CSCI 1510

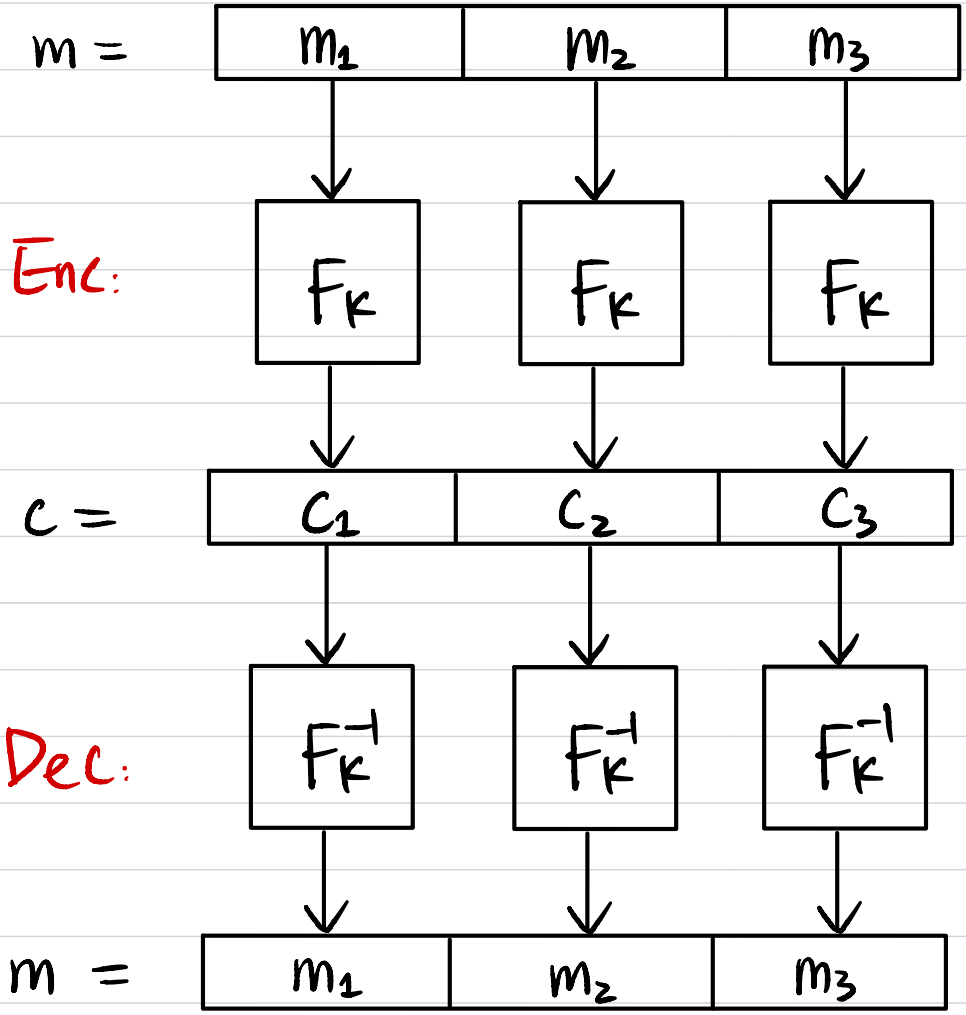
- Block Cipher Modes of Operation (continued)
- Practical Constructions of Hash Function
- Midterm Review

Block Cipher Modes of Operation

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

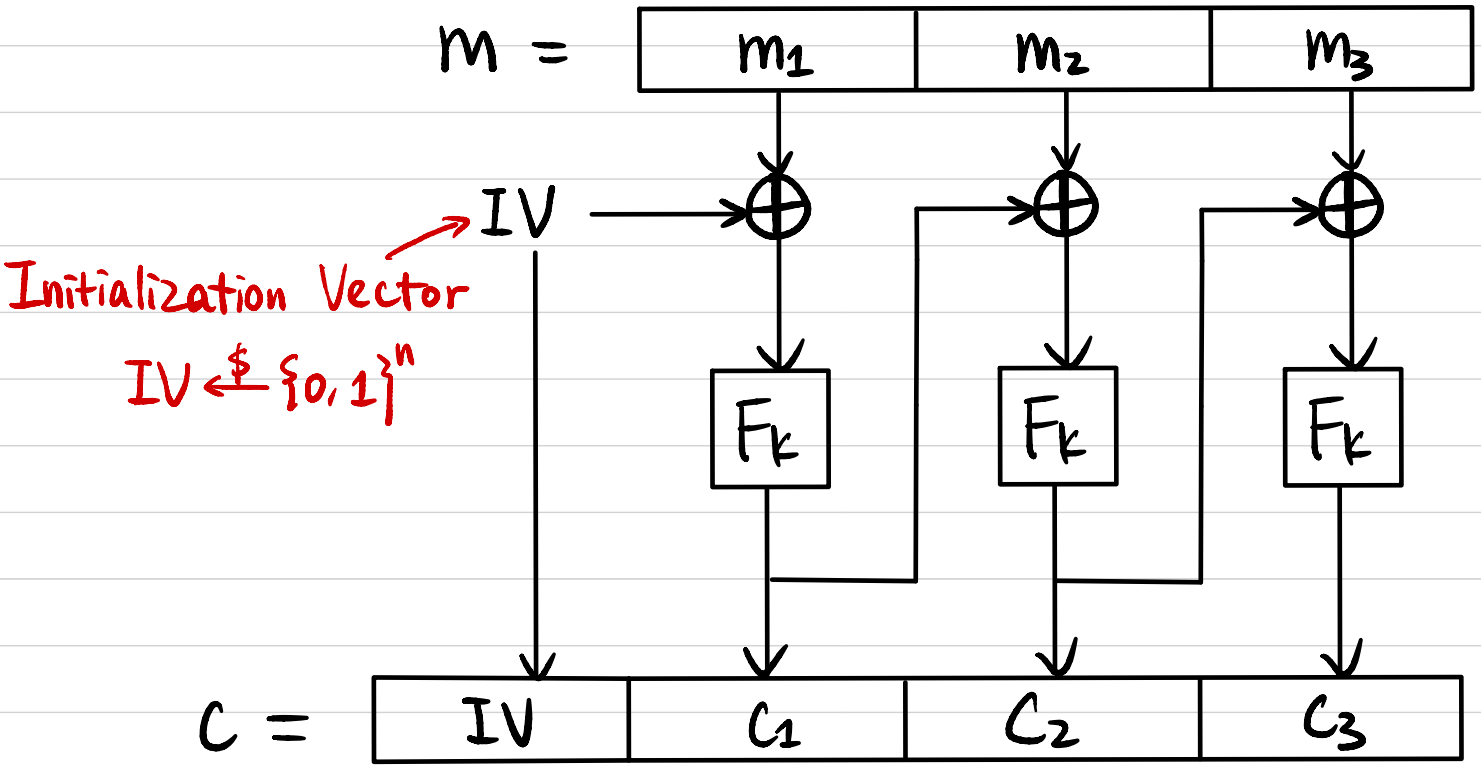
Goal: Construct a CPA-secure encryption scheme for arbitrary-length messages.

Electronic Code Book (ECB) Mode



CPA secure? No!

Cipher Block Chaining (CBC) Mode



H_0: Enc(m_0)

H_1: $F_k \to f$

H_2: $m_0 \to m_1$

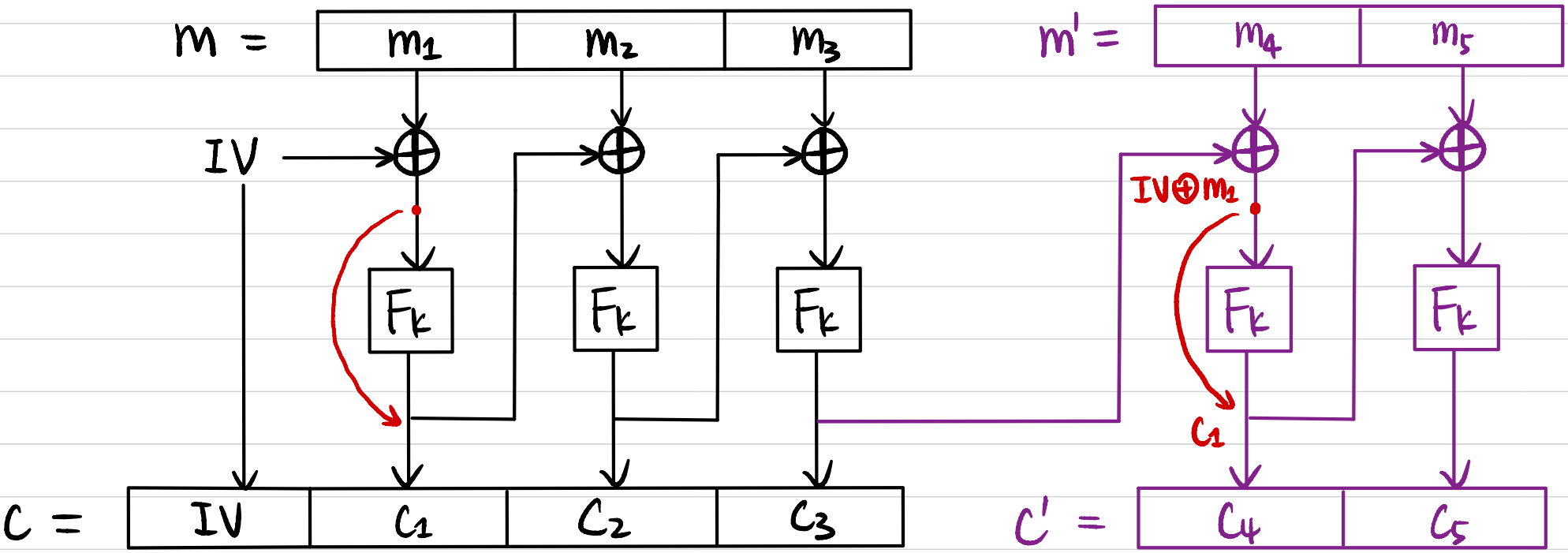
H_3: $f \to F_k$

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

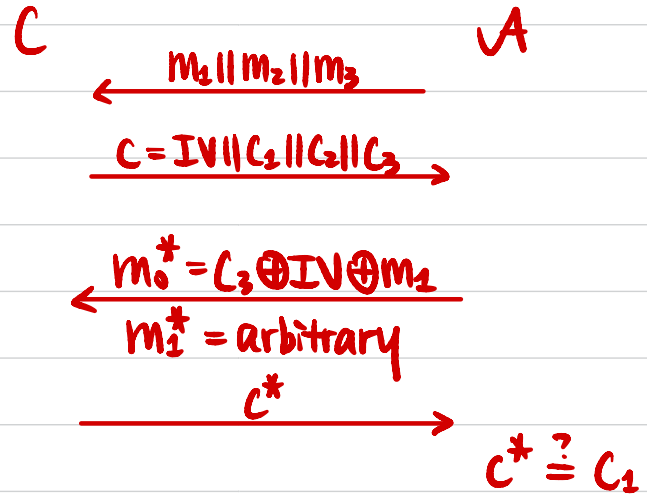
CPA secure? Yes!

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

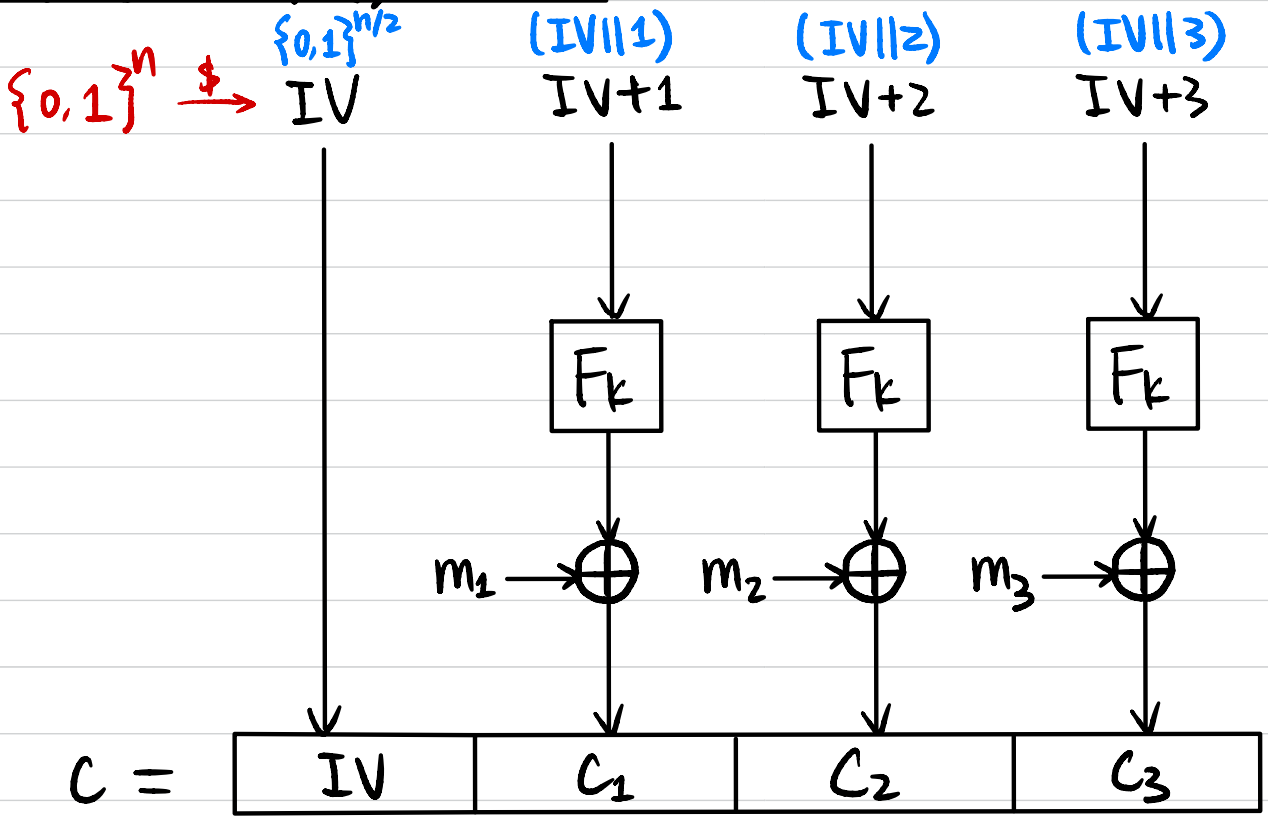
Chained Cipher Block Chaining (CBC) Mode



CPA secure ?



Counter (CTR) Mode



H_0: $Enc(m_0)$

H_1: $F_k \to f$

H_2: $m_0 \to m_1$

H_3: $f \to F_k$

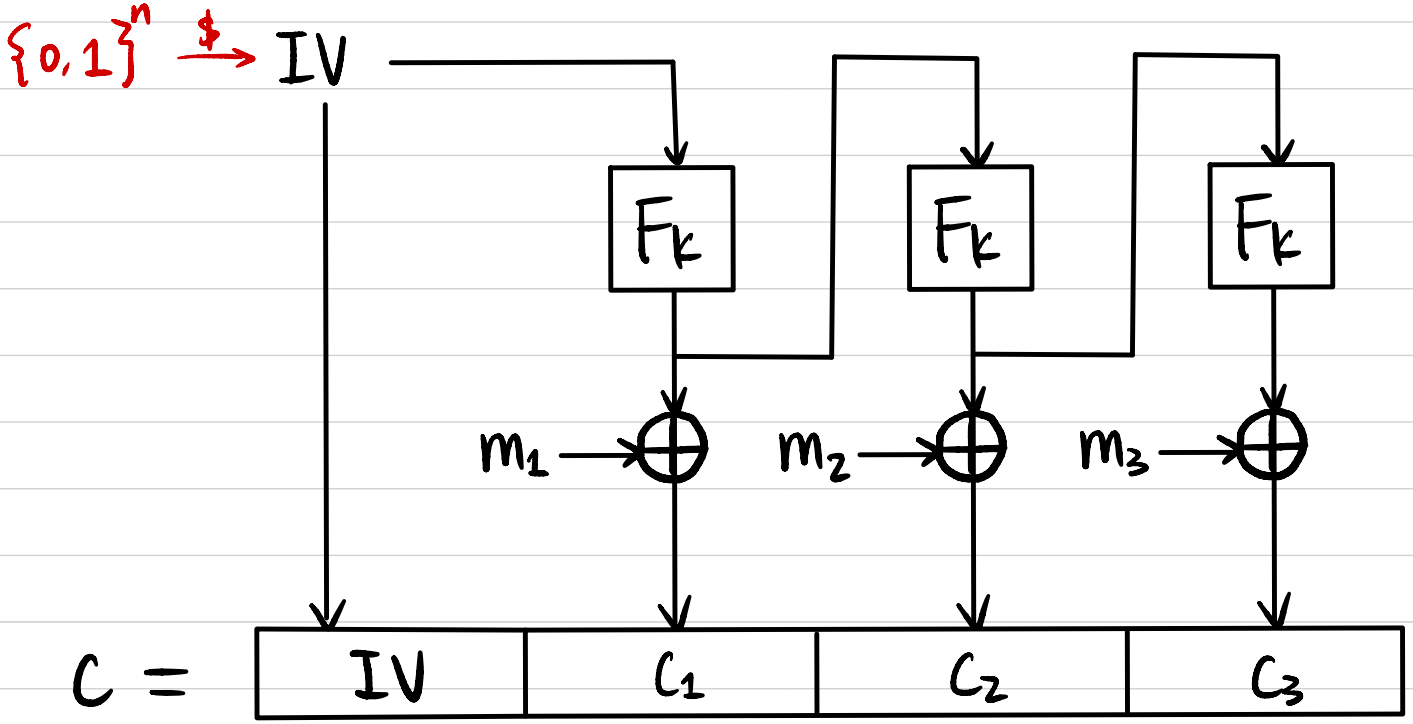
How to decrypt? $F_k(IV+i) \oplus C_i \Rightarrow m_i$

CPA secure? Yes!

Can we parallelize the computation? Yes!

PRG from PRF $G: \{0,1\}^{2n} \to \{0,1\}^{3n}$

Output Feedback (OFB) Mode



How to decrypt?

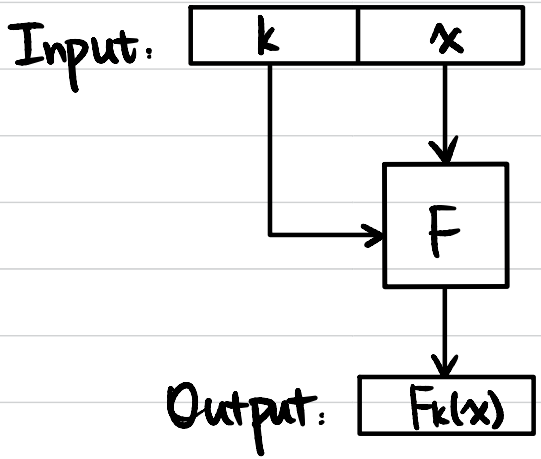
CPA secure?

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

Midterm Review

- Symmetric-Key Encryption
  - Syntax
  - Kerckhoff's Principle
- Perfect Security
  - Definition
  - Construction: One-Time Pad
  - Limitations: $|K| \geq |M|$
- Computational Security
  - Negligible function & Asymptotic approach

Midterm Review

- Computational Security for Message Secrecy
  - * Semantic Security
    - Definition
    - Construction: Pseudo-OTP from PRG ← Definition
    - Proof by reduction
    - Limitations: Cannot reuse key
  - * CPA Security
    - Definition
    - Construction from PRF ← Definition
    - Proof by hybrid argument + reduction
    - Limitations: Cannot query for decryption
  - * CCA Security
    - Definition

Midterm Review

- Message Integrity
  - * Message Authentication Code (MAC)
    - Syntax
    - Definitions: Secure / Strongly secure
    - Constructions
      - Fixed-length MAC of length n from PRF
      - Fixed-length MAC of length $\ell(n) \cdot n$ from PRF: CBC-MAC
      - Arbitrary-length MAC: extension of CBC-MAC
  - * Unforgeability of Encryption Scheme
    - Definition

- Authenticated Encryption: Secrecy & Integrity
  - Definition: CCA Secure & Unforgeable
  - Constructions: CPA-secure encryption + MAC

Midterm Review

- Practical Constructions
  - Block Cipher: PRP / PRF
  - Constructions: SPN / Feistel Network / DES / AES
  - Attacks on reduced rounds
  - Modes of Operation: pros & cons

Midterm Review

- Hash Function
  - Definition: Collision-Resistant
  - Birthday Attack & Implications
  - Merkle-Damgård Transform
  - Applications
  - Practical Constructions: Davies-Meyer / SHA