CSCI 1510

This Lecture:

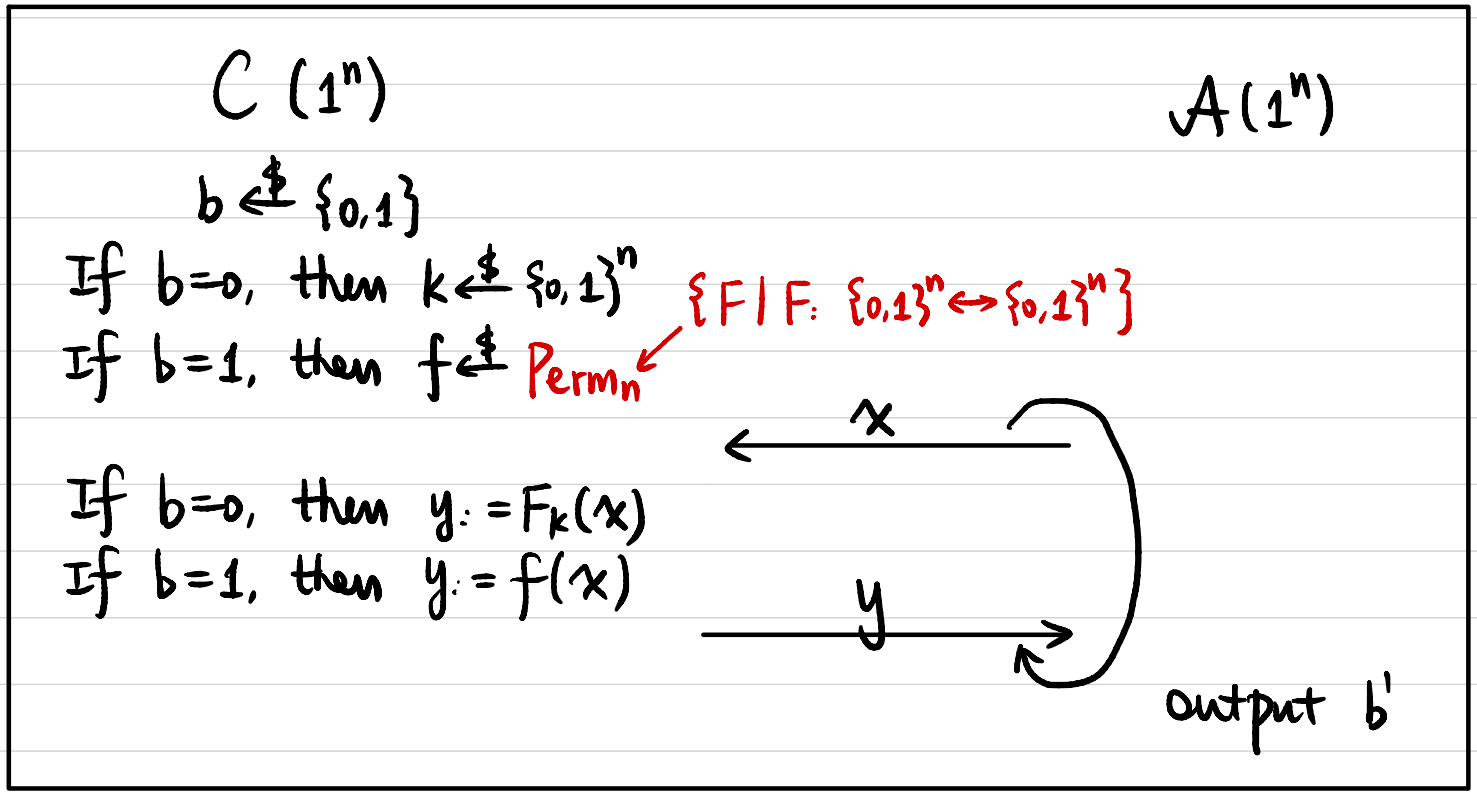
- Constructions of Block Cipher (continued)
- Data Encryption Standard (DES)
- Block Cipher Modes of Operation
- Practical Constructions of Hash Function

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

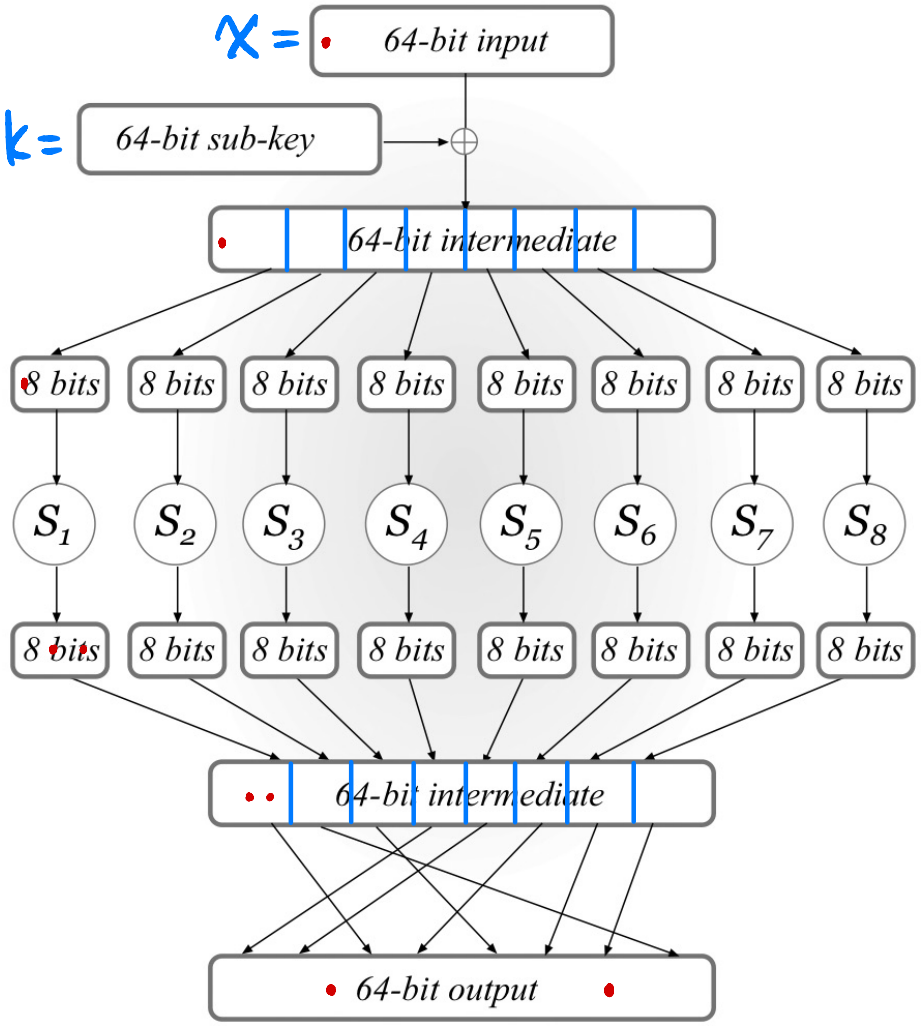
l: block length

$F_k(\cdot)$: 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)

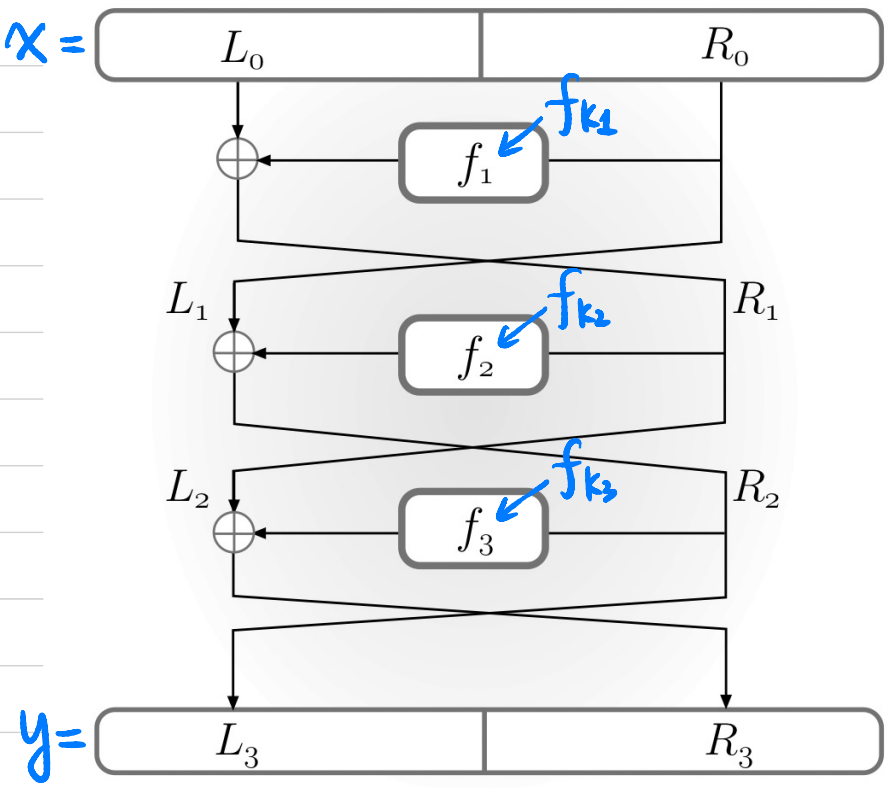
$P : [64] \to [64]$

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 $F_k^{-1}(y)$?

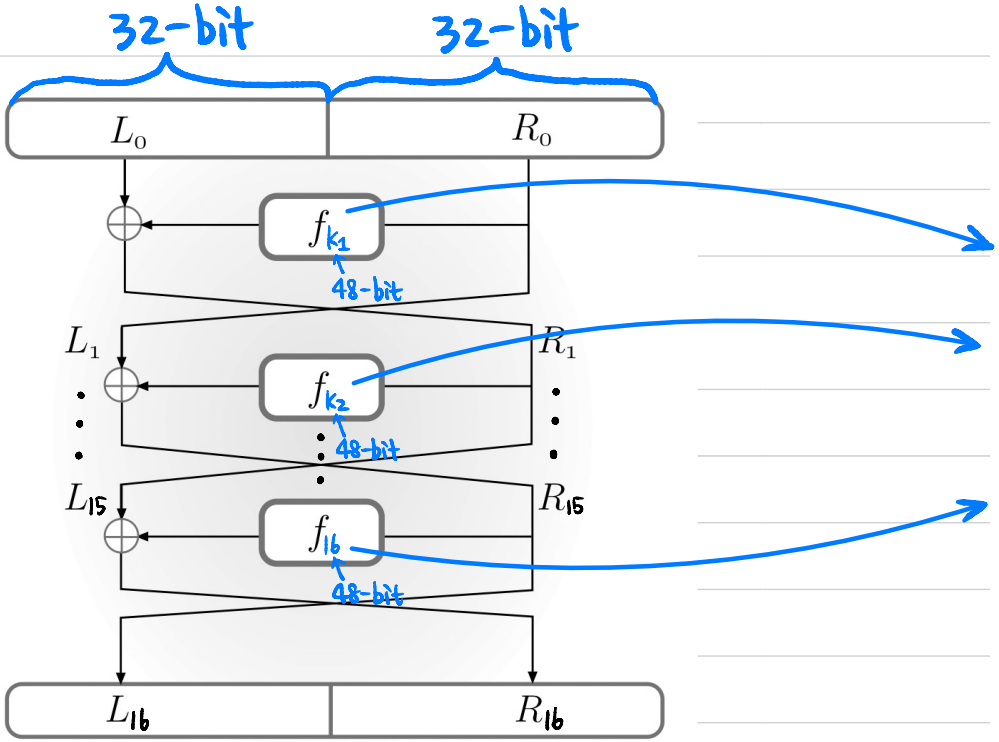
Data Encryption Standard (DES)

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

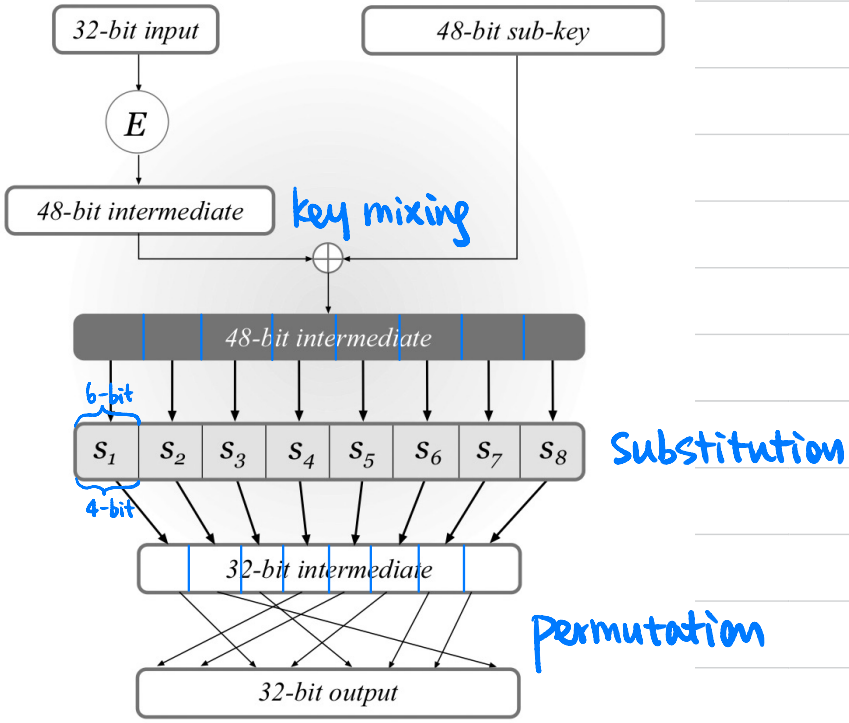
block length $l = 64$

master key length $n = 56$

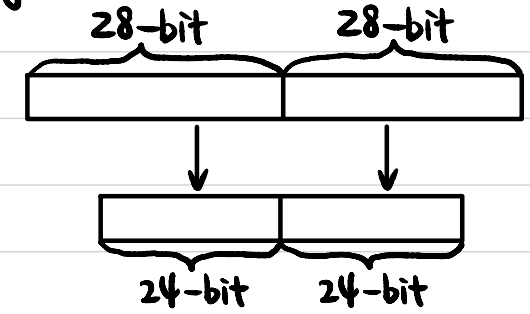
16-round Feistel Network



DES mangler function

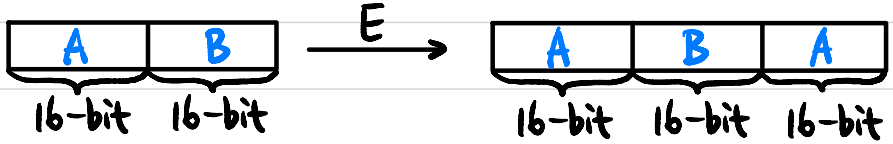


Key Schedule:



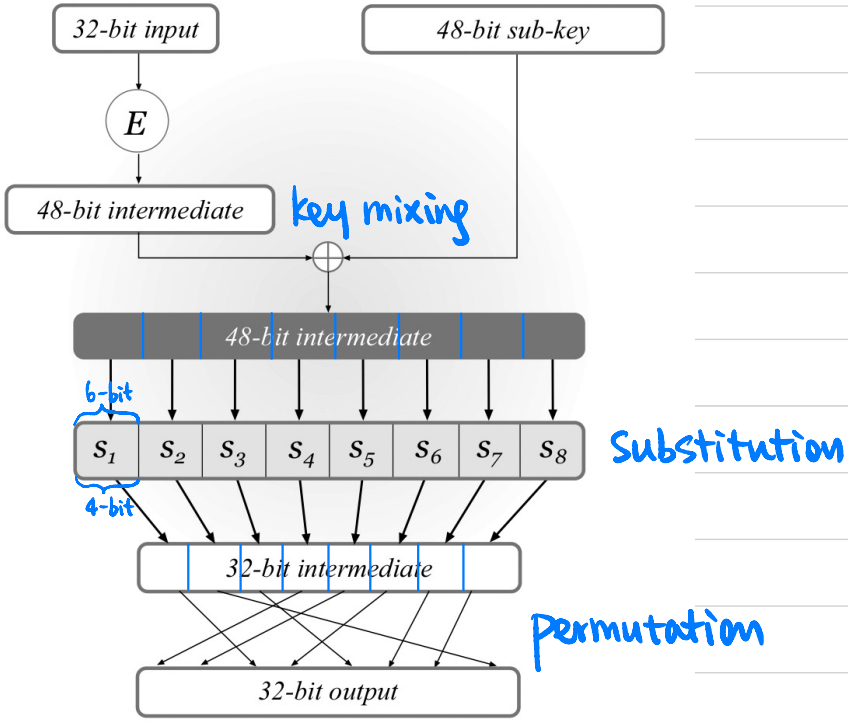
(master key)

E: expansion function



Data Encryption Standard (DES)

DES mangler function



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

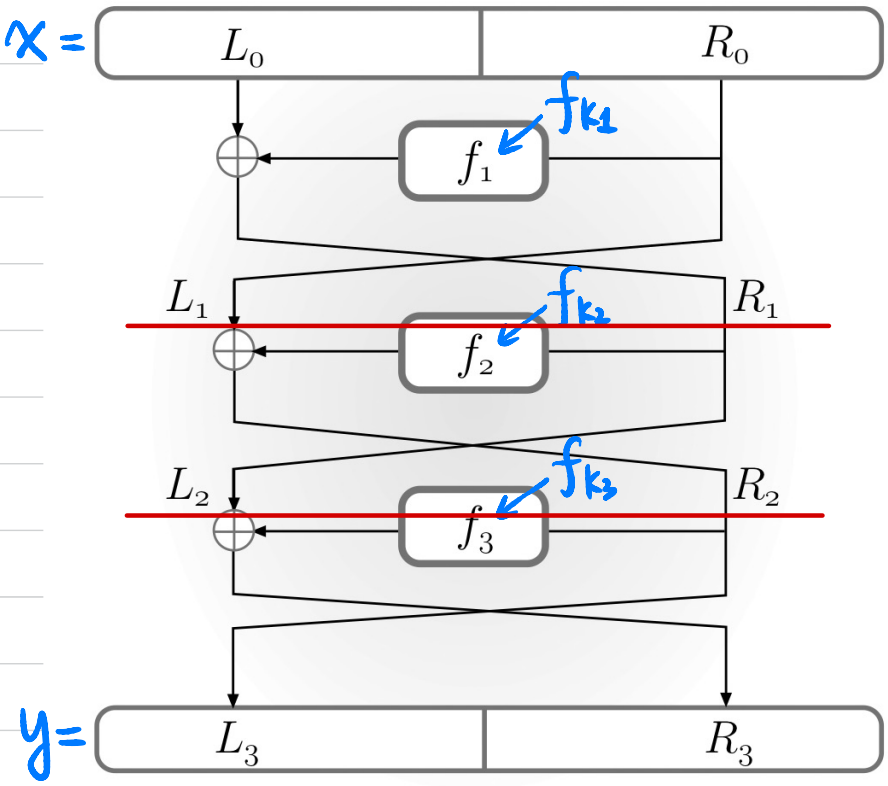
① "4-to-1":
Exactly 4 inputs map to same output

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 DES



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

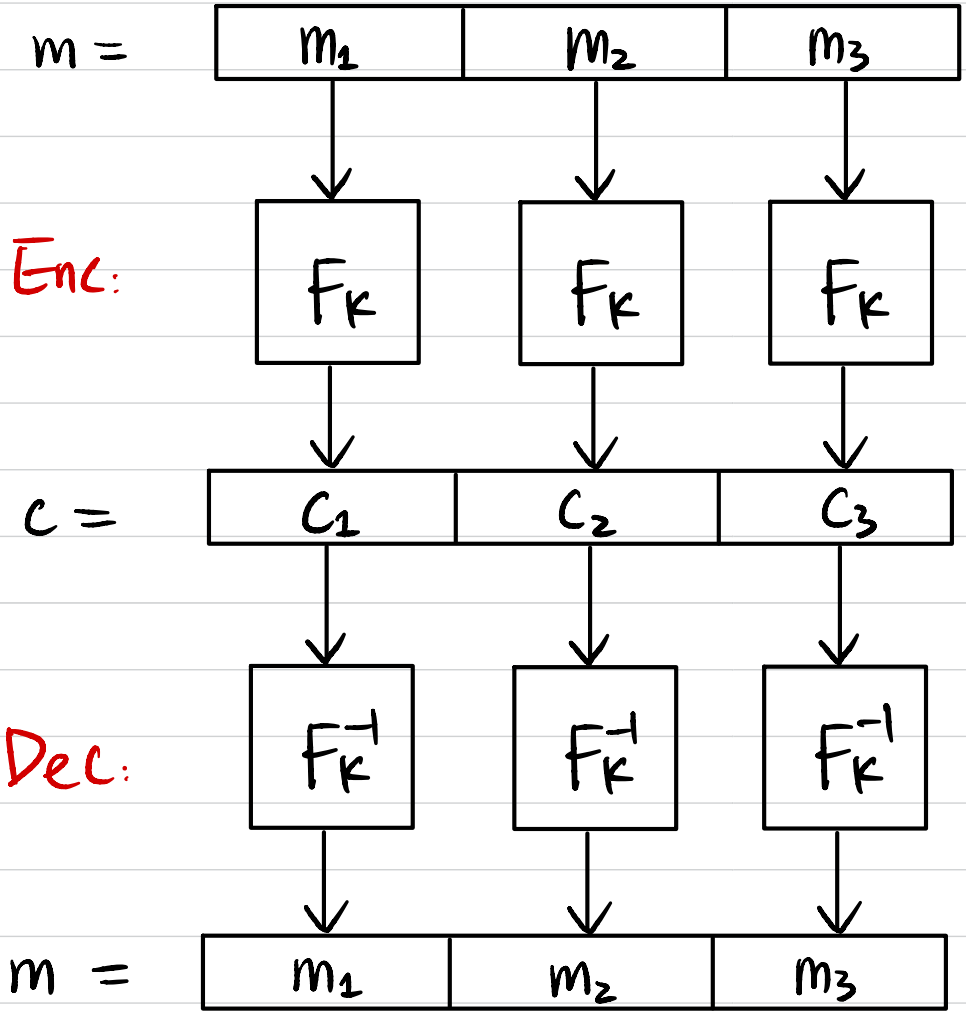
- $n = 128/192/256$, $l = 128$
- Standardized by NIST in 2001
- Competition 1997-2000

Block Cipher Modes of Operation

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

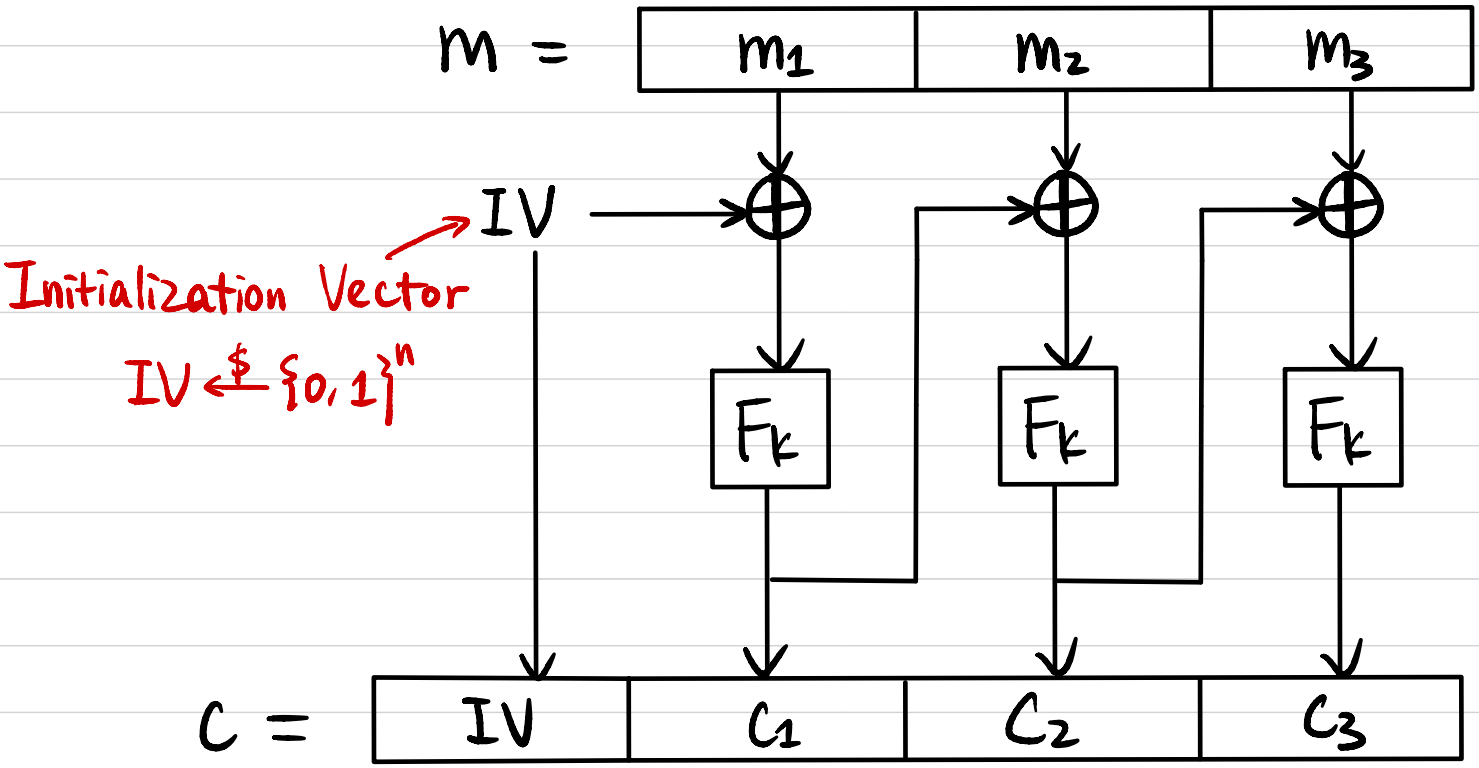
Goal: Construct a CPA-secure encryption scheme for arbitrary-length messages.

Electronic Code Book (ECB) Mode



CPA secure?

Cipher Block Chaining (CBC) Mode

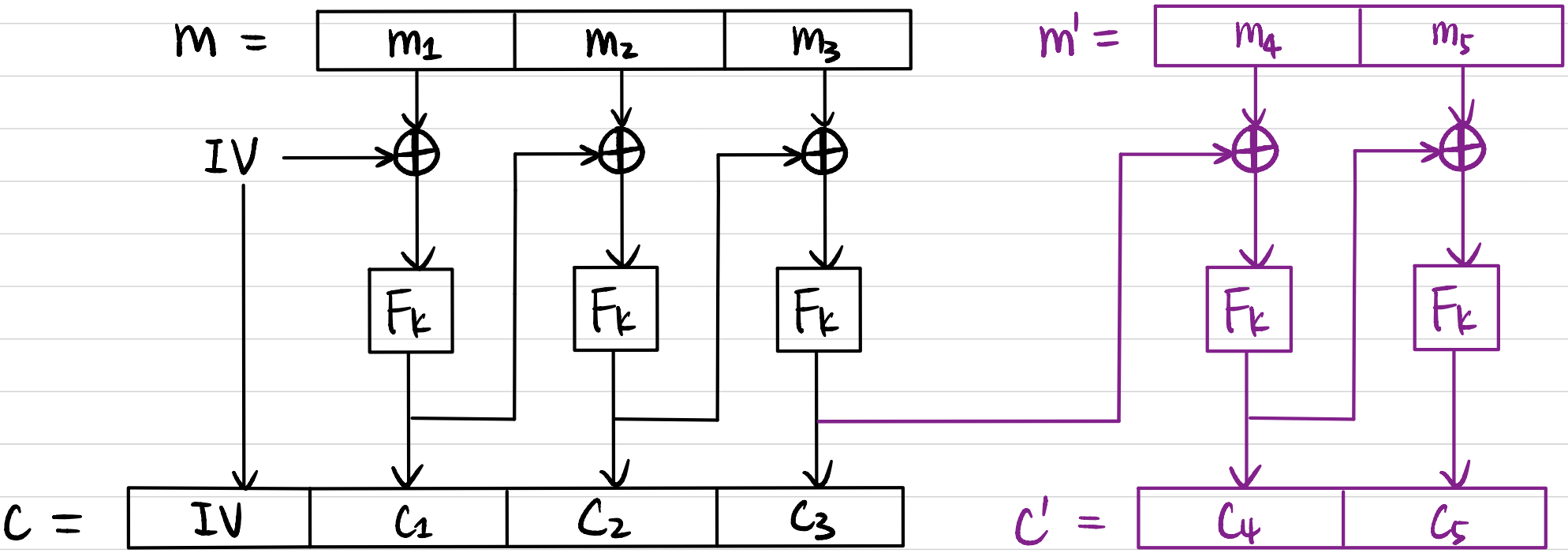


How to decrypt?

CPA secure?

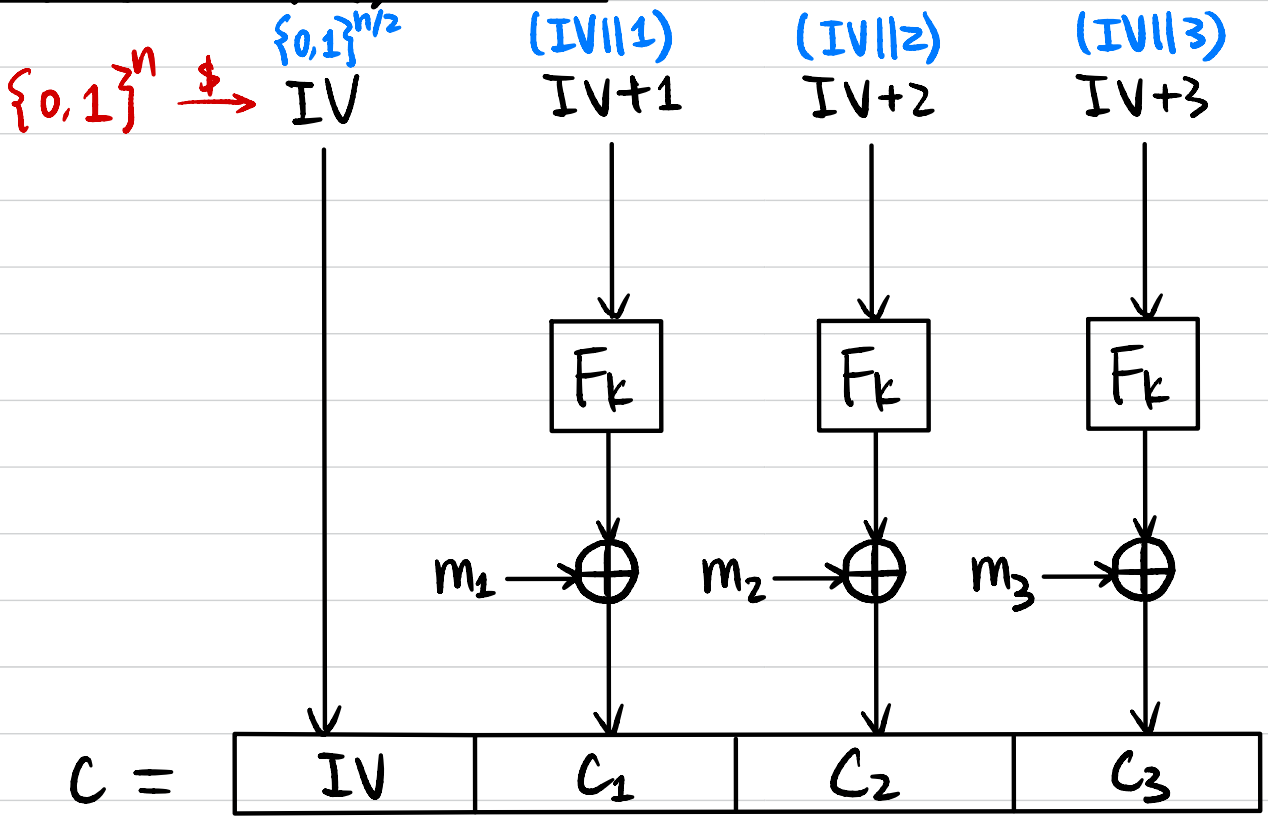
Can we parallelize the computation?

Chained Cipher Block Chaining (CBC) Mode



CPA secure ?

Counter (CTR) Mode



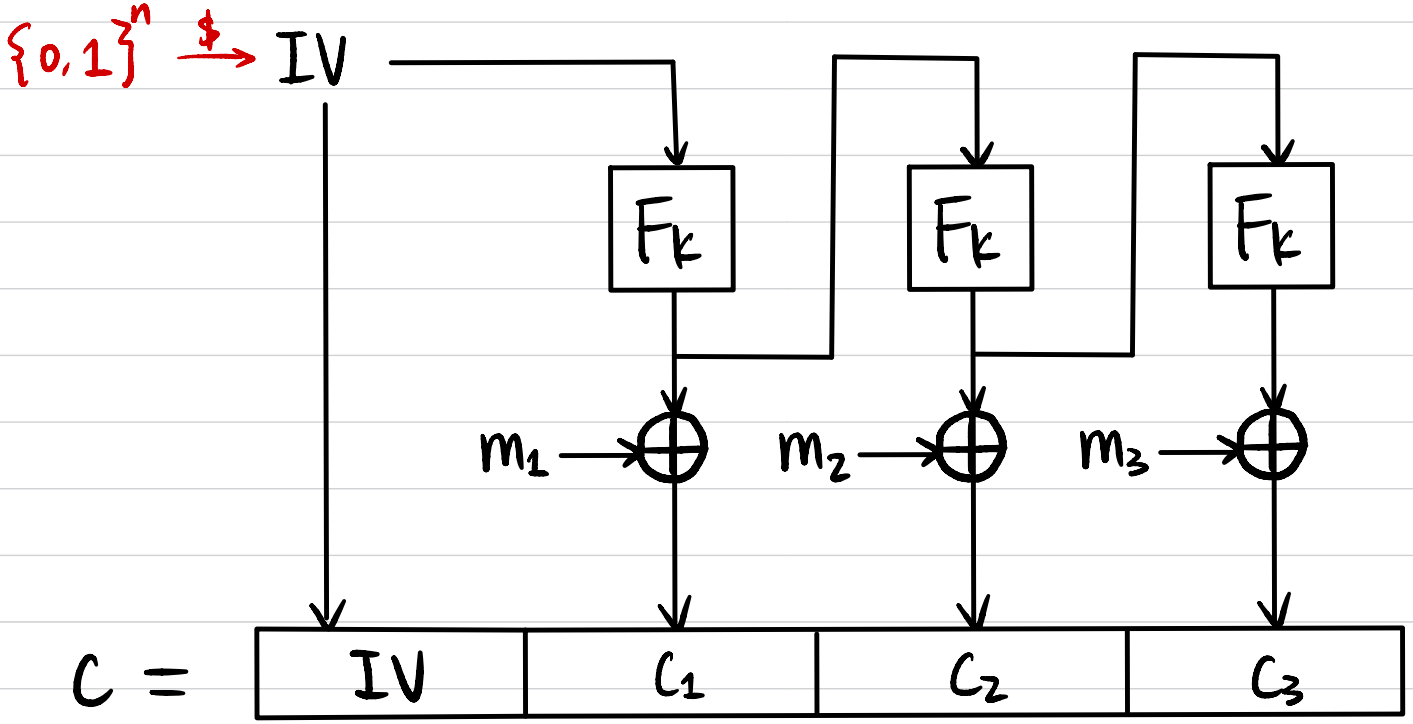
How to decrypt?

CPA secure?

Can we parallelize the computation?

PRG from PRF

Output Feedback (OFB) Mode



How to decrypt?

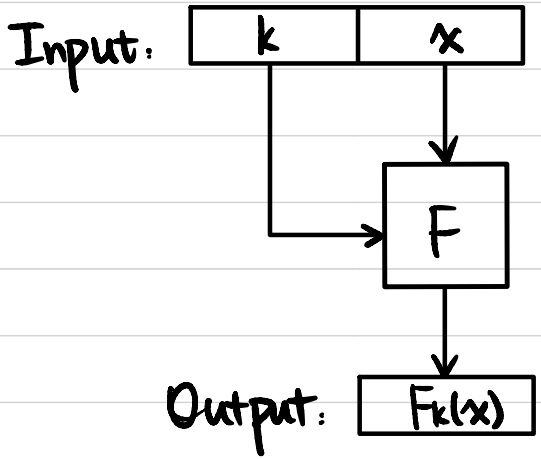
CPA secure?

Can we parallelize the computation?

PRG from PRF

Compression Function from Block Cipher

Block Cipher $\xrightarrow{\text{Davies-Meyer}}$ Compression Function (fixed-length hash function) $\xrightarrow{\text{Merkle-Damgård}}$ Arbitrary-length hash function



If F is model as an "ideal cipher", then Davies-Meyer construction is collision-resistent.

Practical Constructions of Hash Function

MD5: output length 128-bit
best know attack 2^{16}
Collision found in 2004

Secure Hash Functions (SHA): Standardized by NIST.

- SHA-0: Standardized in 1993
  output length 160-bit
  best know attack 2^{39}

- SHA-1: Standardized in 1995
  output length 160-bit
  best know attack 2^{63}
  Collision found in 2017

Practical Constructions of Hash Function

Secure Hash Functions (SHA): Standardized by NIST.

- SHA-2: Standardized in 2001
  output length 224, 256, 384, 512-bit

- SHA-3: Competition 2007–2012
  released in 2015
  output length 224, 256, 384, 512-bit