CSCI 1510

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

Block Cipher

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

n: key length

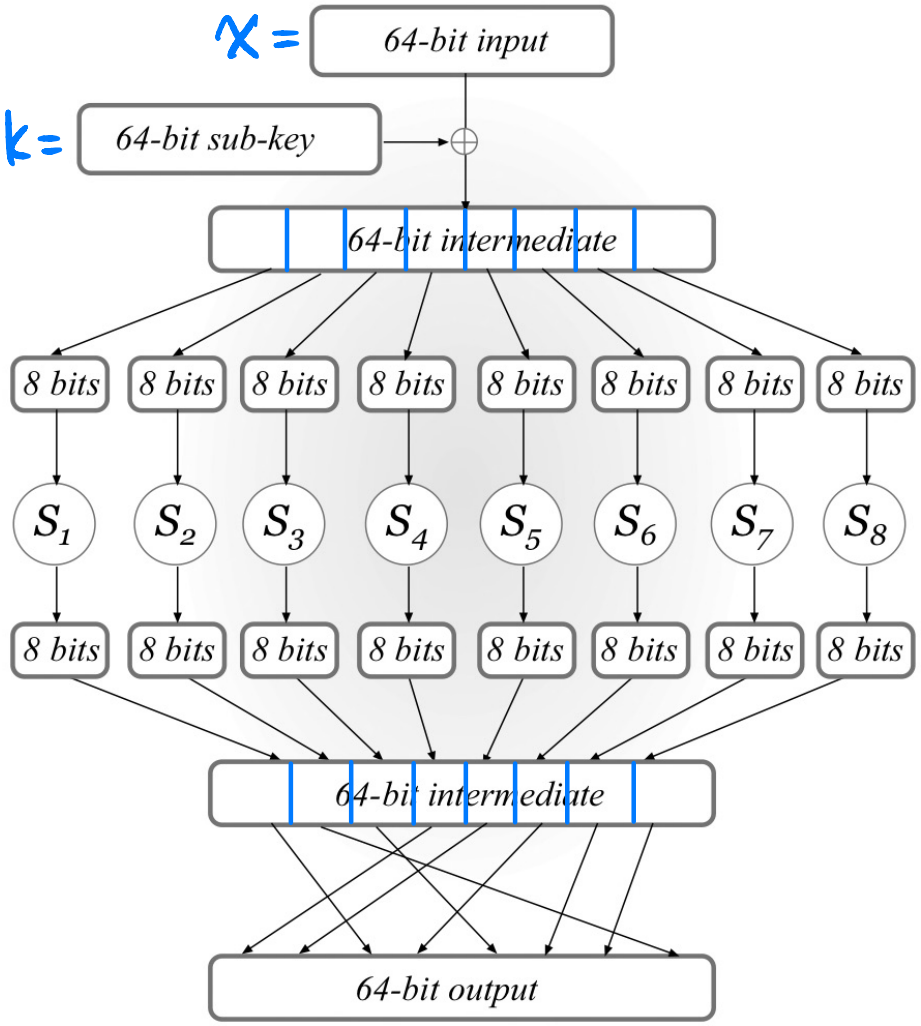
l: block length

$F_k(\cdot)$: 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)

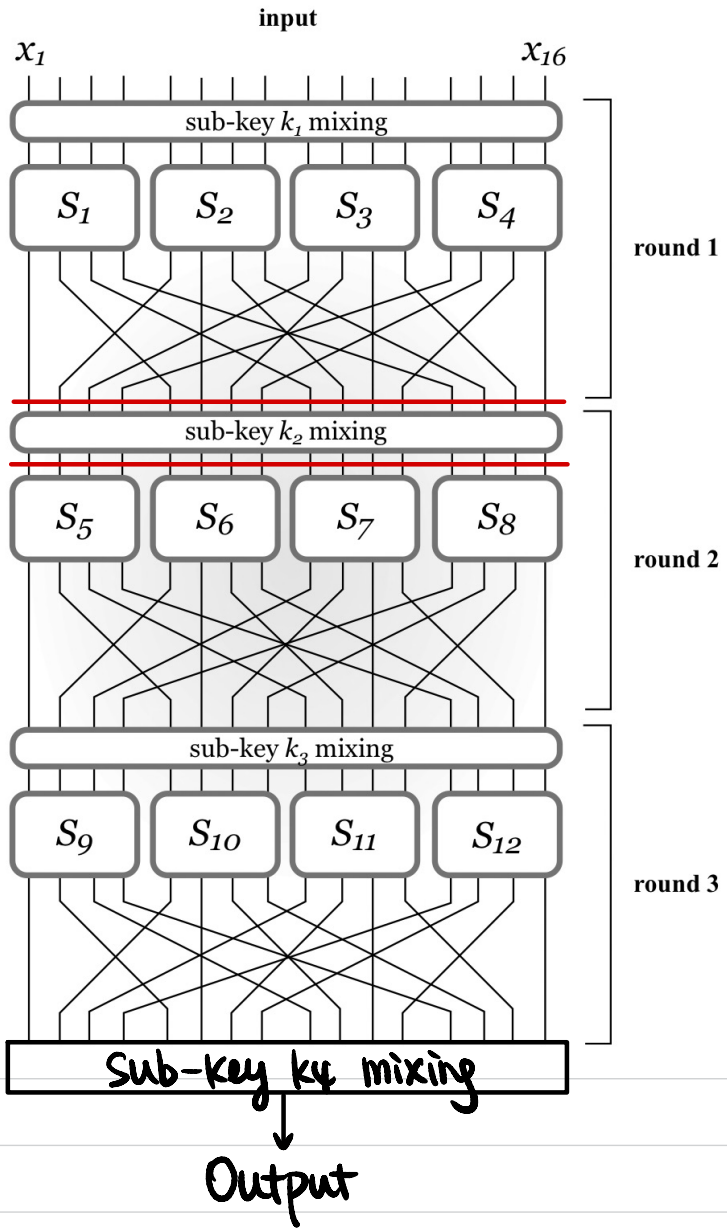
$P : [64] \to [64]$

Public mixing permutation

↓

affect input to multiple S-boxes next round

Attacks on Reduced-Round SPN



1-round SPN without final key mixing?

C ← x ← A

y →

$\Rightarrow k_1$

1-round SPN with final key mixing?

C ← x ← A

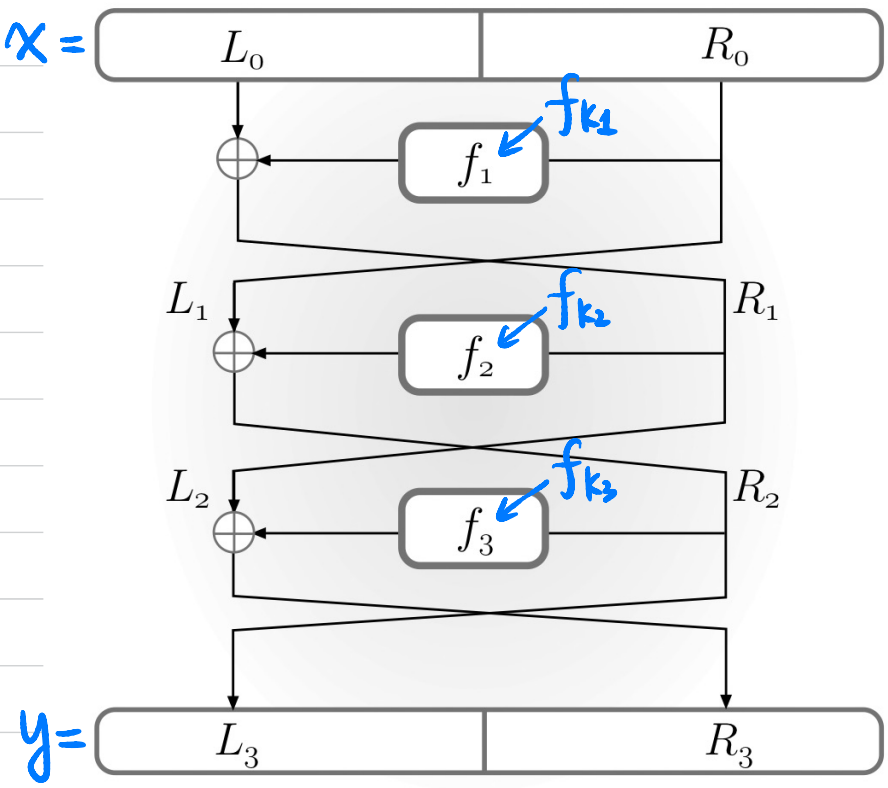
y →

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

Why do we need a final key mixing step?

Can we do r-round key mixing, then r-round substitution, then r-round permutation?

Feistel Network



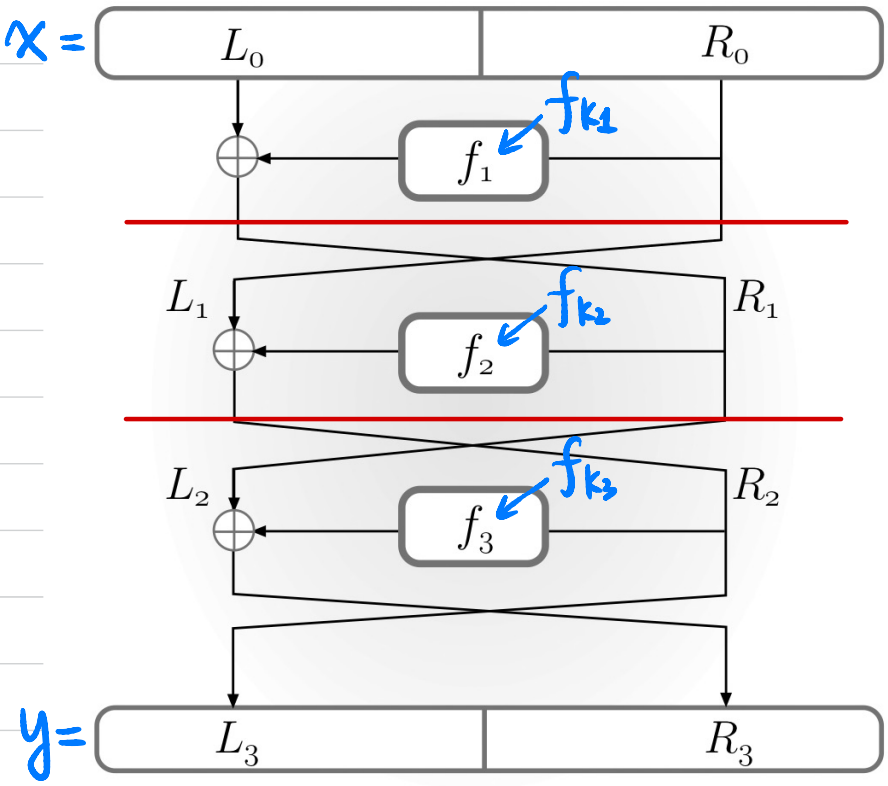
3-round Feistel Network

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

↑ round function

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

Attacks on Reduced-Round Feistel Network



1-round ?

2-round ?

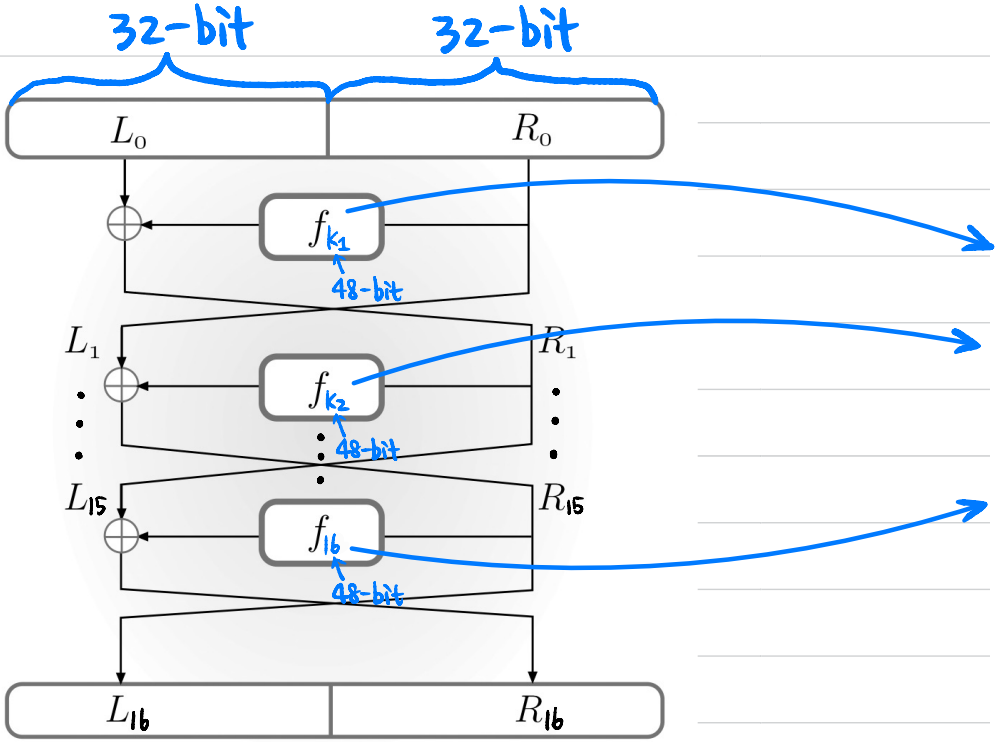
Data Encryption Standard (DES)

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

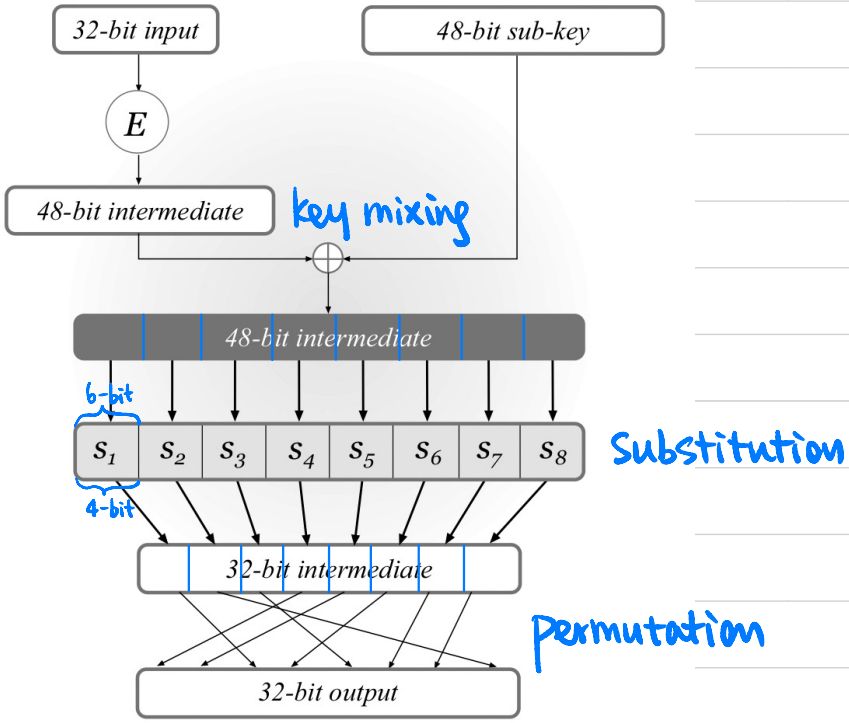
block length $l = 64$

master key length $n = 56$

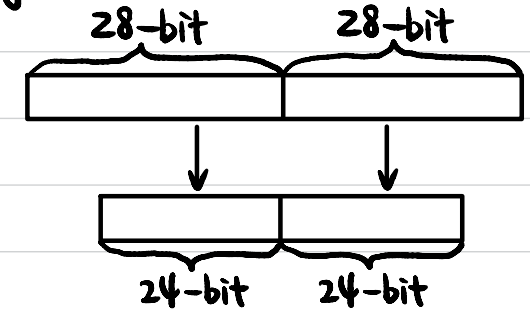
16-round Feistel Network



DES mangler function

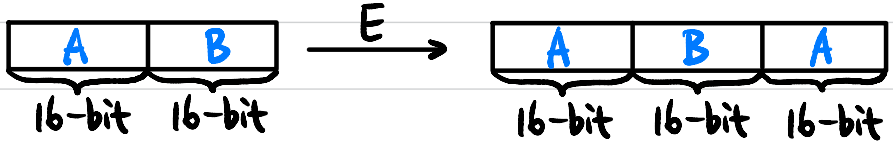


Key Schedule:



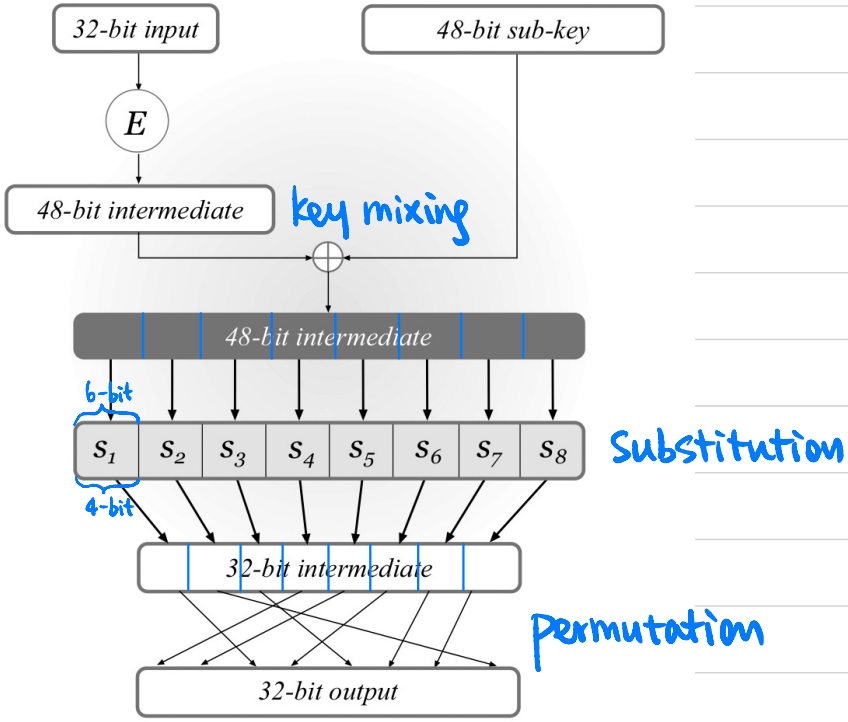
(master key)

E: expansion function



Data Encryption Standard (DES)

DES mangler function



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

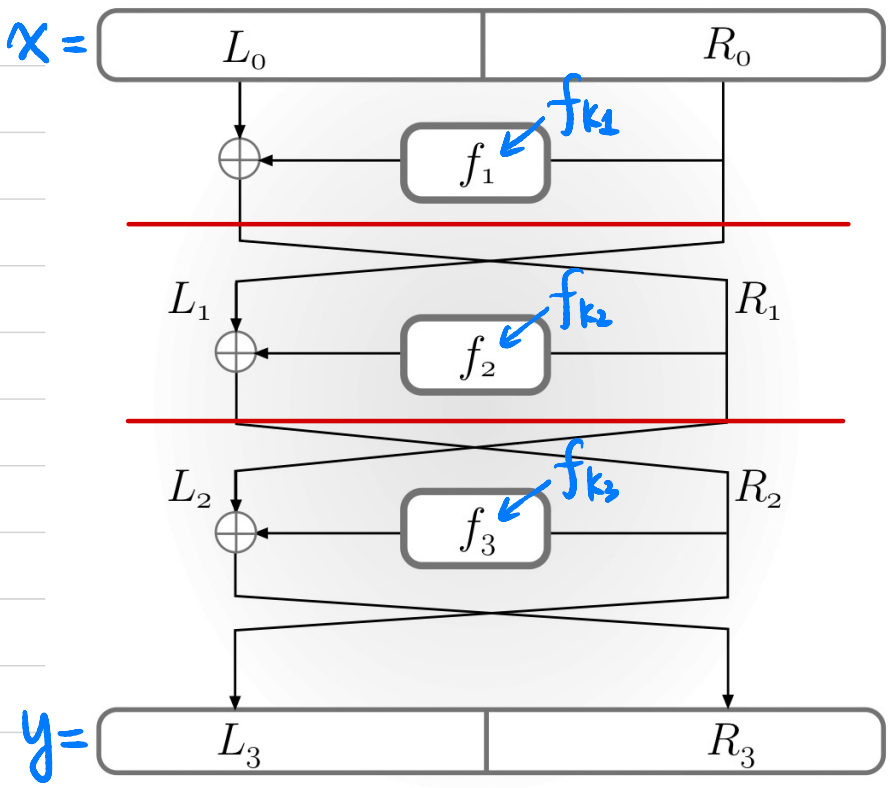
① "4-to-1":
Exactly 4 inputs map to same output

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

Mixing Permutation: [32] → [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 ?

2-round ?

Advanced Encryption Standard (AES)

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

n: key length

l: block length

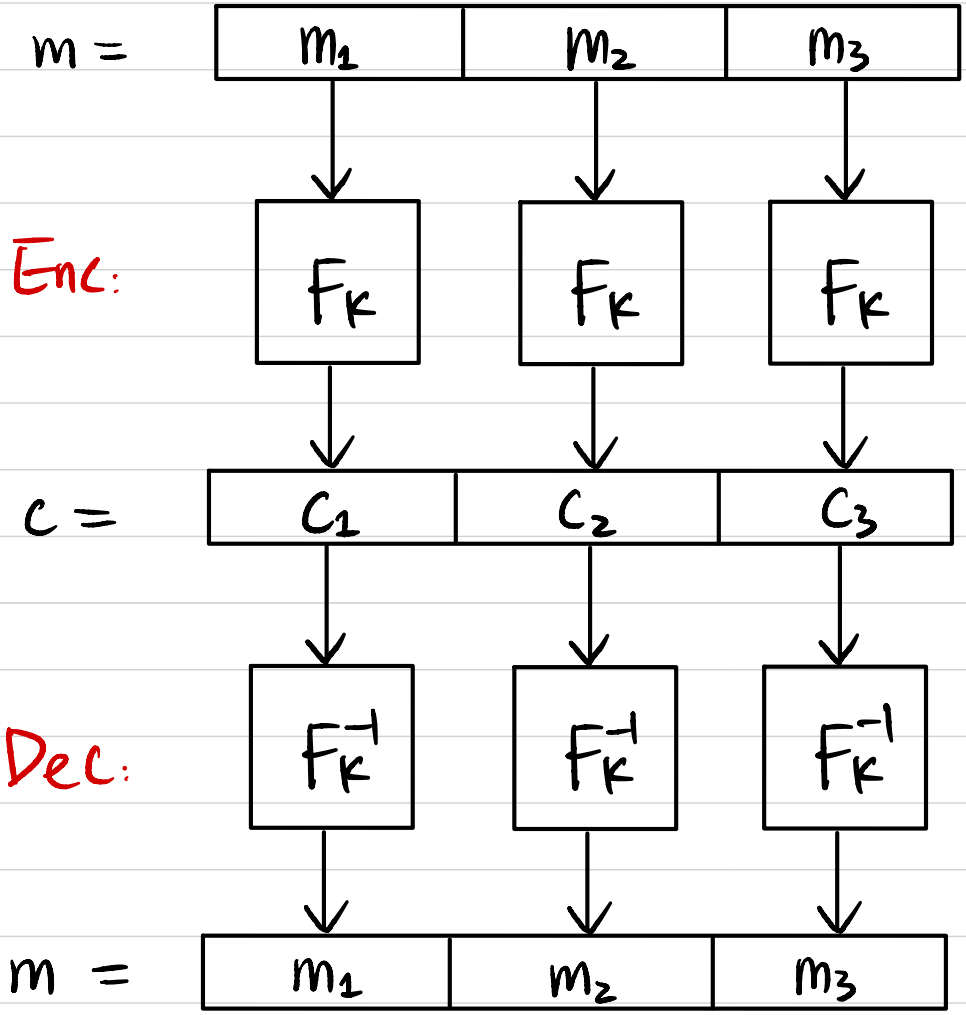
- $n = 128/192/256$, $l = 128$
- Standardized by NIST in 2001
- Competition 1997-2000

Block Cipher Modes of Operation

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

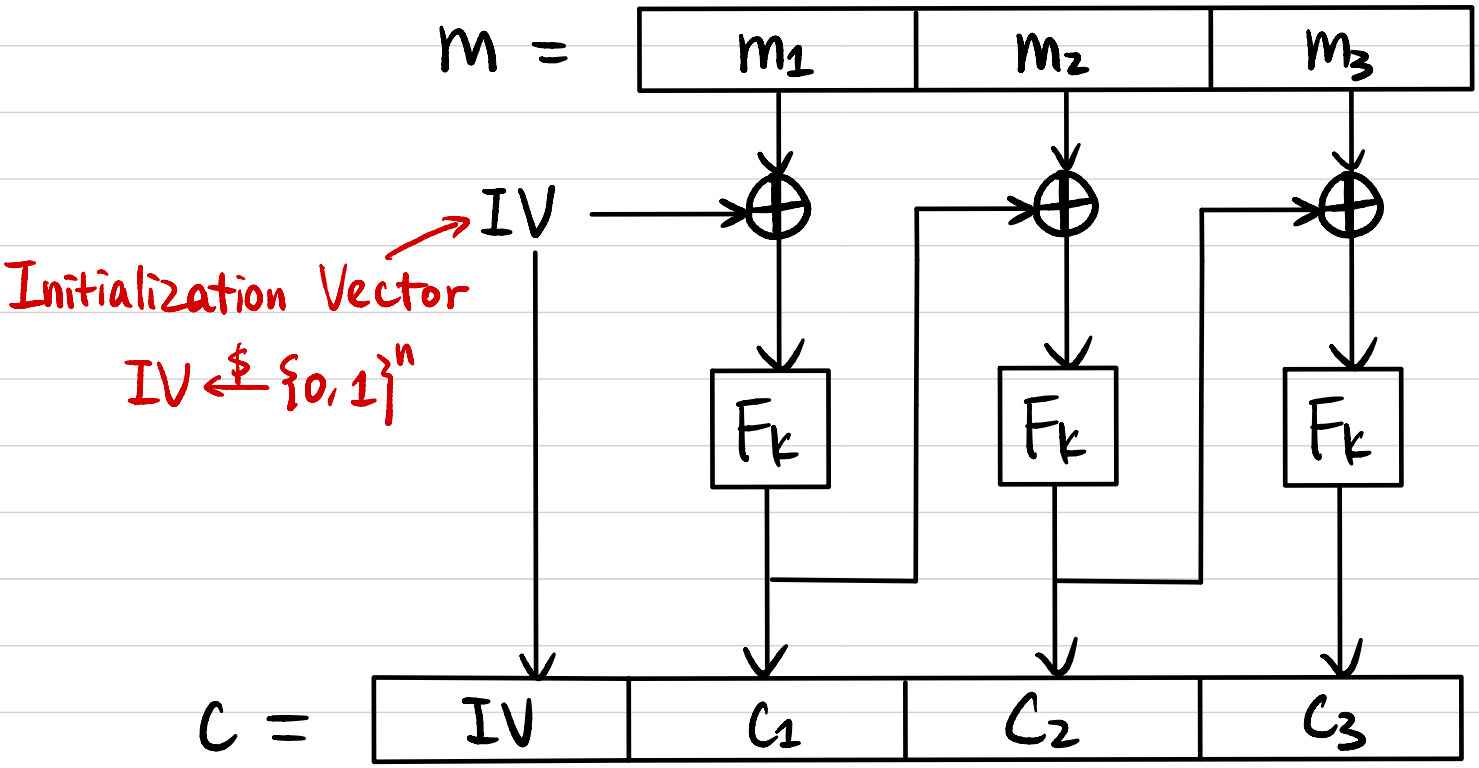
Goal: Construct a CPA-secure encryption scheme for arbitrary-length messages.

Electronic Code Book (ECB) Mode



CPA secure?

Cipher Block Chaining (CBC) Mode

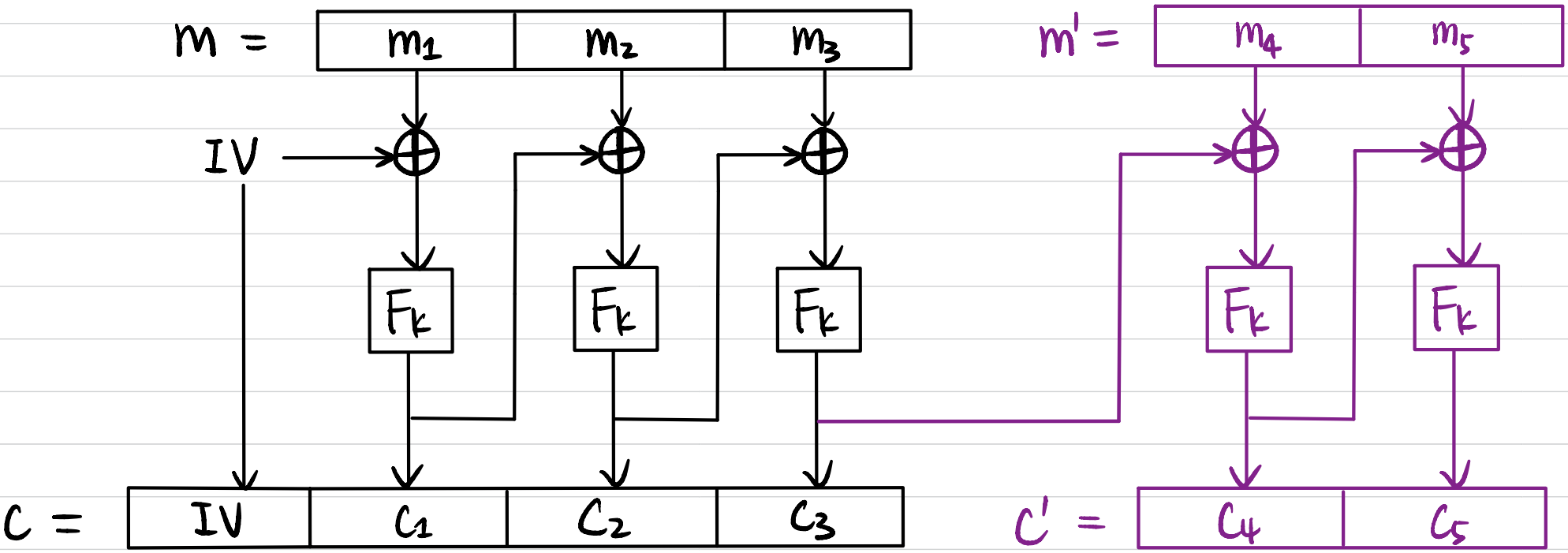


How to decrypt?

CPA secure?

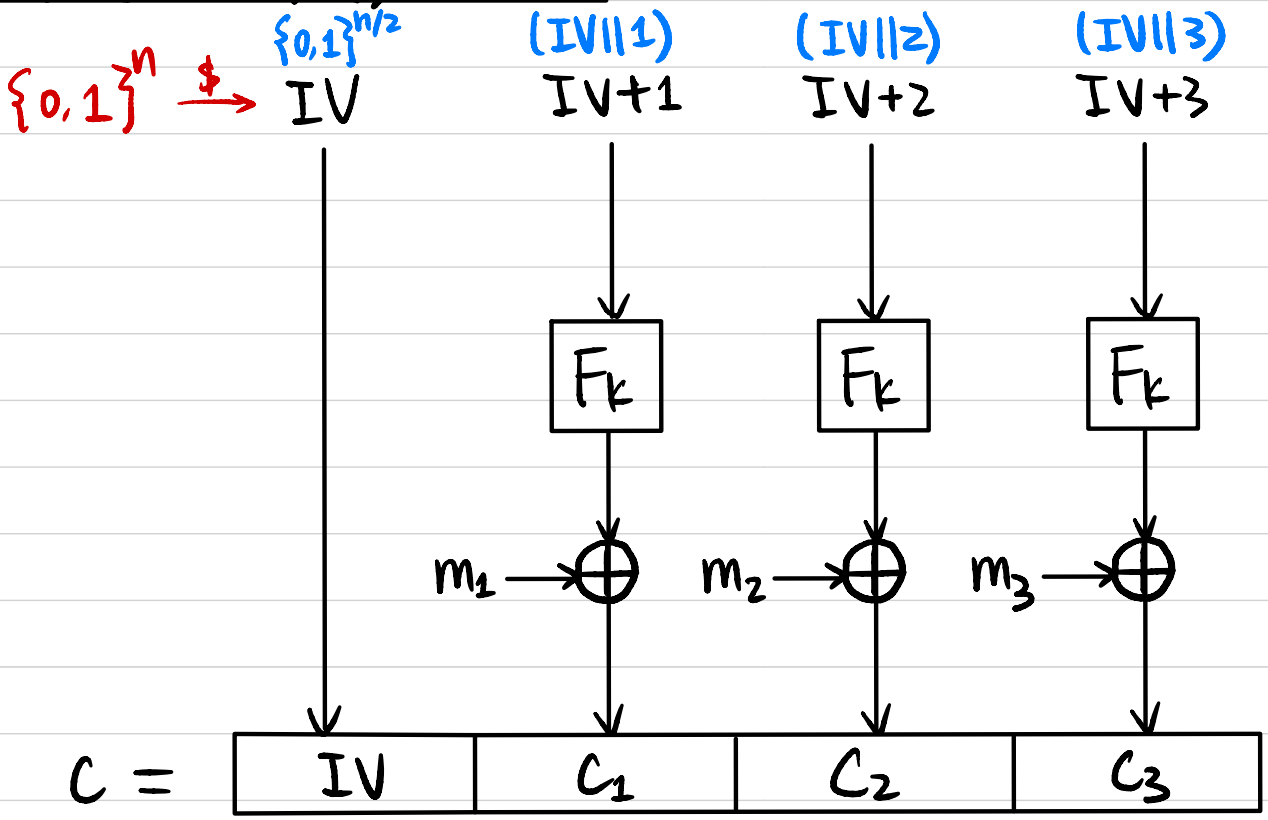
Can we parallelize the computation?

Chained Cipher Block Chaining (CBC) Mode



CPA secure ?

Counter (CTR) Mode



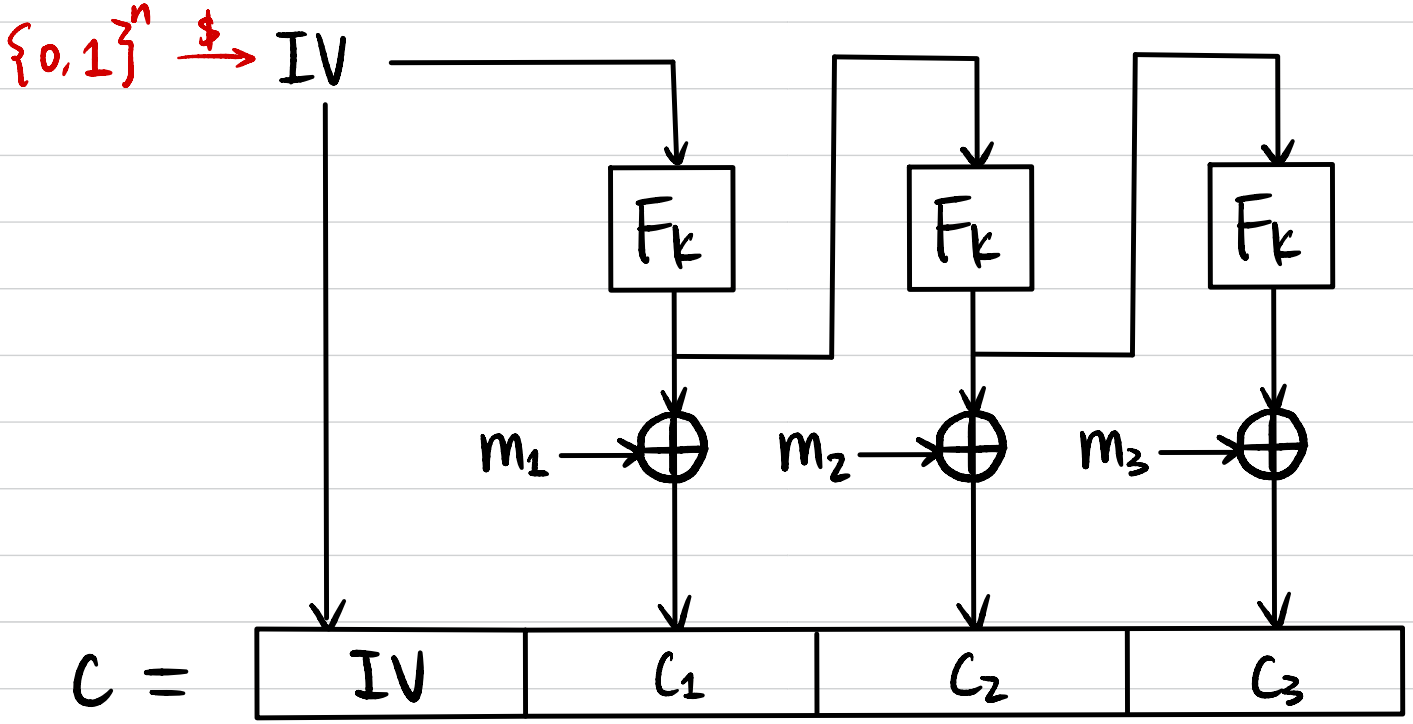
How to decrypt?

CPA secure?

Can we parallelize the computation?

PRG from PRF

Output Feedback (OFB) Mode



How to decrypt?

CPA secure?

Can we parallelize the computation?

PRG from PRF