CSCI 1515 Applied Cryptography

This Lecture:

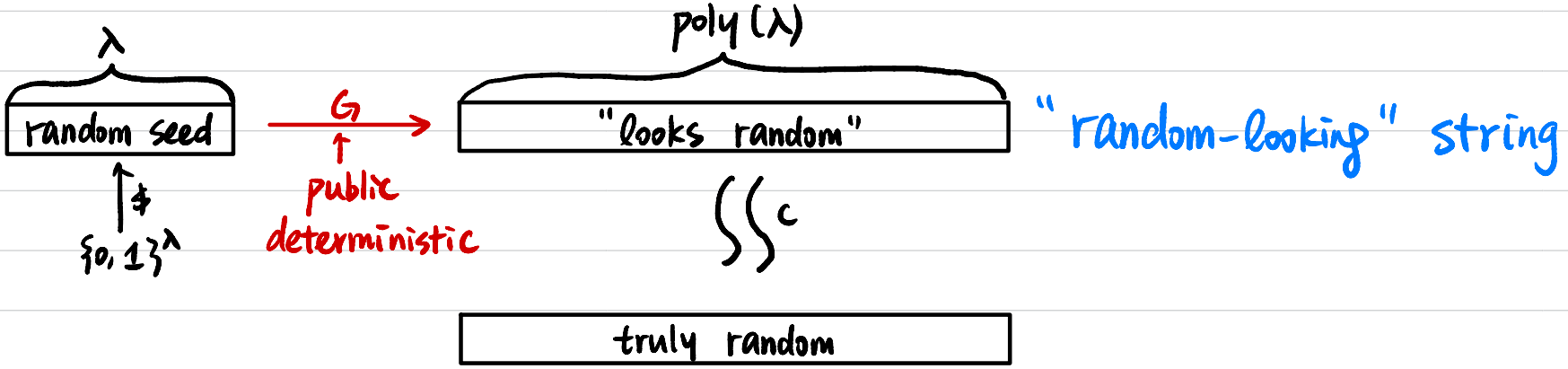
- Pseudorandom Function (PRF)
  Pseudorandom Permutation (PRP)
- Block Cipher and Modes of Operation
- CBC-MAC

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
Secrecy & 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

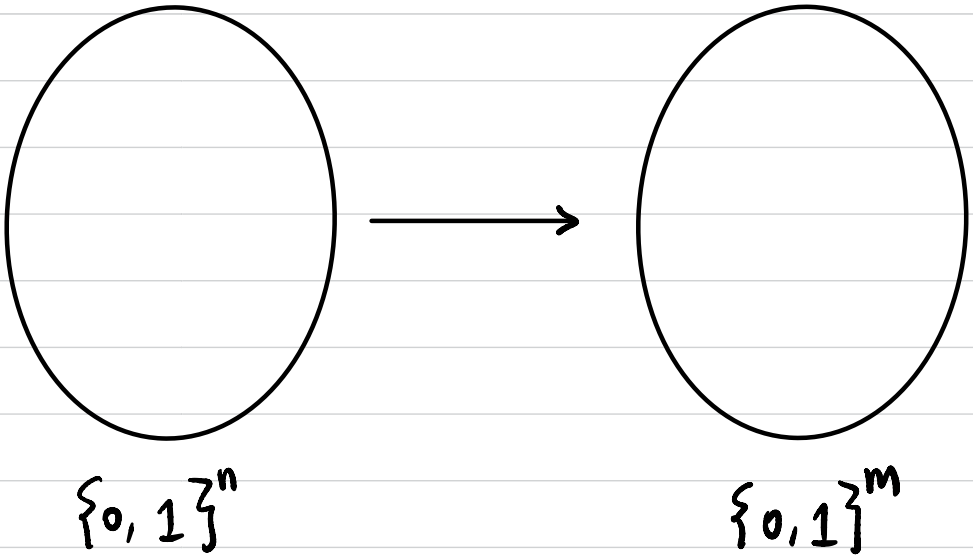
Pseudorandom Function (PRF)

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

$F(k, x) \to y$

- F: deterministic poly-time
- k: key
- x: input
- y: output

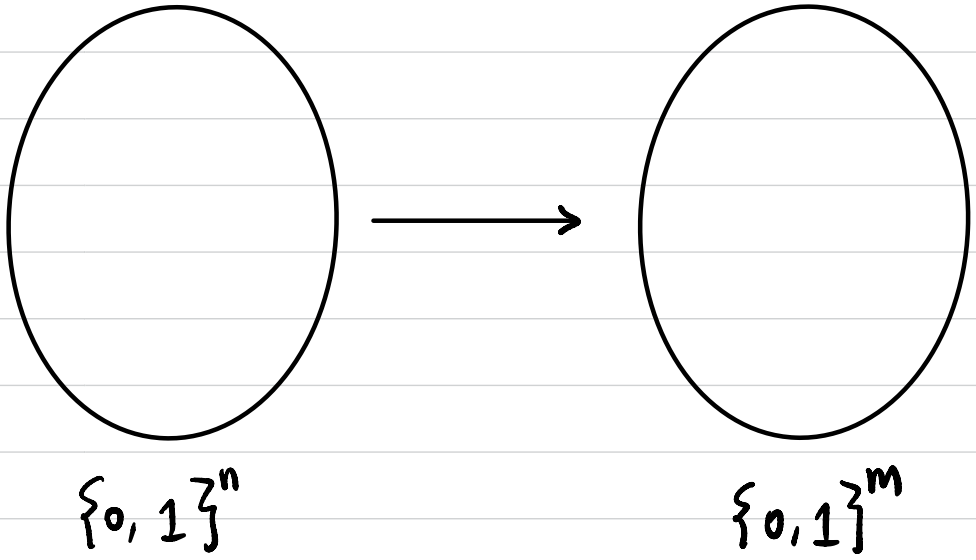
$k \xleftarrow{\$} \{0,1\}^\lambda$ $\quad F_k:$



"looks like a random function"

Pseudorandom Function (PRF)

$k \xleftarrow{\$} \{0,1\}^\lambda$ $\quad F_k :$



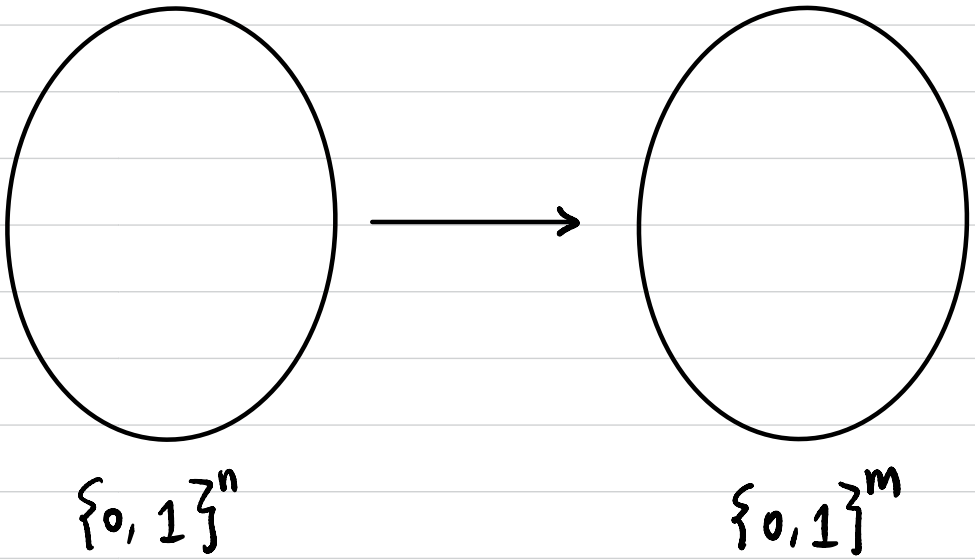
How many possible F_k's ?

2^λ

$\{\{C$ (not knowing k)

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

$f :$

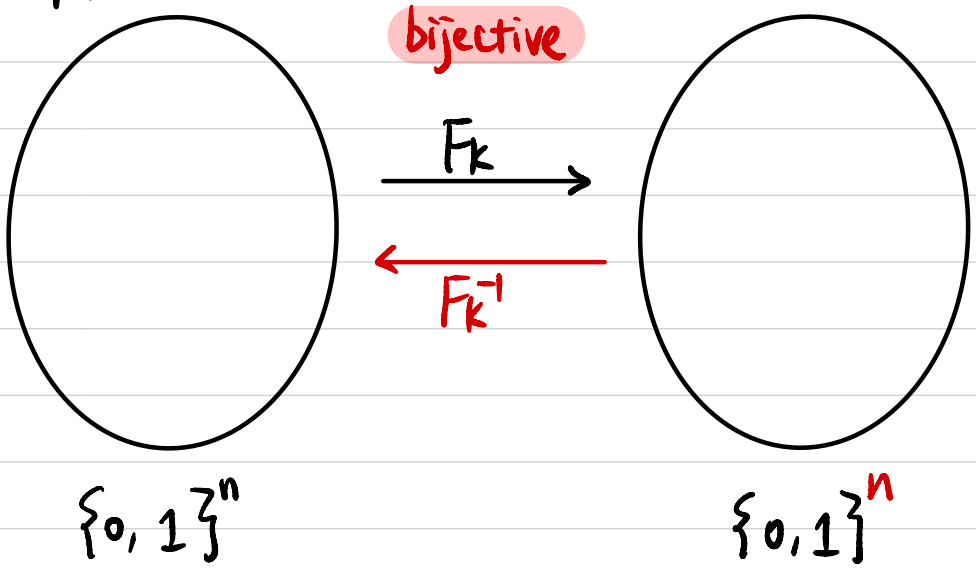


How many possible f's ?

$(2^m)^{2^n}$

Pseudorandom Permutation (PRP)

$k \xleftarrow{\$} \{0,1\}^\lambda$ $\quad F_k :$



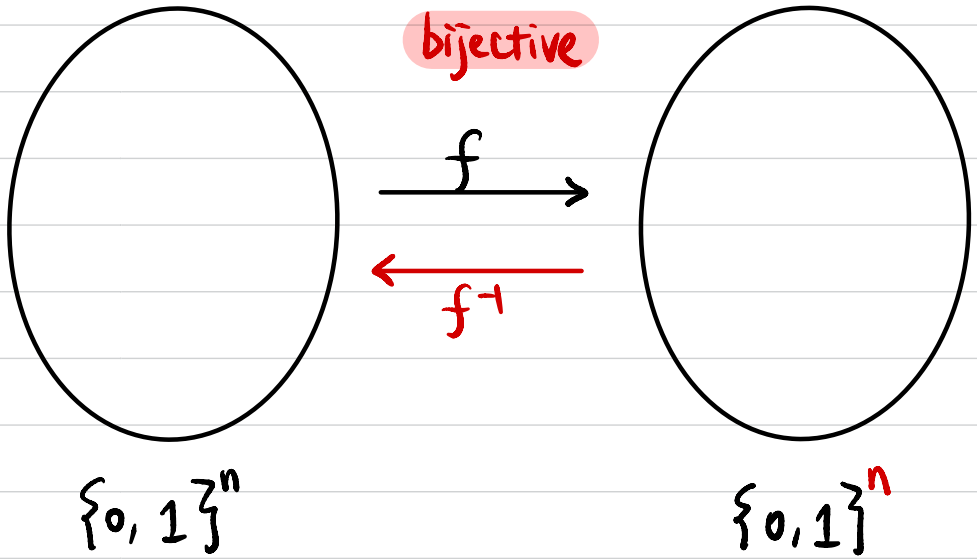
How many possible F_k's ?

2^λ

$\{\{\}\}_c$ (not knowing k)

$f \xleftarrow{\$} \{ F \mid F: \{0,1\}^n \to \{0,1\}^n,$ F is bijective $\}$

$f :$



How many possible f's ?

$2^n!$

Block Cipher

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

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

$$F: \{0,1\}^{\lambda} \times \{0,1\}^{\lambda} \to \{0,1\}^{\lambda}$$ ← 128

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

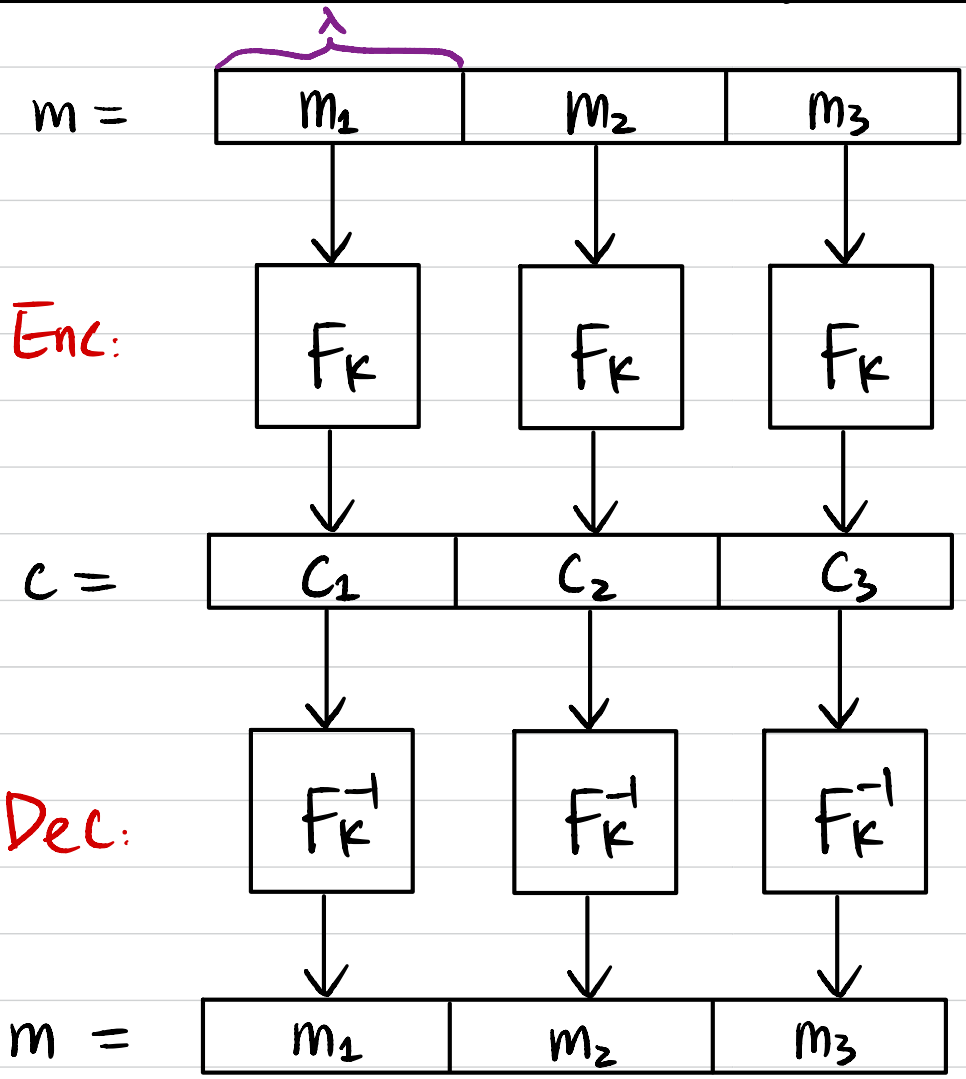
Construct an SKE scheme from F for **arbitrary-length messages**.

- $k \xleftarrow{\$} \{0,1\}^{\lambda}$
- $Enc_k(m)$
- $Dec_k(c)$

$|m| = \alpha \cdot \lambda$ (If not, pad it to a multiple of λ)

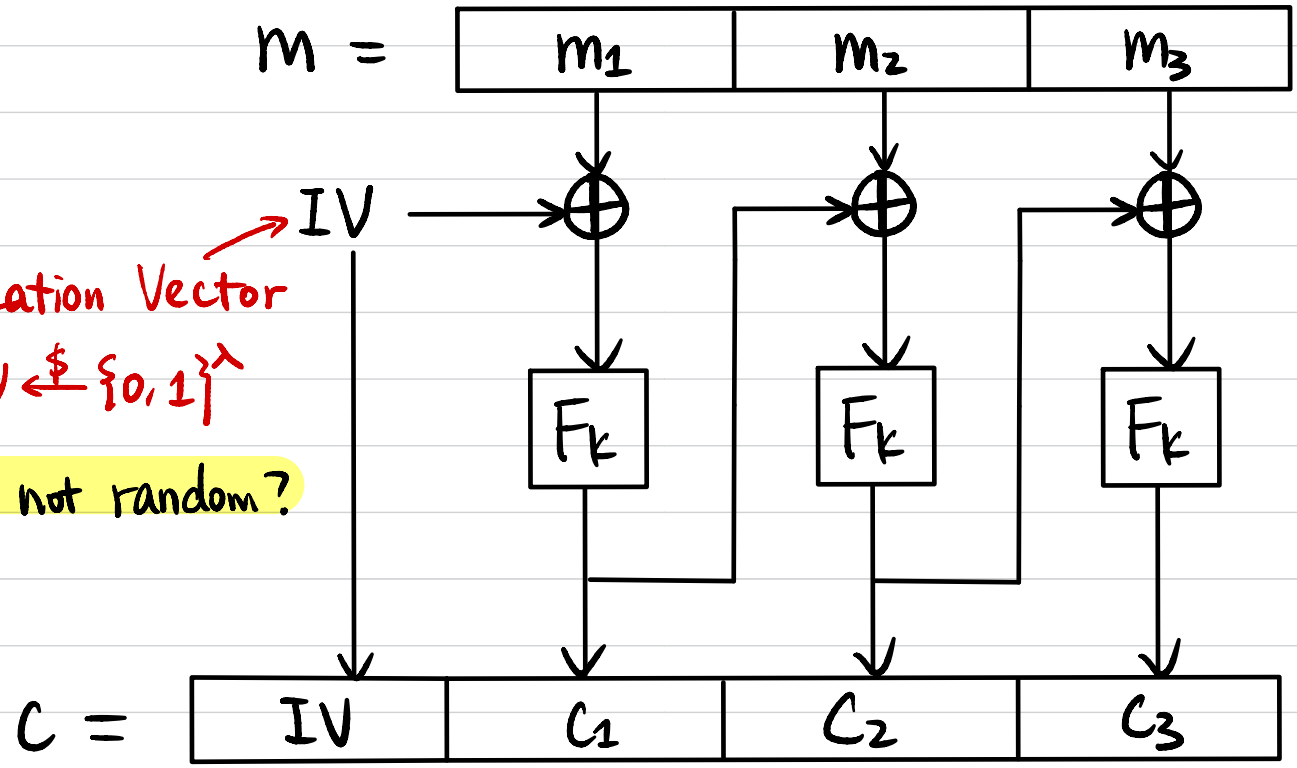
Goal: CPA (Chosen Plaintext Attack) Security

Electronic Code Book (ECB) Mode



CPA secure?

Cipher Block Chaining (CBC) Mode



Initialization Vector

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

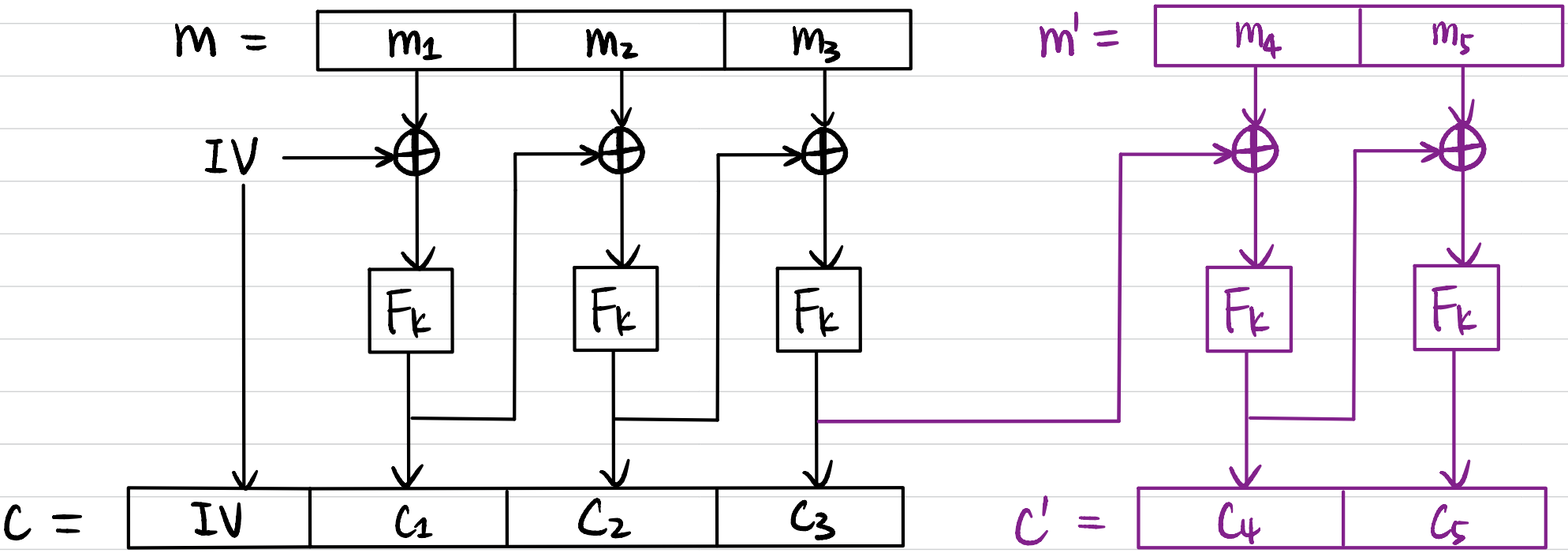
What if not random?

How to decrypt?

CPA secure?

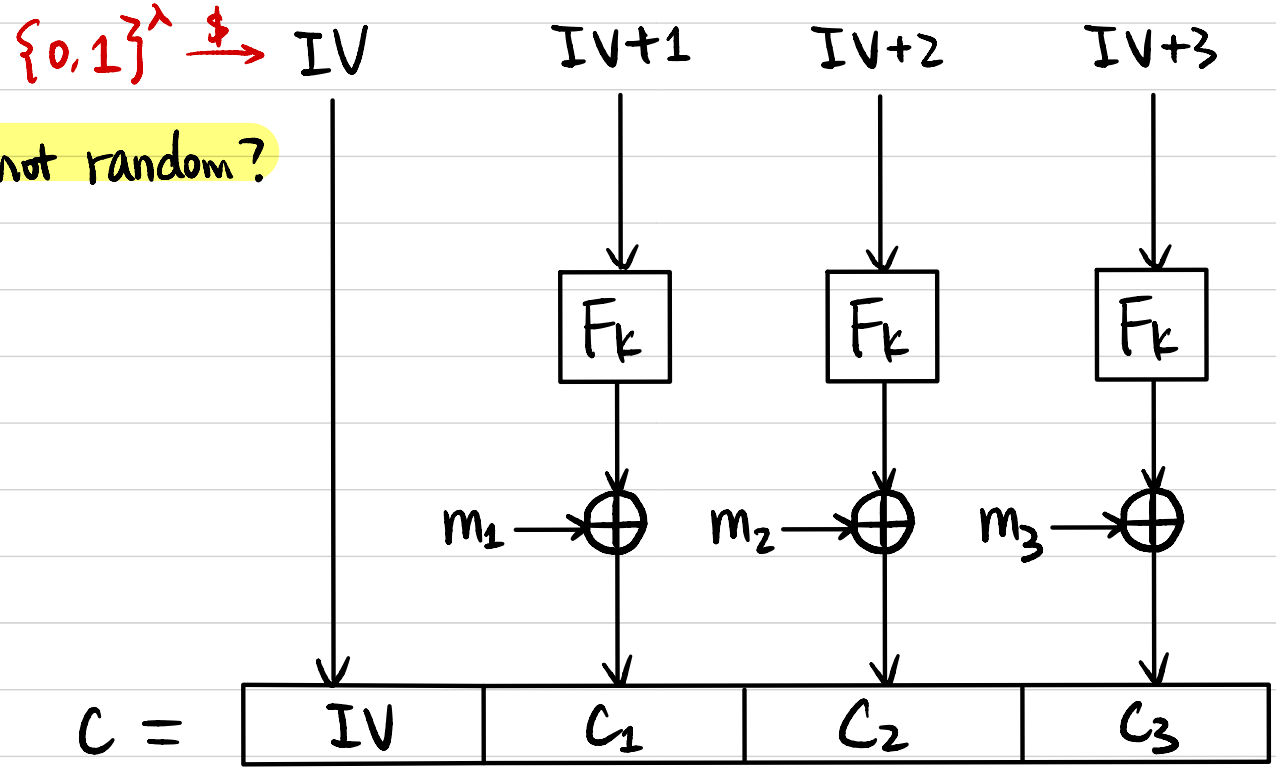
Can we parallelize the computation?

Chained Cipher Block Chaining (CBC) Mode



CPA secure ?

Counter (CTR) Mode



What if not random?

How to decrypt?

CPA secure?

"Stateful" CTR Mode?

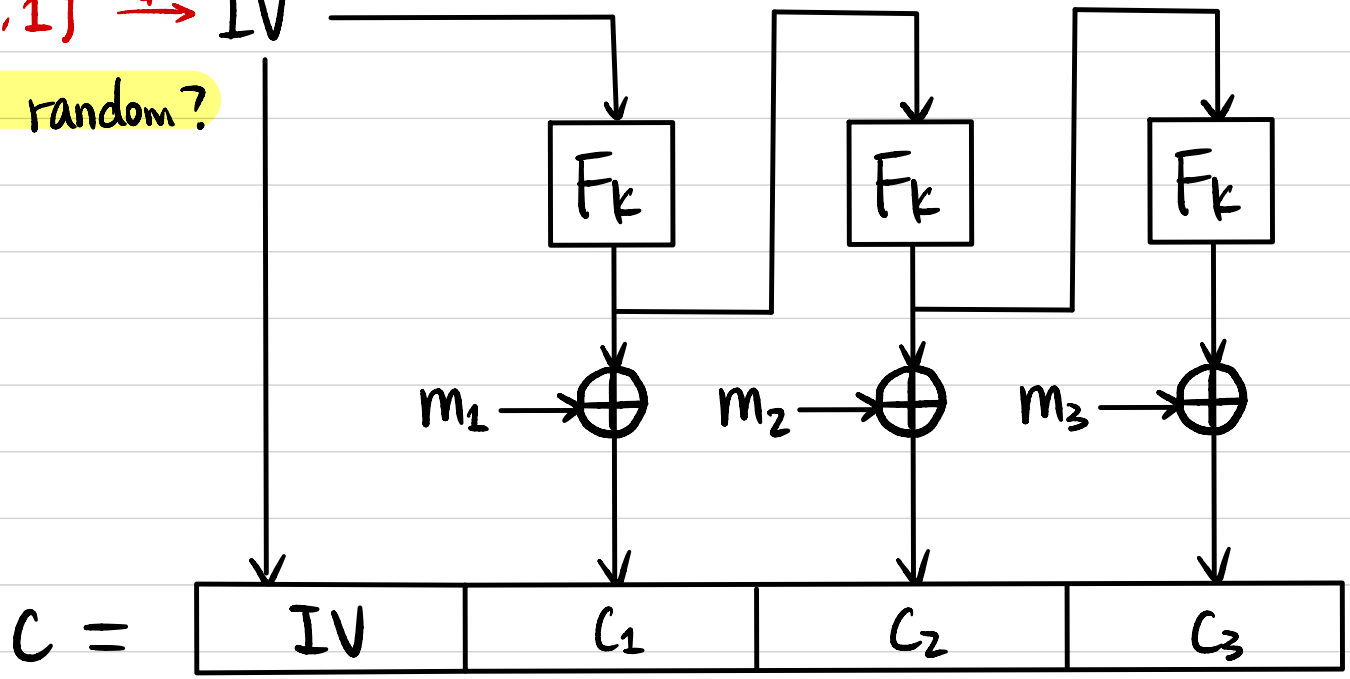
Can we parallelize the computation?

PRG from PRF

Output Feedback (OFB) Mode

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

What if not random?



How to decrypt?

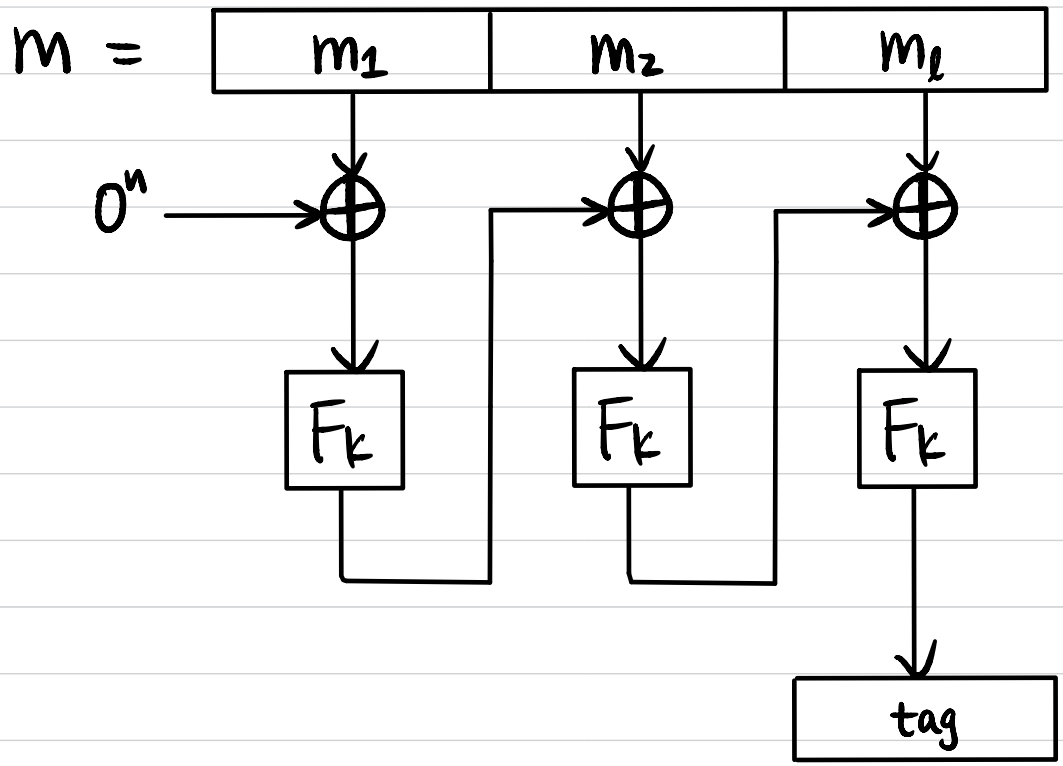
CPA secure?

"Stateful" OFB Mode?

Can we parallelize the computation?

PRG from PRF

CBC-MAC

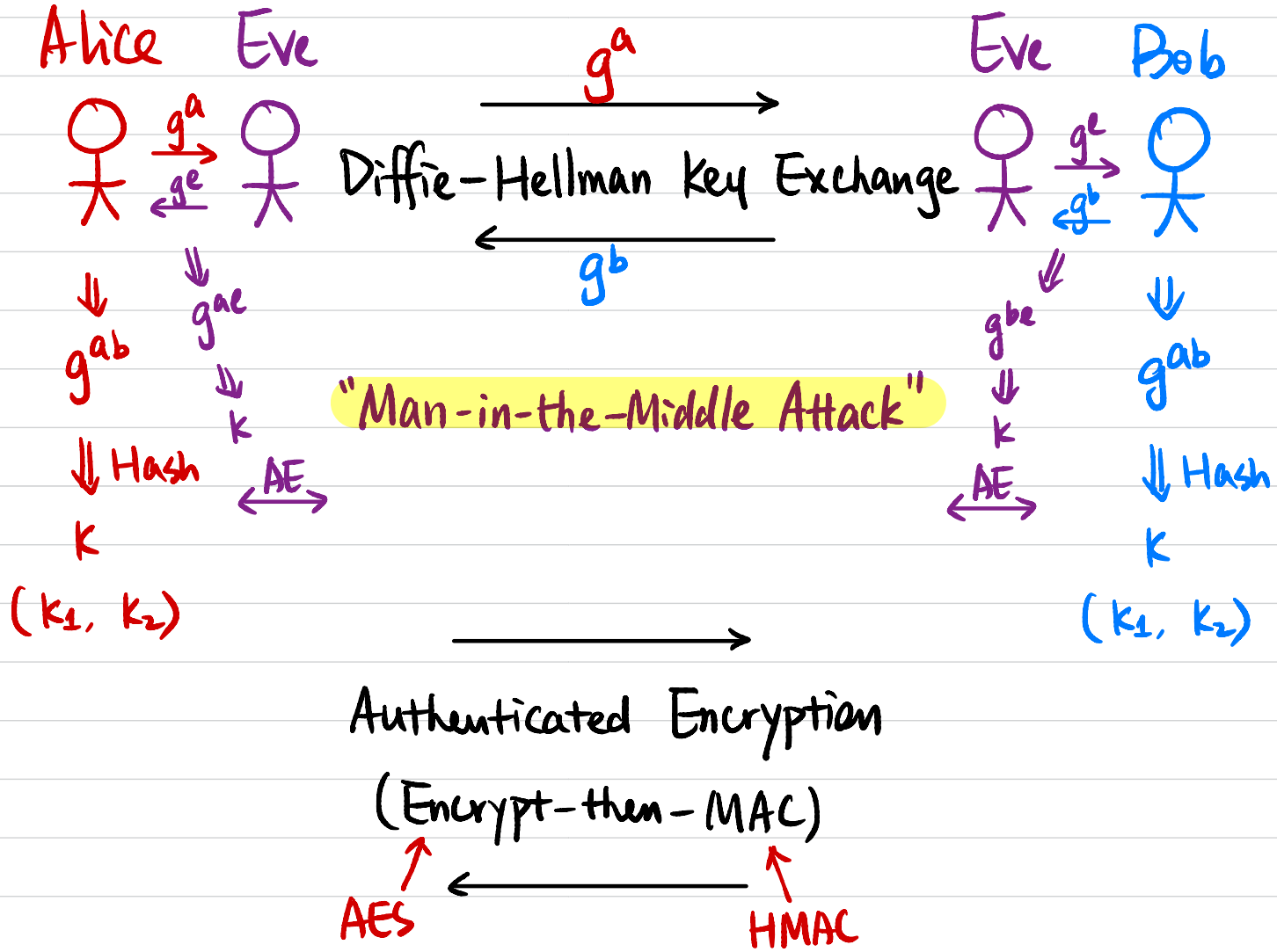


How to verify?

CMA (Chosen Message Attack) Secure?

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

Putting it All Together: Secure Communication



Any security issue?