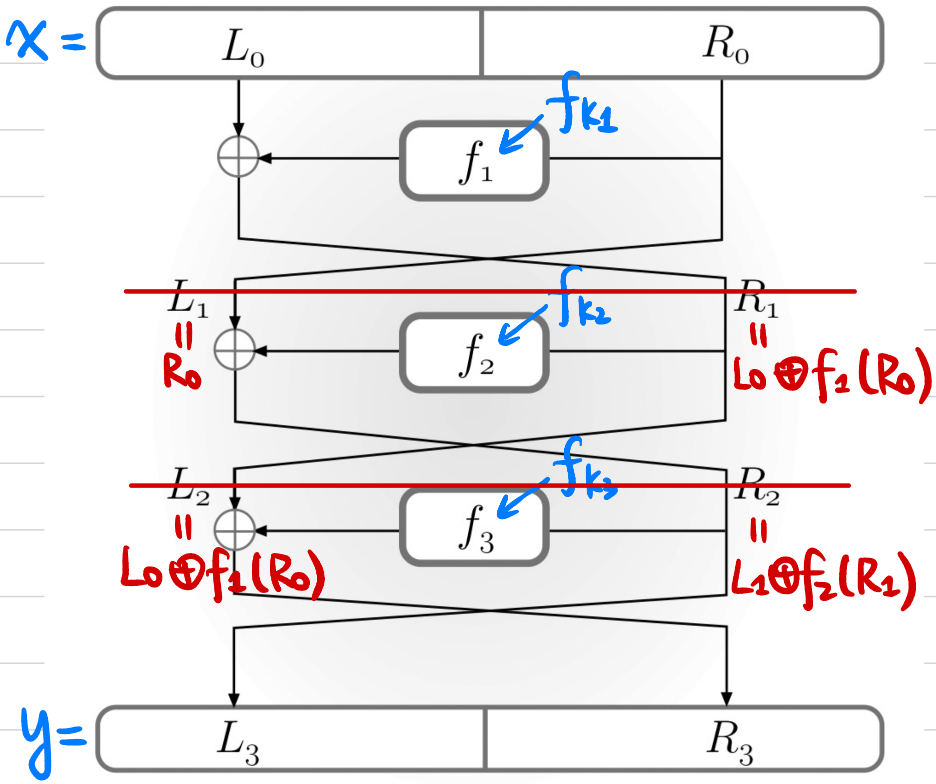
$f_{k_i} : \{0,1\}^{n/2} \to \{0,1\}^{n/2}$

↑

round function

How to compute $F_k^{-1}(y)$?

Attacks on Reduced-Round Feistel Network



1-round? Feistel Network or PRF?

C $\xleftarrow{L_0 \| R_0}$ A

$\xrightarrow{L_1 \| R_1}$

$L_1 \stackrel{?}{=} R_0$

2-round?

C $\xleftarrow{L_0 \| R_0}$ A

$L_0 \oplus f_1(R_0) \leftarrow L_2 \| R_2 \rightarrow$

brute force search on k_1

$\xleftarrow{L_0' \| R_0}$

$L_0' \oplus f_1(R_0) \leftarrow L_2' \| R_2 \rightarrow$

$L_0 \oplus L_0' \stackrel{?}{=} L_2 \oplus L_2'$

Data Encryption Standard (DES)

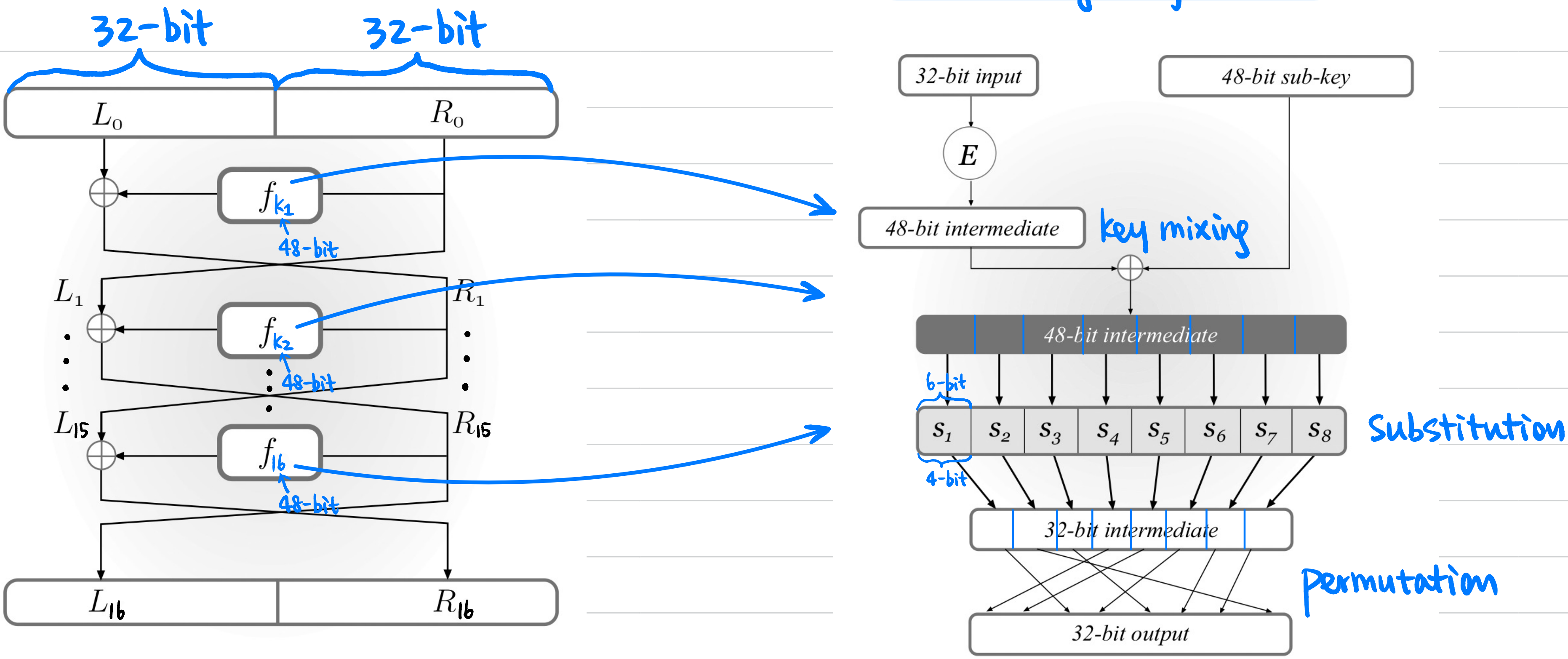
$F: \{0,1\}^n \times \{0,1\}^\ell \to \{0,1\}^\ell$

block length $\ell = 64$

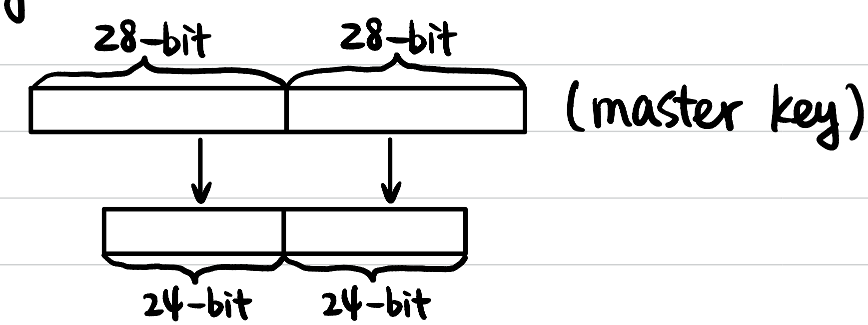
master key length $n = 56$

16-round Feistel Network

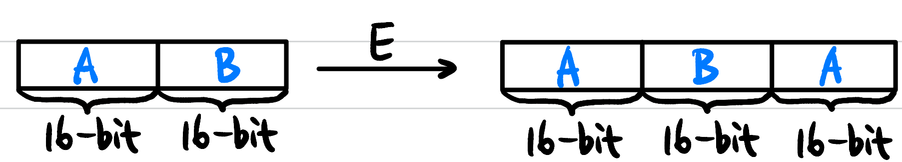
DES mangler function



Key Schedule:

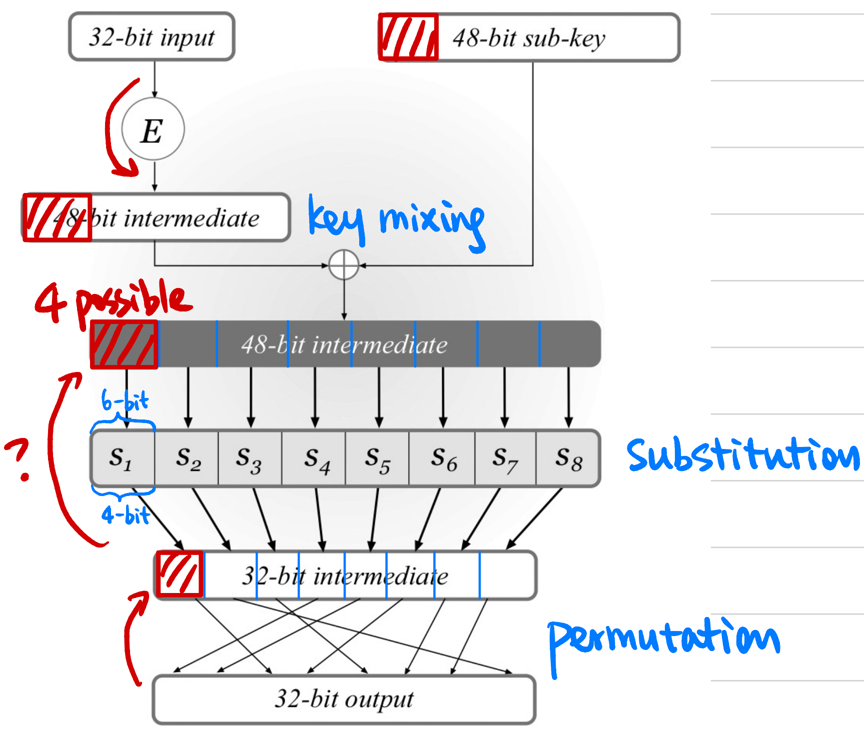


E: expansion function



Data Encryption Standard (DES)

DES mangler function



key recovery: $O(4 \cdot 8)$

S-box: $\{0,1\}^6 \to \{0,1\}^4$

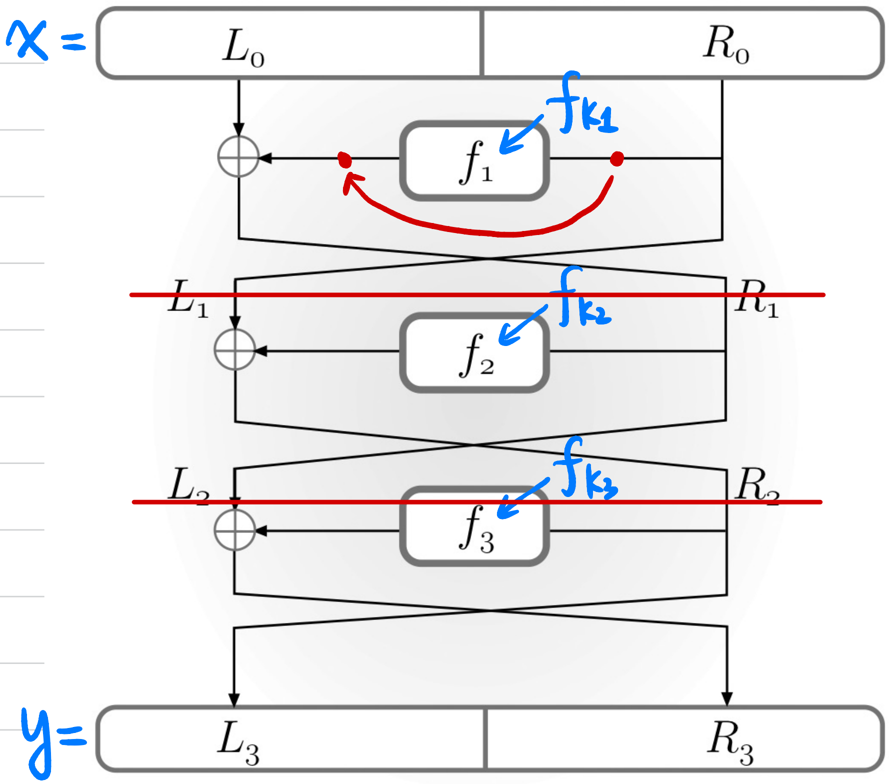
① "4-to-1":
Exactly 4 inputs map to same output

② 1-bit change of input
→ at least 2-bit change of output

Mixing Permutation: $[32] \to [32]$

4 bits from each S-box will affect the input to 6 S-boxes in the next round

Attacks on Reduced-Round SPN



1-round?

Can $\mathcal{A}$ recover sub-key in less than 2^{48} time?

$$C \xleftarrow{L_0 \| R_0} \mathcal{A}$$

$$\xrightarrow{L_1 \| R_1}$$

$L_1 = R_0$

$R_1 = L_0 \oplus f_{k_1}(R_0)$

$\Rightarrow f_{k_1}(R_0) = L_0 \oplus R_1$

Recover k_1 in time $O(4 \cdot 8)$

2-round?

$$C \xleftarrow{L_0 \| R_0} \mathcal{A}$$

$$\xrightarrow{L_2 \| R_2}$$

$L_2 = L_0 \oplus f_{k_1}(R_0) \Rightarrow$ Recover k_1

$\Downarrow$

R_1

$\Downarrow$

$R_2 = L_1 \oplus f_{k_2}(R_1) \Rightarrow$ Recover k_2

Advanced Encryption Standard (AES)

$F: \{0,1\}^n \times \{0,1\}^l \to \{0,1\}^l$

n: key length

l: block length

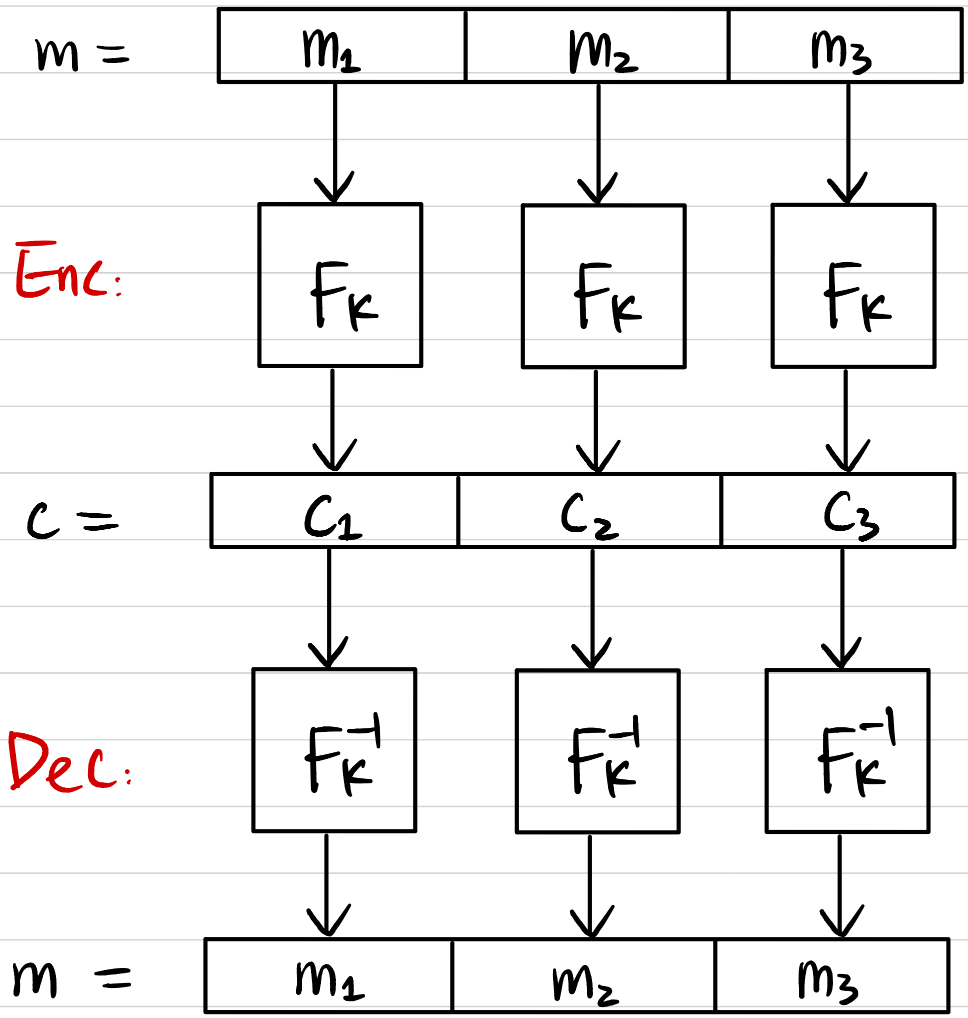
- $n = 128/192/256$, $l = 128$
- Standardized by NIST in 2001
- Competition 1997-2000

Block Cipher Modes of Operation

$F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$

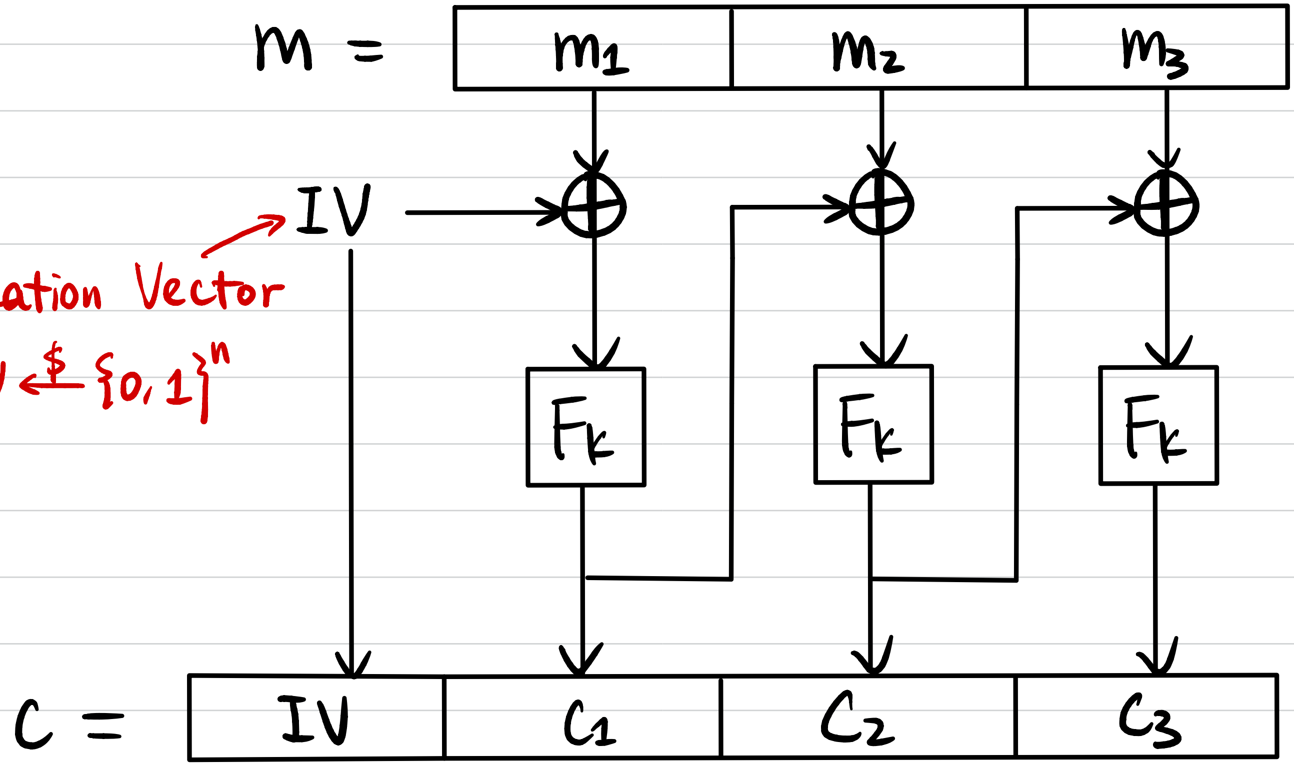
Goal: Construct a CPA-secure encryption scheme for arbitrary-length messages.

Electronic Code Book (ECB) Mode



CPA Secure ? No!

Cipher Block Chaining (CBC) Mode



Initialization Vector

$IV \xleftarrow{\$} \{0,1\}^n$

$\mathcal{H}_0$: $Enc(m_0)$

$\mathcal{H}_1$: $F_k \to f$

$\mathcal{H}_2$: $m_0 \to m_1$

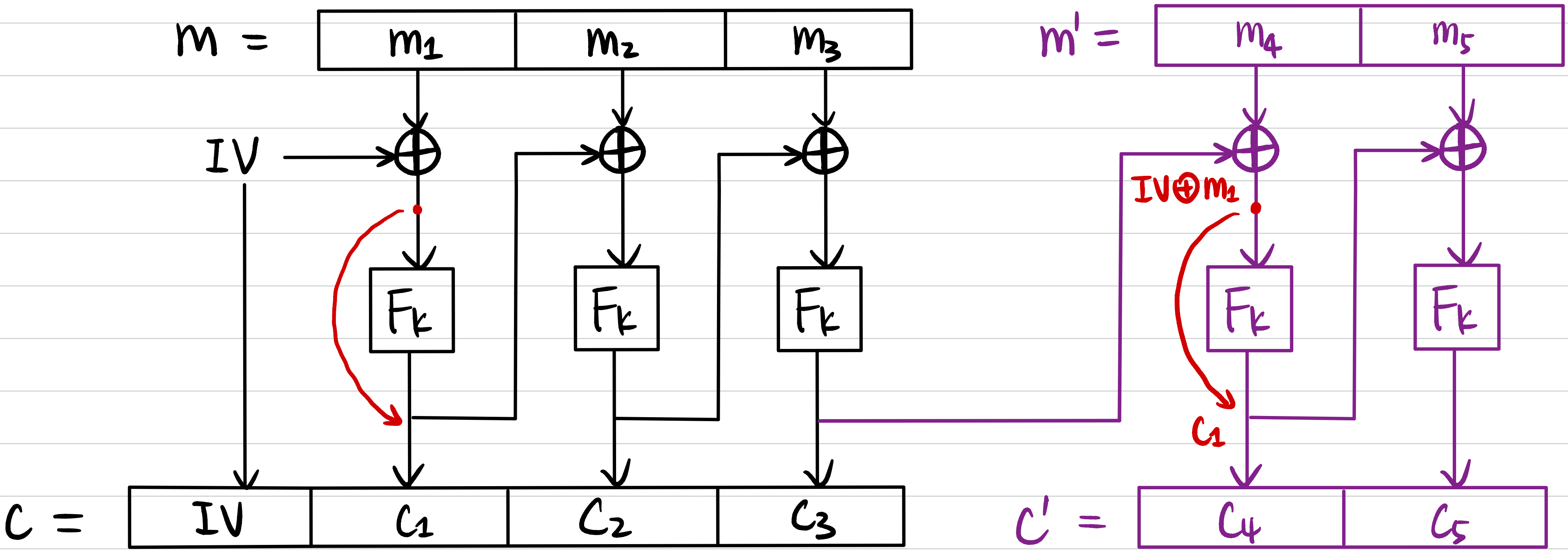
$\mathcal{H}_3$: $f \to F_k$

How to decrypt? $F_k^{-1}(c_i) \oplus c_{i-1} \to m_i$

CPA secure? Yes!

Can we parallelize the computation? No for Enc, Yes for Dec.

Chained Cipher Block Chaining (CBC) Mode



CPA Secure ?

$\mathcal{C}$ $\mathcal{A}$

$\xleftarrow{m_1 \| m_2 \| m_3}$

$\xrightarrow{c = IV \| c_1 \| c_2 \| c_3}$

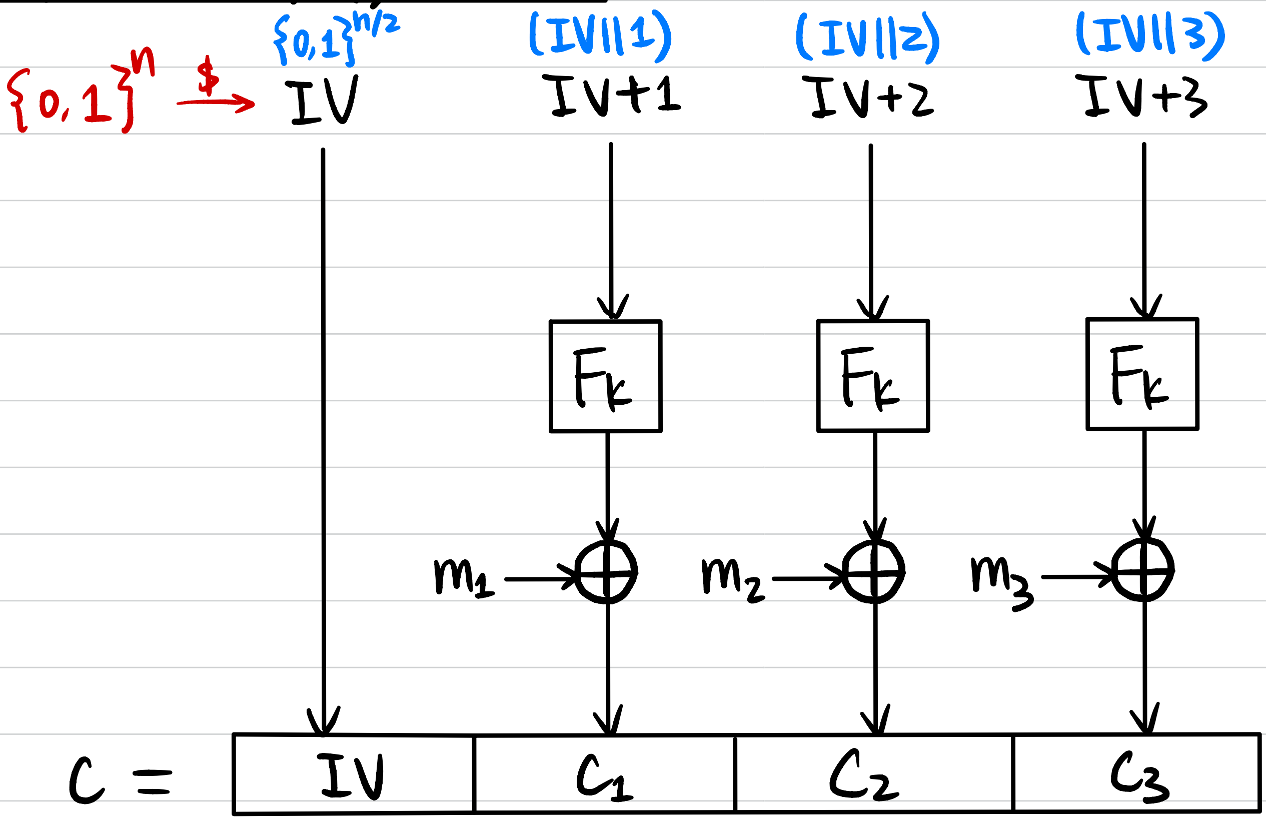
$m_0^* = c_3 \oplus IV \oplus m_1$

$m_1^* = \text{arbitrary}$

$\xrightarrow{c^*}$

$c^* \stackrel{?}{=} c_1$

Counter (CTR) Mode



$\mathcal{H}_0$: $Enc(m_0)$

$\mathcal{H}_1$: $F_k \to f$

$\mathcal{H}_2$: $m_0 \to m_1$

$\mathcal{H}_3$: $f \to F_k$

How to decrypt? $F_k(IV+i) \oplus c_i \Rightarrow m_i$

CPA Secure? Yes!

Can we parallelize the computation? Yes!

PRG from PRF $G: \{0,1\}^{2n} \to \{0,1\}^{k \cdot n}$