

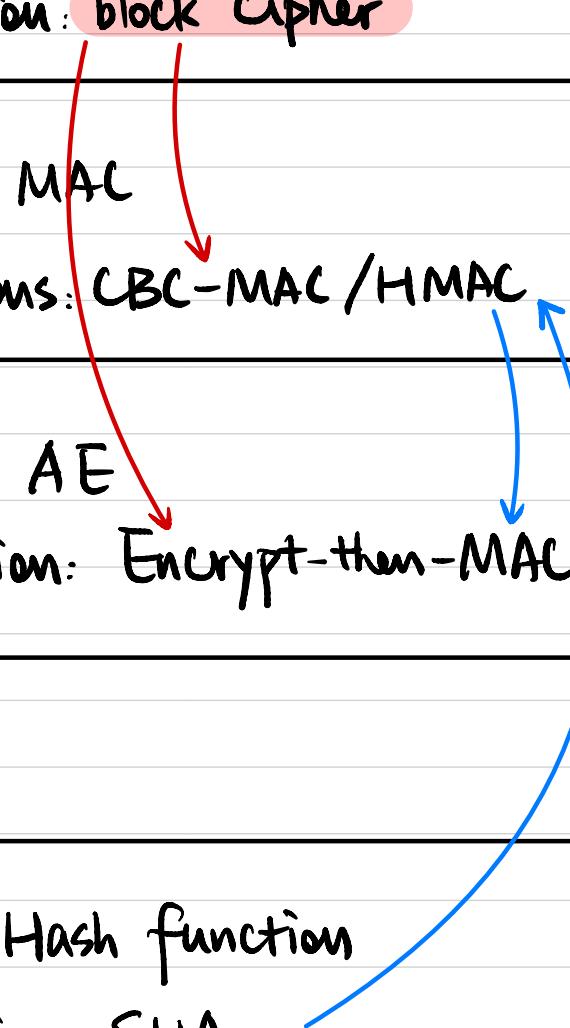
CSCI 1515 Applied Cryptography

This Lecture:

- Pseudorandom Function (PRF)
Pseudorandom Permutation (PRP)
- Block Cipher and Modes of Operation

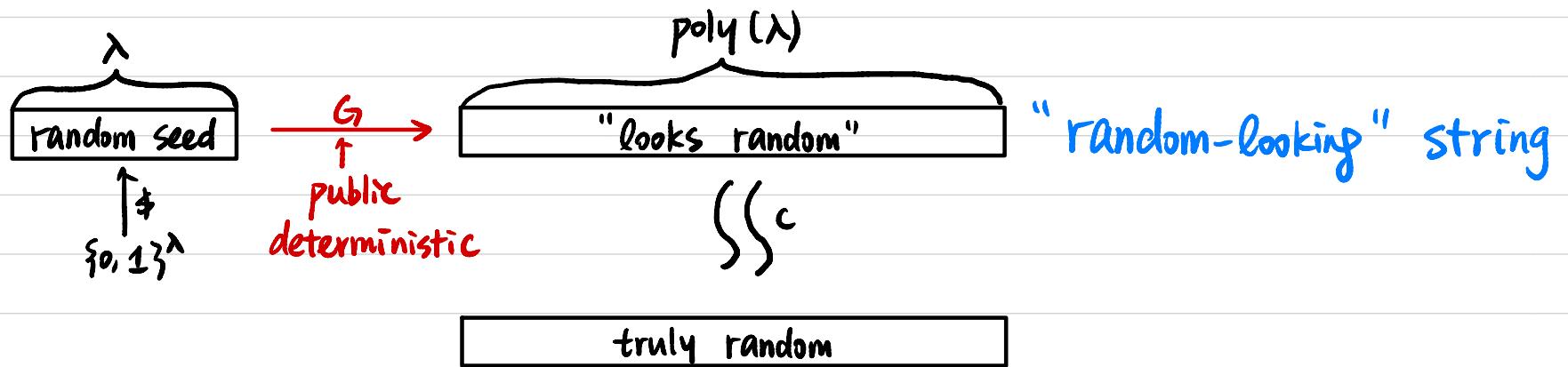
Summary

	Symmetric-Key	Public-Key
Message Secrecy	Primitive: SKE Construction: block Cipher	Primitive: PKE Constructions: RSA / ElGamal
Message Integrity	Primitive: MAC Constructions: CBC-MAC / HMAC	Primitive: Signature Constructions: RSA / DSA
Secret & Integrity	Primitive: AE Construction: Encrypt-then-MAC	
Key Exchange		Construction: Diffie-Hellman
Important Tool	Primitive: Hash function Construction: SHA	



Pseudorandom Function (PRF)

Pseudorandom Generator (PRG)



Pseudorandom Function (PRF): "random-looking" function

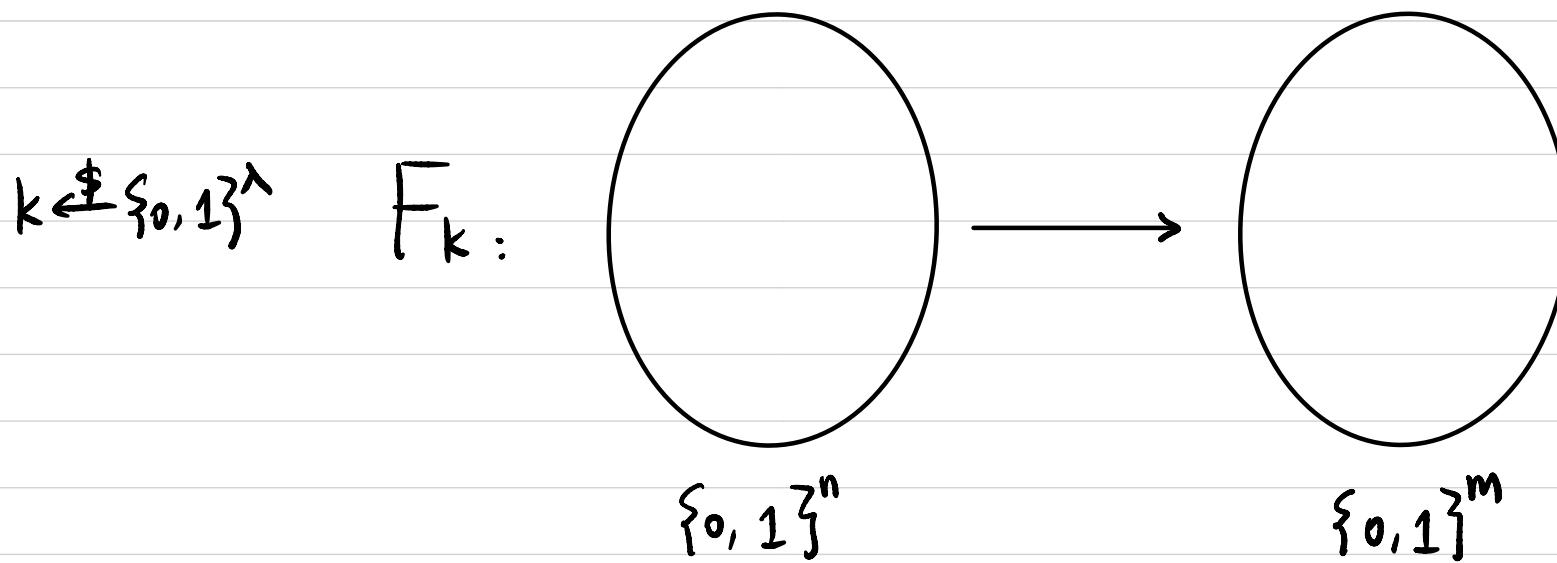
Pseudorandom Function (PRF)

Keyed Function $F: \{0,1\}^\lambda \times \{0,1\}^n \rightarrow \{0,1\}^m$

$F(k, x) \rightarrow y$

↑
key
↑
input
↑
output

deterministic
poly-time

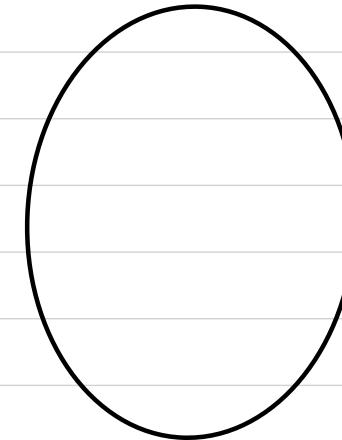
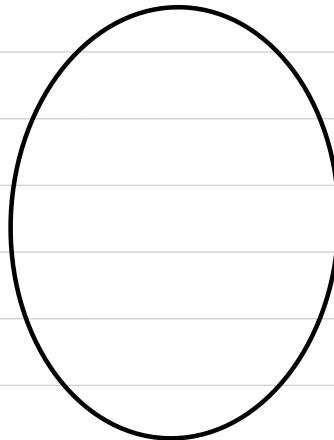


"looks like a random function"

Pseudorandom Function (PRF)

$$k \xleftarrow{\$} \{0,1\}^\lambda$$

$F_k :$



How many possible F_k 's ?

\beth^λ

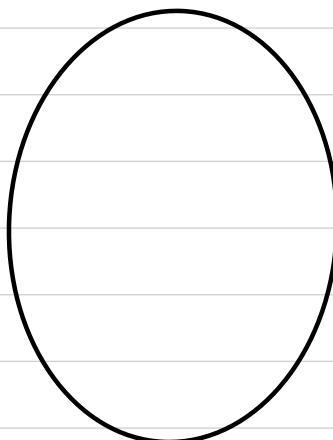
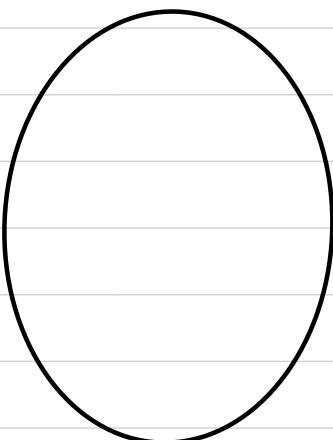
$$\{0,1\}^n$$

$$\{0,1\}^m$$

\beth^c (not knowing k)

$$f \xleftarrow{\$} \{F \mid F : \{0,1\}^n \rightarrow \{0,1\}^m\}$$

$f :$



How many possible f 's ?

$$(\beth^m)^{\beth^n}$$

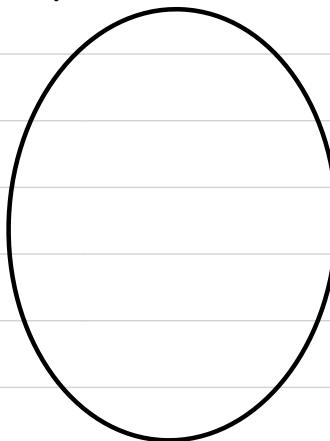
$$\{0,1\}^n$$

$$\{0,1\}^m$$

Pseudorandom Permutation (PRP)

$$k \leftarrow \{0, 1\}^\lambda$$

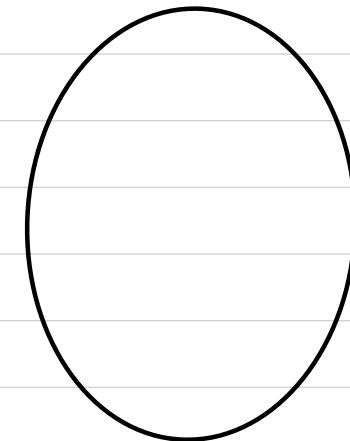
$F_k :$



bijective

$$F_k$$

$$F_k^{-1}$$



How many possible F_k 's ?

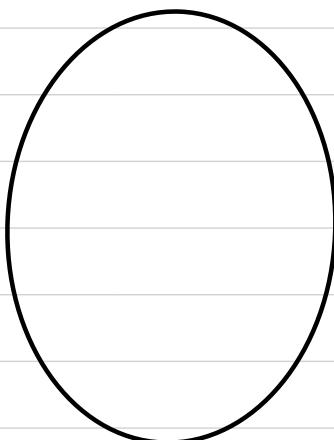
$$2^\lambda$$

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

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

$$f \leftarrow \{ F \mid F : \{0, 1\}^n \rightarrow \{0, 1\}^n, \\ F \text{ is bijective} \}$$

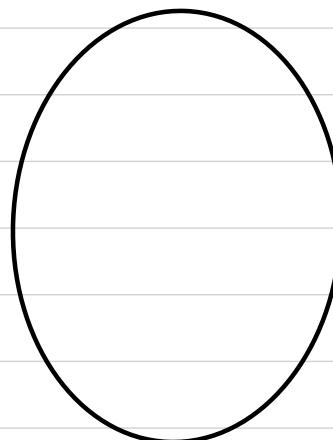
$f :$



bijective

$$f$$

$$f^{-1}$$



How many possible f 's ?

$$2^n!$$

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

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

Block Cipher

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

λ : key length

n : block length

It is assumed to be a pseudorandom permutation (PRP).

Construction: Advanced Encryption Standard (AES)

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

Before AES: Data Encryption Standard (DES)

- $\lambda = 56$, $n = 64$

Block Cipher Modes of Operation

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

It is assumed to be a pseudorandom permutation (PRP).

Construct an SKE scheme from F for arbitrary-length messages.

- $k \leftarrow \{0, 1\}^\lambda$

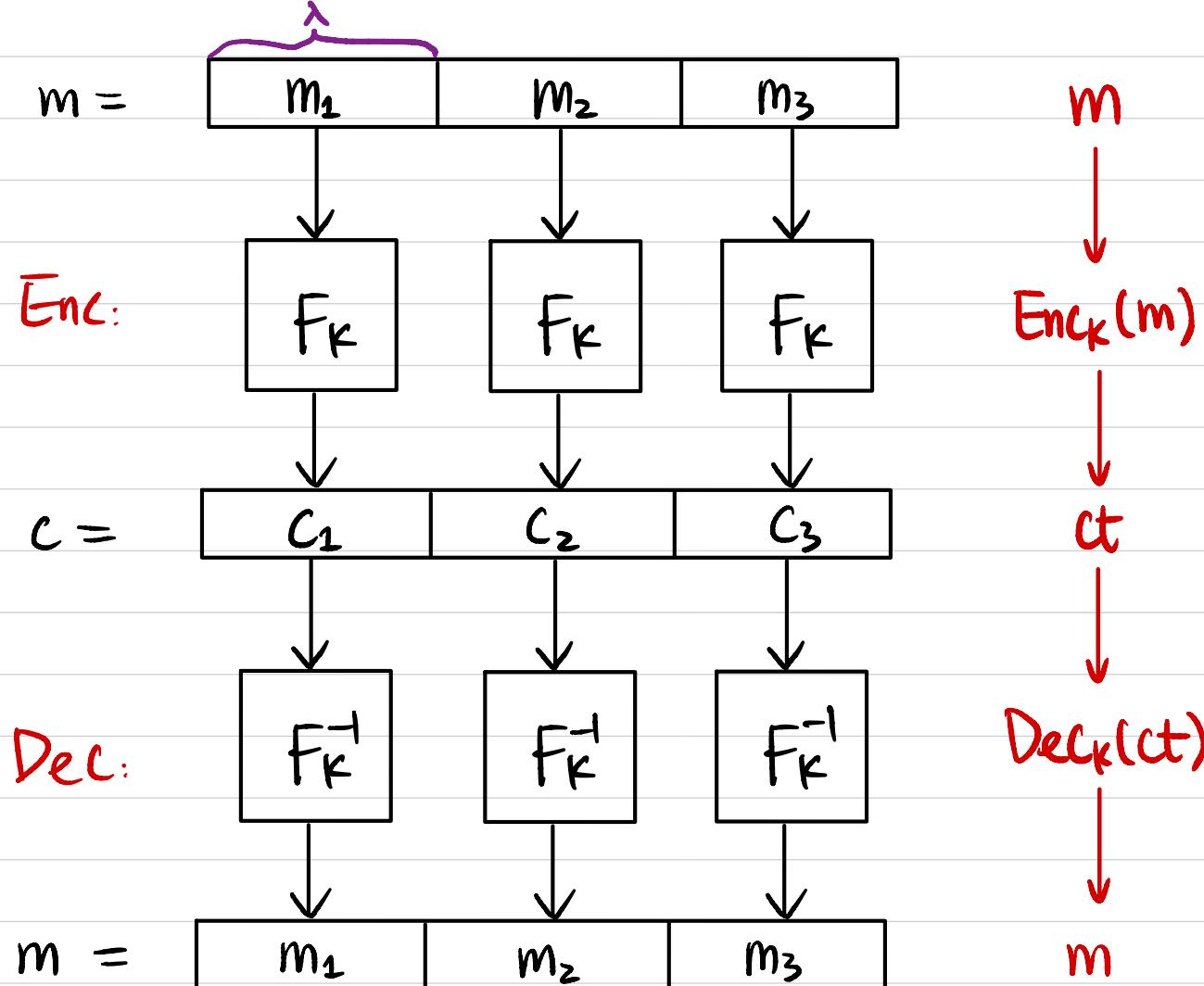
- $\text{Enc}_k(m)$

$$|m| = \alpha \cdot \lambda \quad (\text{If not, pad it to a multiple of } \lambda)$$

- $\text{Dec}_k(c)$

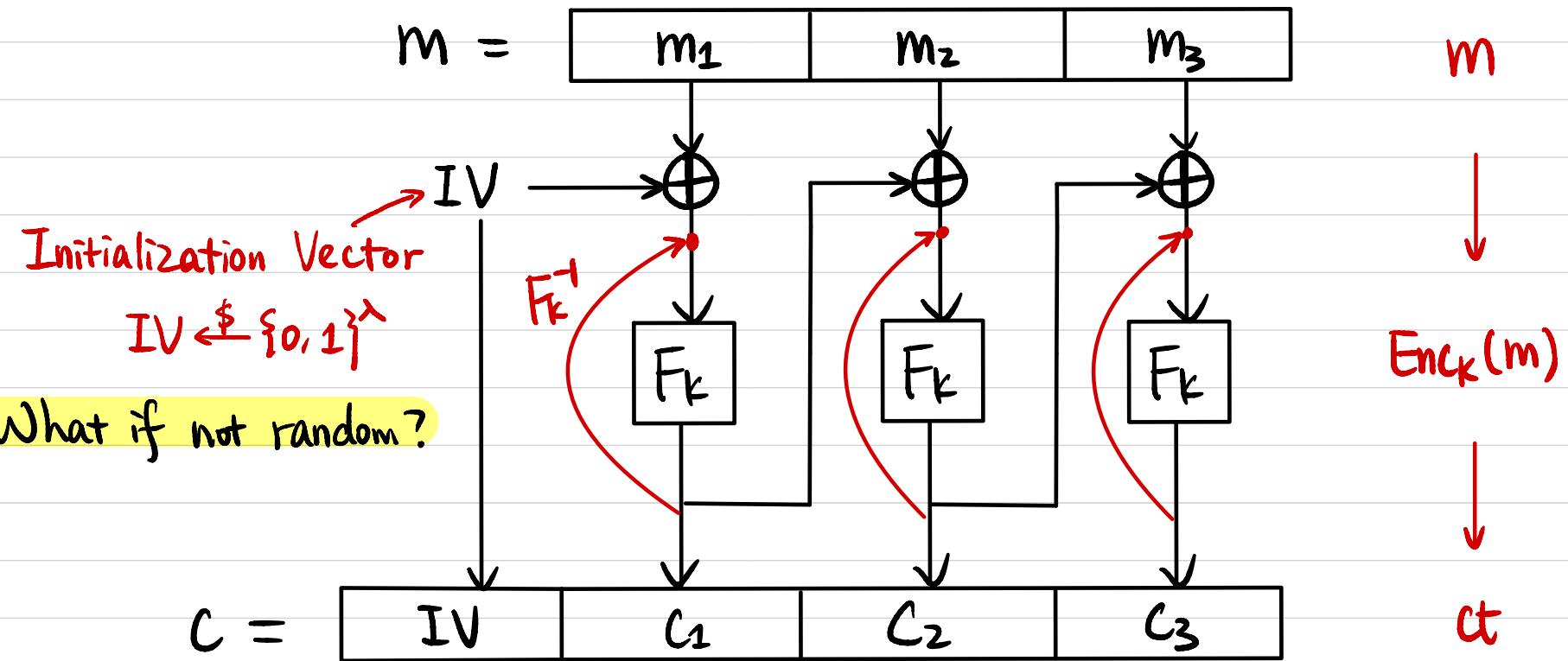
Goal: CPA (Chosen Plaintext Attack) Security

Electronic Code Book (ECB) Mode



CPA Secure? No! Deterministic!

Cipher Block Chaining (CBC) Mode

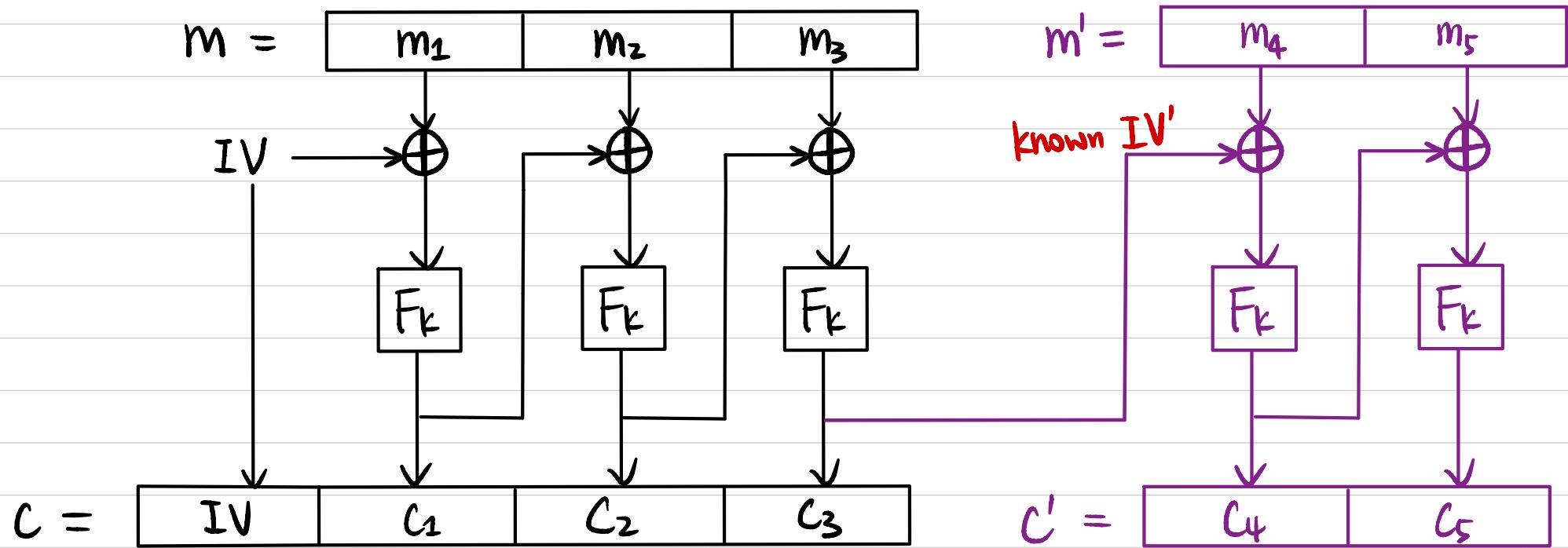


How to decrypt?

CPA Secure? YES!

Can we parallelize the computation? NO for Enc
YES for Dec

Chained Cipher Block Chaining (CBC) Mode

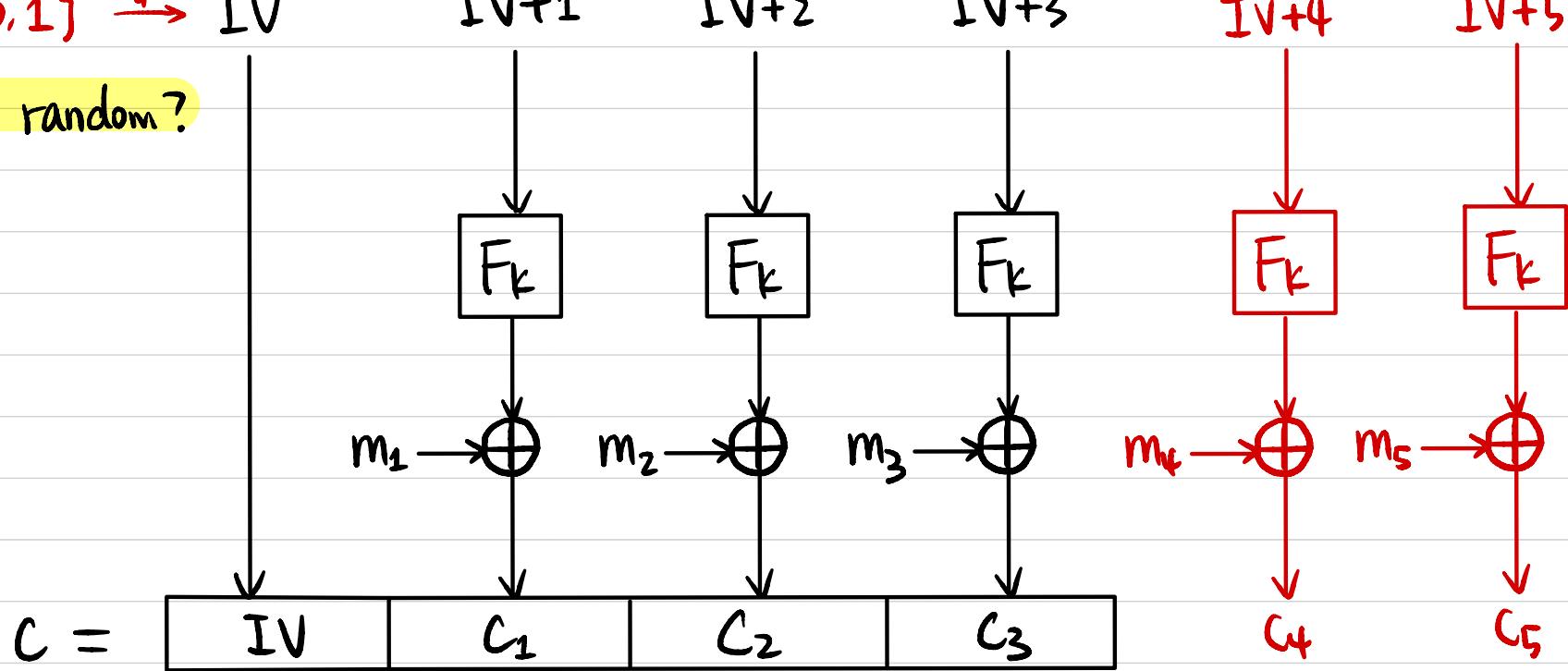


CPA Secure? No!

Counter (CTR) Mode

$$\{0,1\}^\lambda \xrightarrow{\$} IV = 0 \dots 0$$

What if not random?



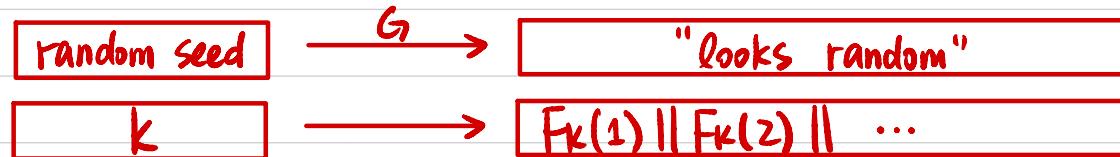
How to decrypt?

CPA Secure? YES!

"Stateful" CTR Mode? YES!

Can we parallelize the computation? YES!

PRG from PRF

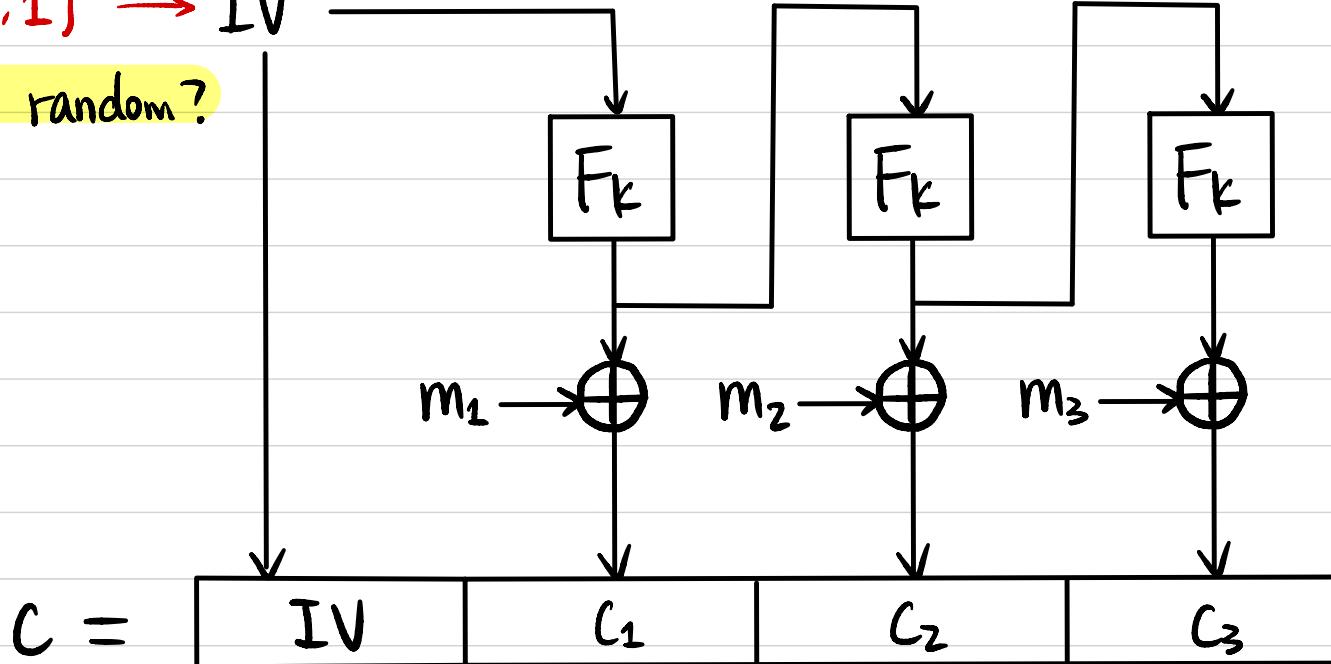


$$G(k) := F_k(1) \parallel F_k(2) \parallel \dots$$

Output Feedback (OFB) Mode

$\{0,1\}^\lambda \xrightarrow{\$} IV$

What if not random?



How to decrypt?

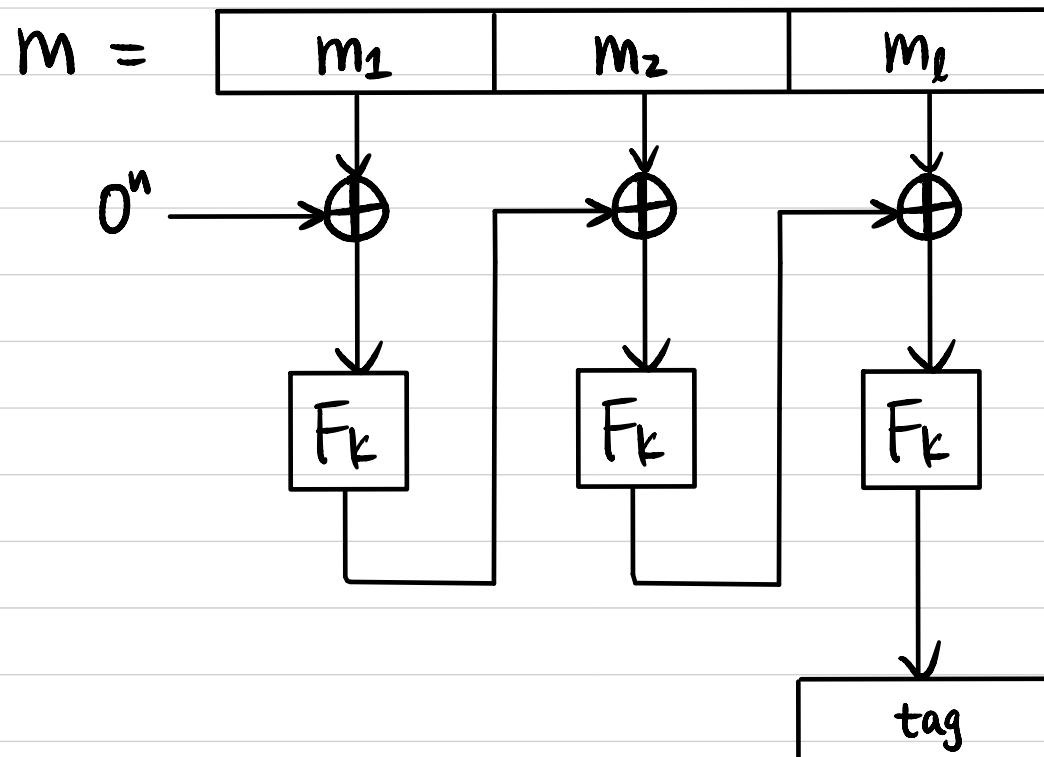
CPA Secure?

"Stateful" DFB Mode?

Can we parallelize the computation?

PRG from PRF

CBC-MAC



How to verify ?

CMA (Chosen Message Attack) Secure ?

- Fixed-length messages of length $l \cdot n$
- Arbitrary-length messages