CSCI 1510

This Lecture:

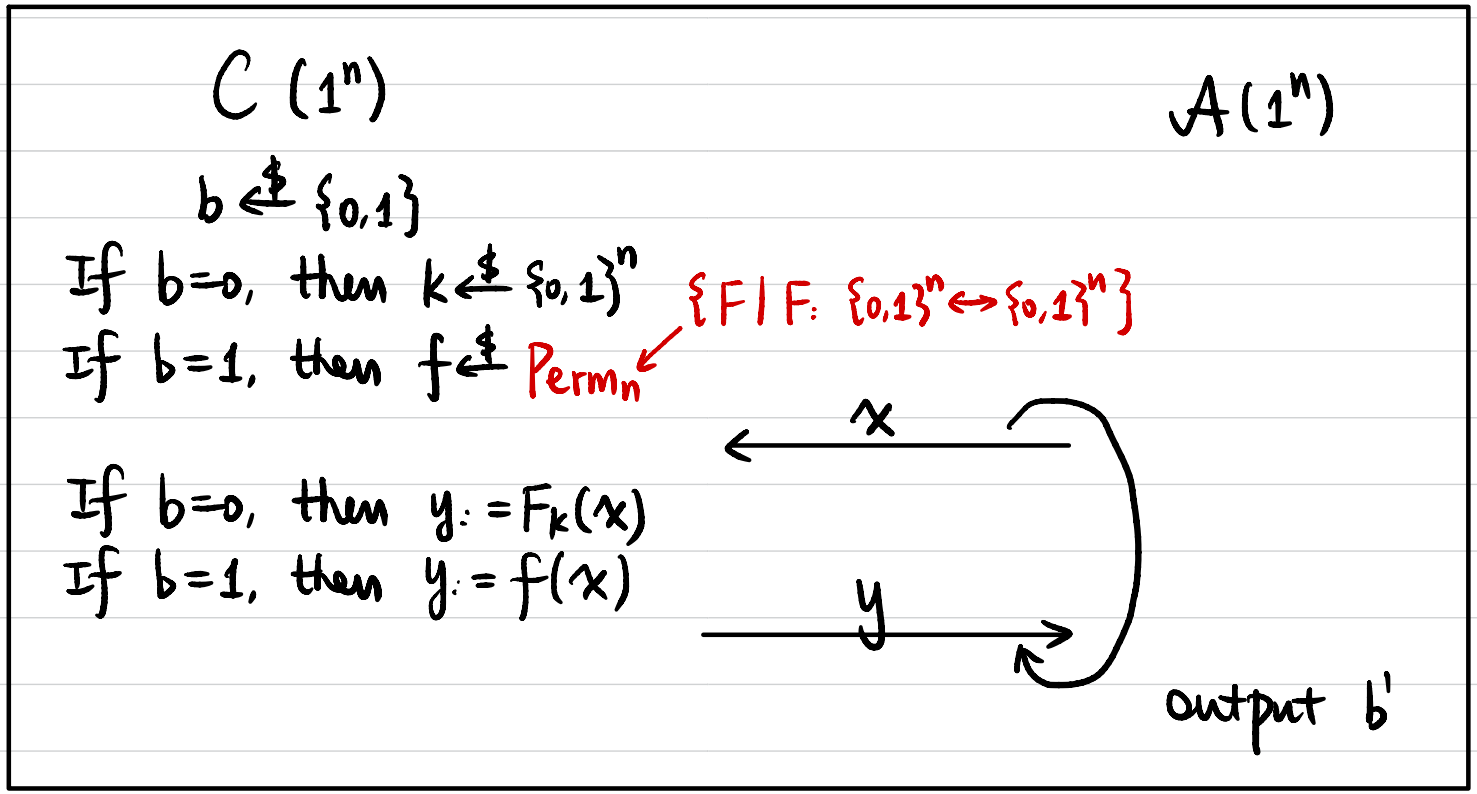
- Constructions of Block Cipher (continued)
- Data Encryption Standard (DES)
- Block Cipher Modes of Operation

Pseudorandom Permutation (PRP)

Def Let $F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a deterministic, poly-time, keyed function. F is a **pseudorandom permutation (PRP)** if $F_k(\cdot)$ is bijective for all k, $F_k^{-1}(\cdot)$ is poly-time computable

$\forall$ PPT A, $\exists$ negligible function $\varepsilon(\cdot)$ s.t.

$$\left| \Pr_{k \leftarrow U_n}[A^{F_k(\cdot)}(1^n) = 1] - \Pr_{f \xleftarrow{\$} Perm_n}[A^{f(\cdot)}(1^n) = 1] \right| \leq \varepsilon(n)$$



$$\Pr[b = b'] \leq \frac{1}{2} + \varepsilon(n)$$

Block Cipher

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

n: key length

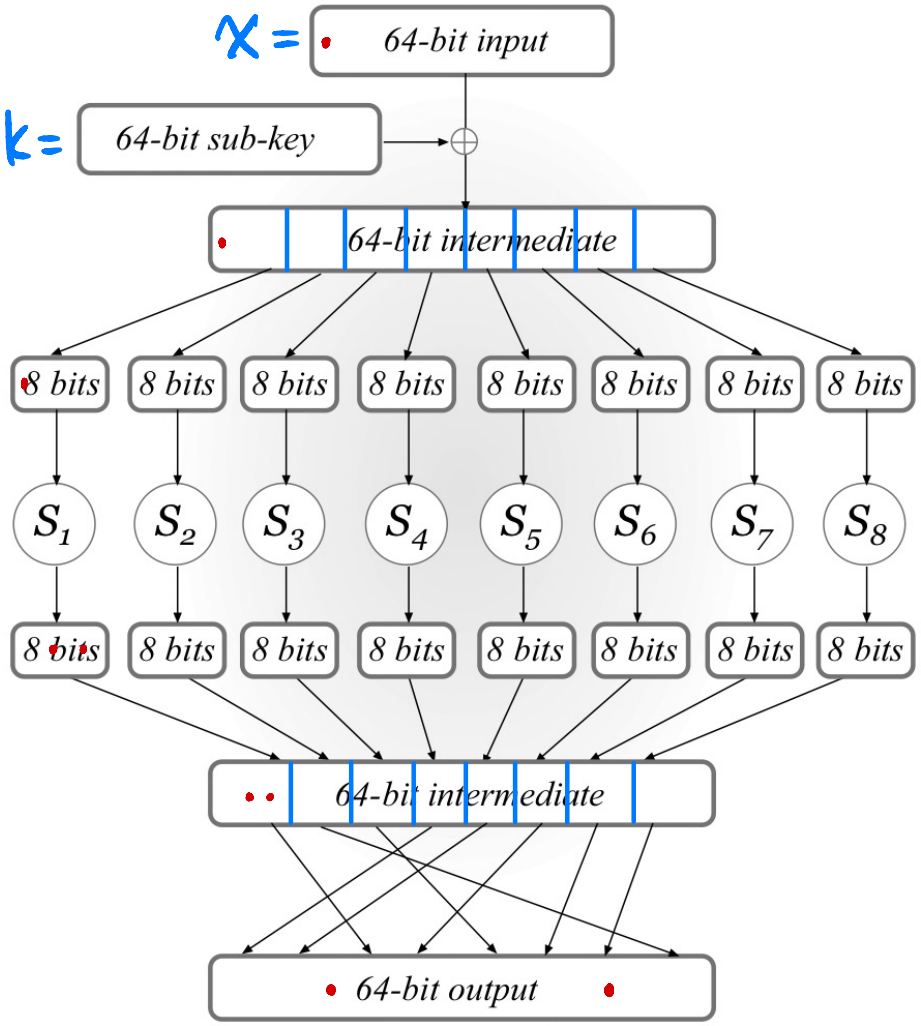
l: block length

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

$F_k^{-1}(\cdot)$: 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)

$S_i : \{0,1\}^8 \to \{0,1\}^8$ (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)

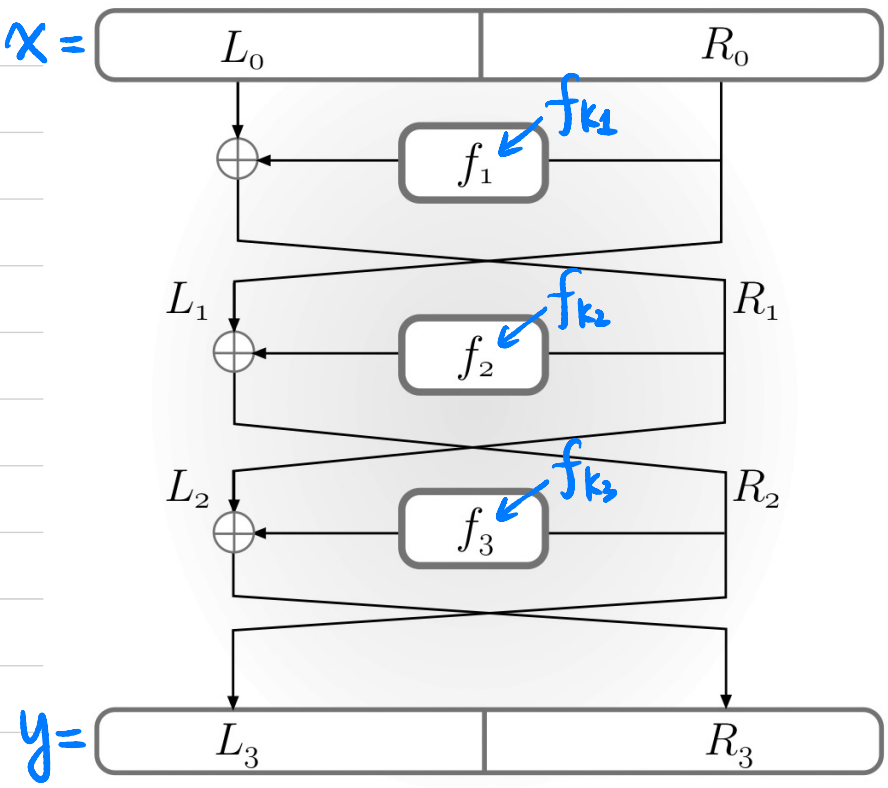
$P : [64] \to [64]$

Public mixing permutation

↓

affect input to multiple S-boxes next round

Feistel Network



3-round Feistel Network

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

↑ round function

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

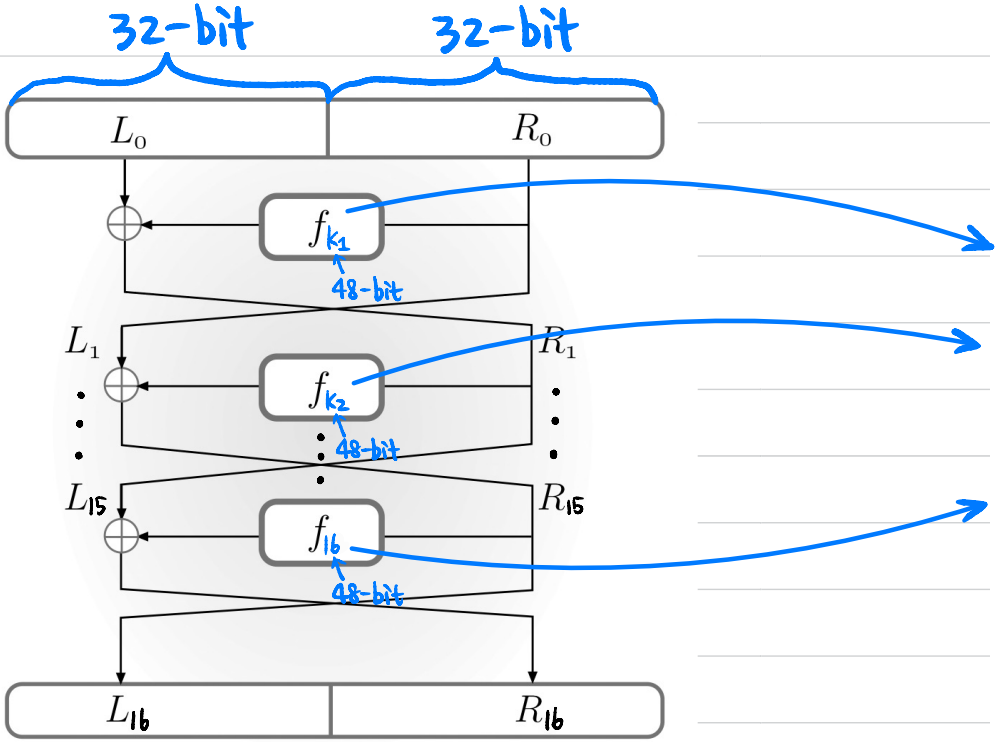
Data Encryption Standard (DES)

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

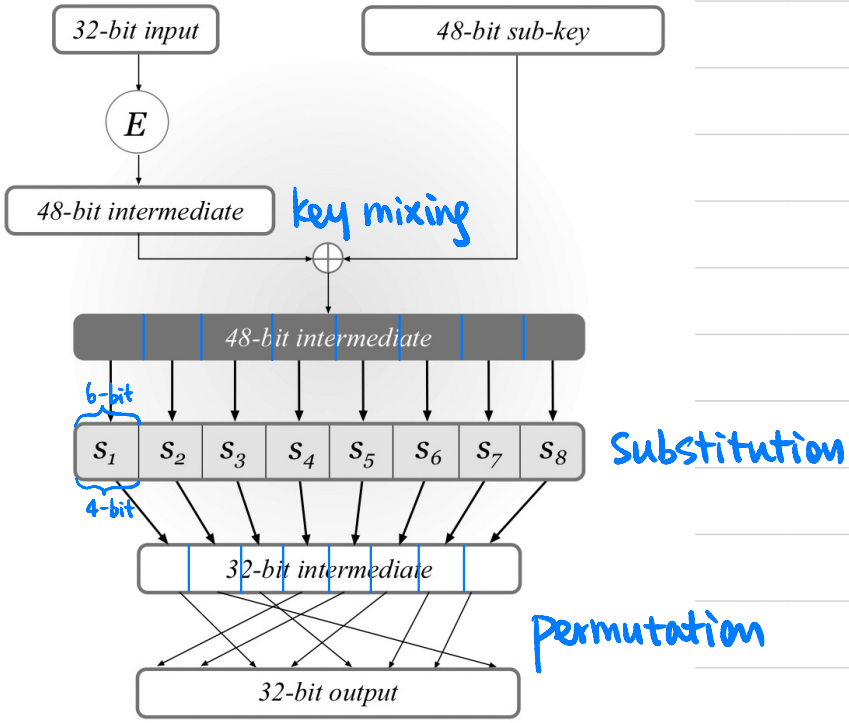
block length $l = 64$

master key length $n = 56$

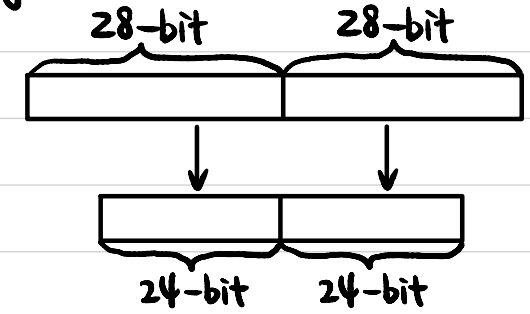
16-round Feistel Network



DES mangler function

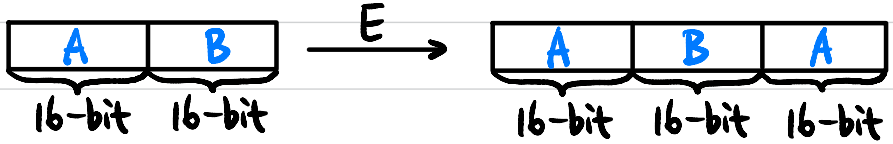


Key Schedule:



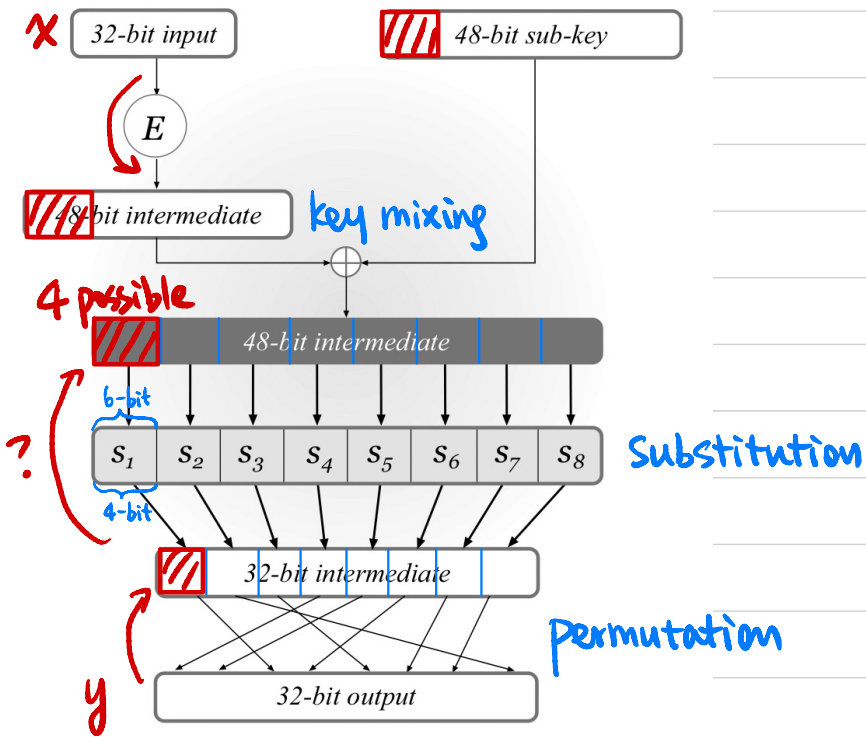
(master key)

E: expansion function



Data Encryption Standard (DES)

DES mangler function



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

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

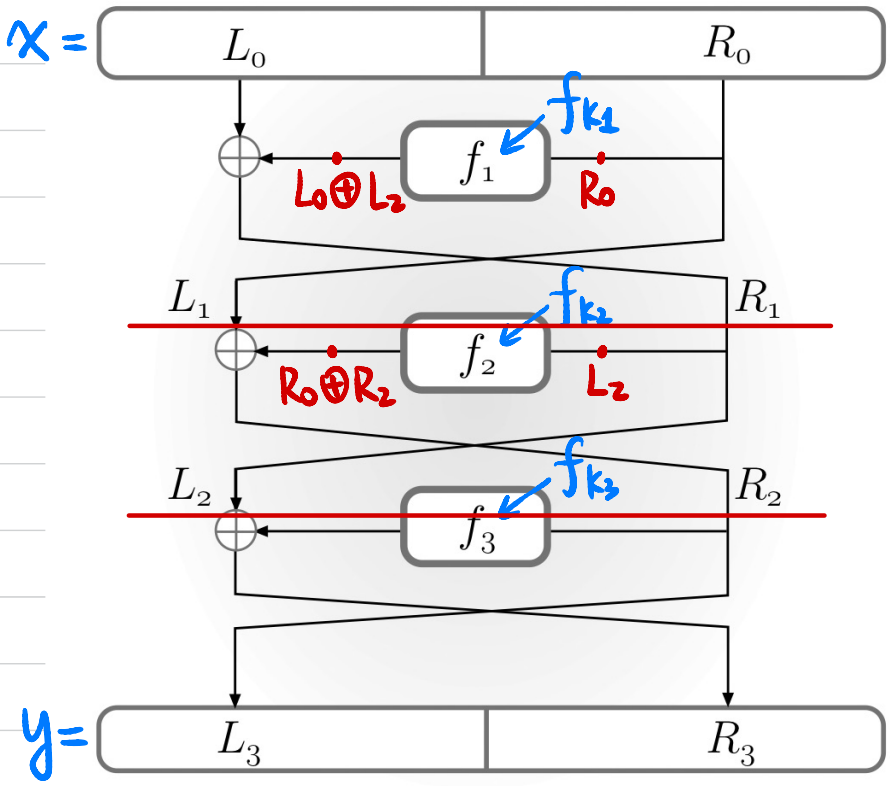
① "4-to-1":
Exactly 4 inputs map to same output

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

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

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

Attacks on Reduced-Round DES



1-round ?

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

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

$L_1 \| R_1 \rightarrow$

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

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

$\xleftarrow{L_0' \| R_0'}$

$L_1' \| R_1' \rightarrow$ Verify

2-round ?

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

$L_2 \| R_2 \rightarrow$

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

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

$f_{k_2}(L_2) = R_0 \oplus R_2$

Recover k_2 in time $O(4 \cdot 8)$

Advanced Encryption Standard (AES)

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

n: key length

l: block length

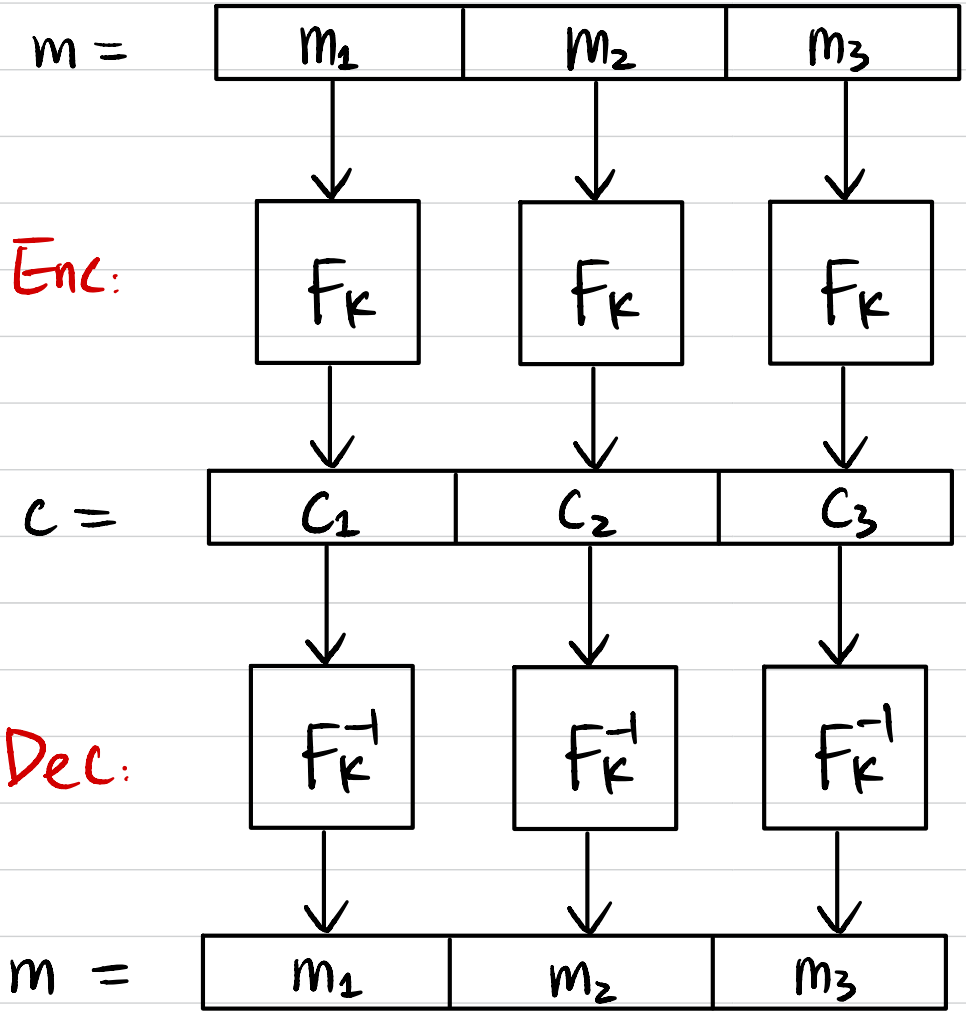
- $n = 128/192/256$, $l = 128$
- Standardized by NIST in 2001
- Competition 1997-2000

Block Cipher Modes of Operation

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

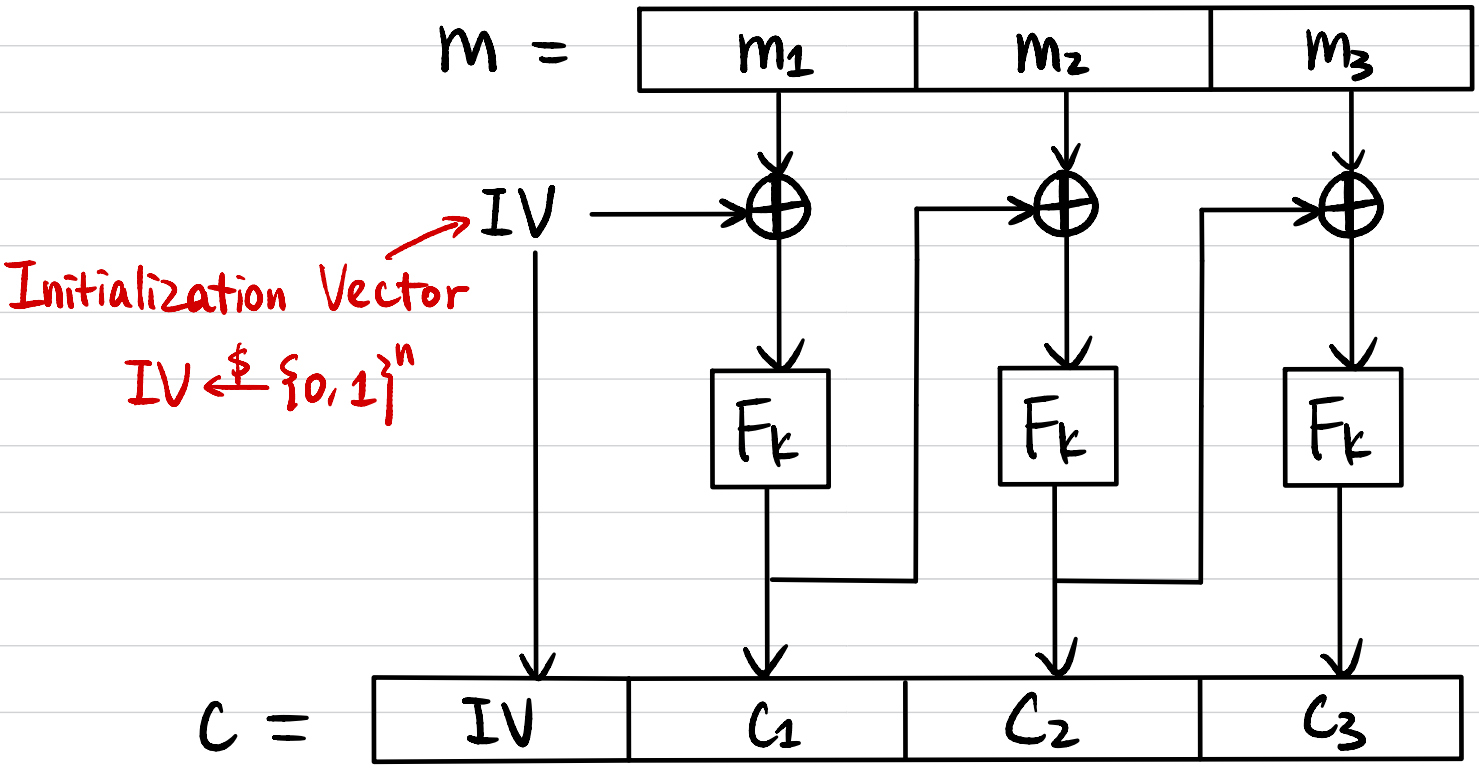
Goal: Construct a CPA-secure encryption scheme for arbitrary-length messages.

Electronic Code Book (ECB) Mode



CPA secure? No! Deterministic Enc

Cipher Block Chaining (CBC) Mode



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

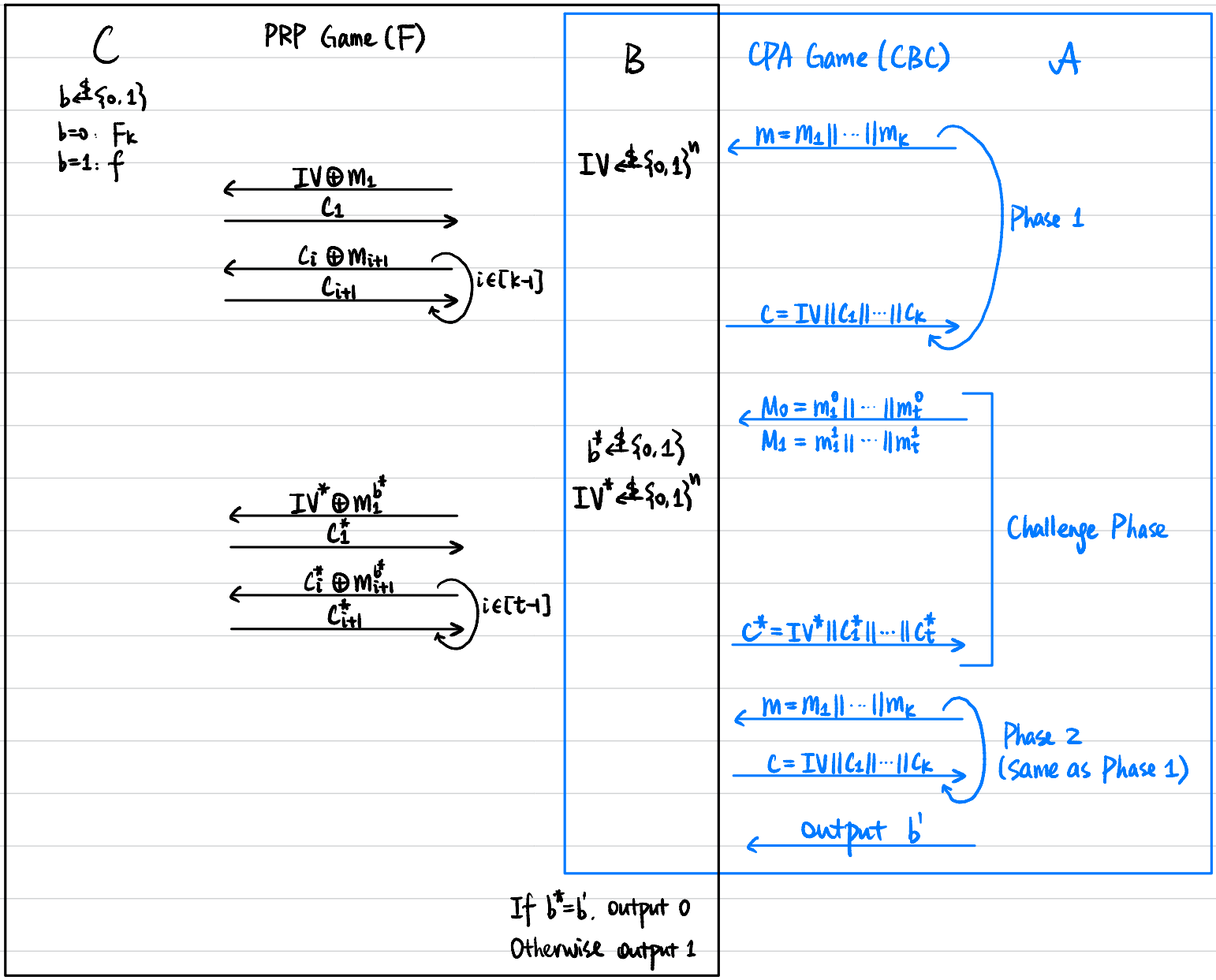
CPA secure? Yes!

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

Theorem If F is a PRP, then block cipher CBC mode is CPA-secure.

Proof Assume not, then $\exists$ PPT $\mathcal{A}$ that breaks CPA security of CBC mode.

We construct PPT B to break the pseudorandomness of F.



Proof (continued)

$$\Pr[B \text{ guesses } b \text{ correctly}] = \Pr[b=0] \cdot \Pr[b^* = b' \mid b=0] + \Pr[b=1] \cdot \left(1 - \Pr[b^* = b' \mid b=1]\right)$$

$\mathcal{A}$ breaks CPA security of CBC $\Rightarrow \Pr[b^* = b' \mid b=0] \geq \frac{1}{2} + \text{non-negl}(n)$

When $b=1$, C uses a random permutation,

the advantage of $\mathcal{A}$ is upper bounded by the probability that inputs to f in c^* collide with other inputs to f.

$$\Rightarrow \Pr[b^* = b' \mid b=1] \leq \frac{1}{2} + \frac{\text{poly}(n)}{2^n} = \frac{1}{2} + \text{negl}(n)$$

$$\Pr[B \text{ guesses } b \text{ correctly}] \geq \frac{1}{2} \cdot \left(\frac{1}{2} + \text{non-negl}(n)\right) + \frac{1}{2} \cdot \left(\frac{1}{2} - \text{negl}(n)\right)$$

$$= \frac{1}{2} + \frac{\text{non-negl}(n)}{2} - \frac{\text{negl}(n)}{2}$$

Alternative Proof:

$\mathcal{H}_0$: CBC mode

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

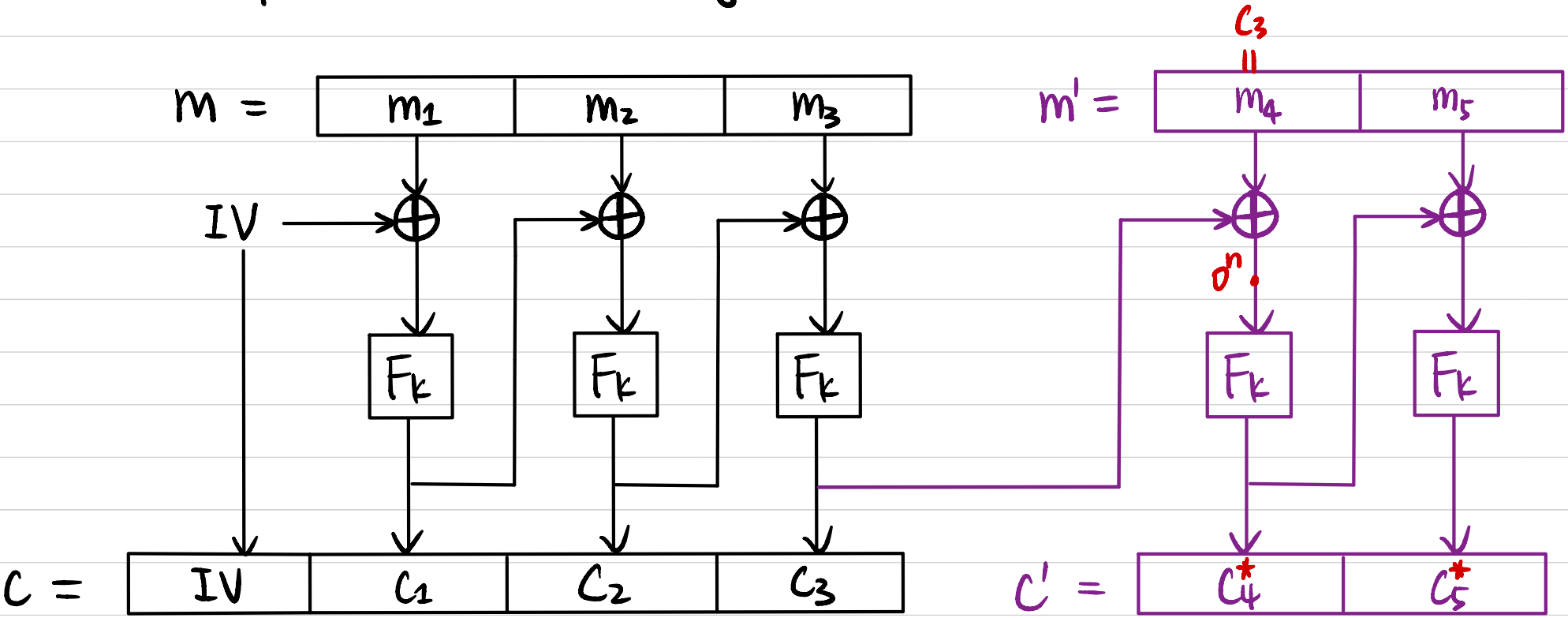
Step 1: $\left| \Pr[A \text{ outputs } 1 \text{ in } \mathcal{H}_0] - \Pr[A \text{ outputs } 1 \text{ in } \mathcal{H}_1] \right| \leq \text{negl}(n)$

(Reduction to PRP security)

Step 2: $\Pr[A \text{ guesses correctly in } \mathcal{H}_1] \leq \frac{1}{2} + \text{negl}(n)$

(Statistical argument)

Chained Cipher Block Chaining (CBC) Mode



CPA Secure ?

C ⟵ A

$m_1 \| m_2 \| m_3$

$C = IV \| C_1 \| C_2 \| C_3$

$M_0 = C_3 \| m_5$

$M_1 = C_3 \| m_5'$

Challenge

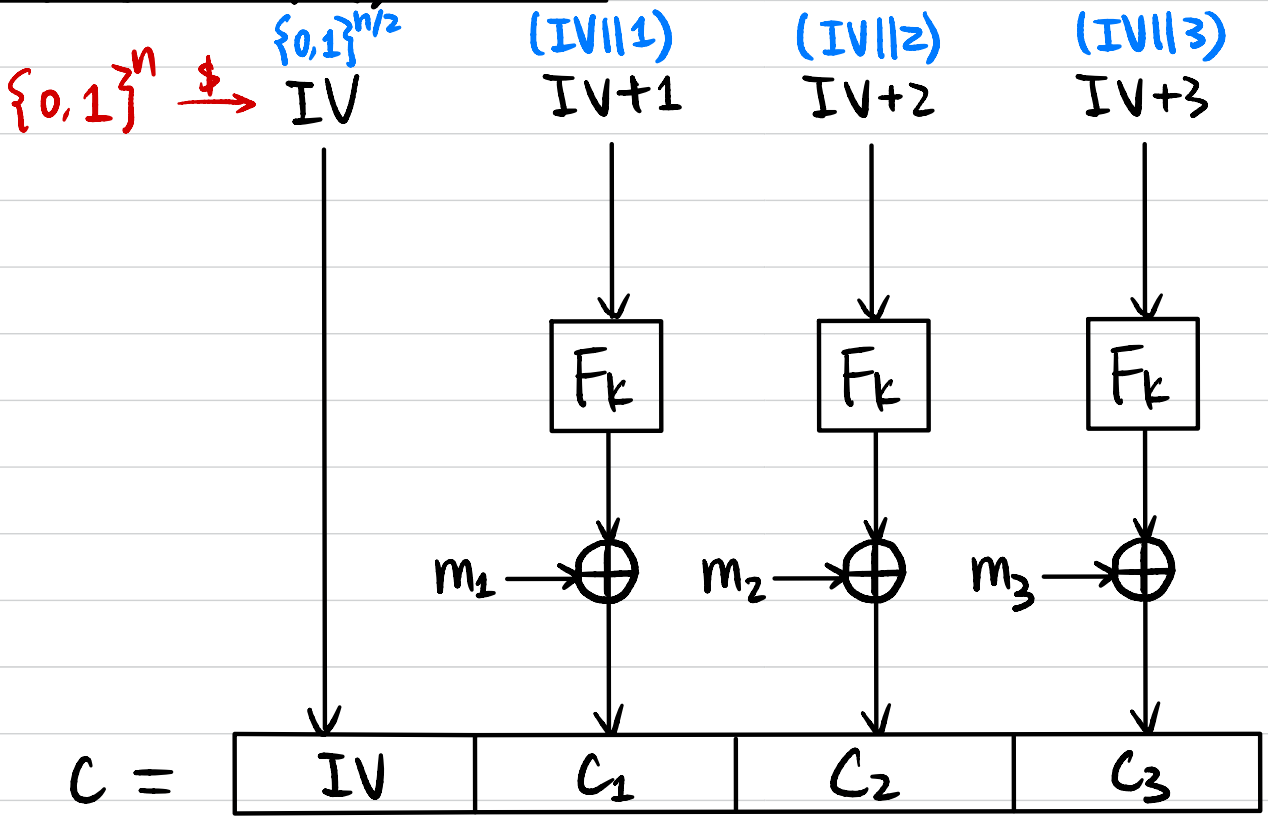
$C^* = C_4^* \| C_5^*$

$C_5^* \| m_5$

$C' = C_6 \| C_7$

$C^* \stackrel{?}{=} C'$

Counter (CTR) Mode



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