CSCI 1515 Applied Cryptography

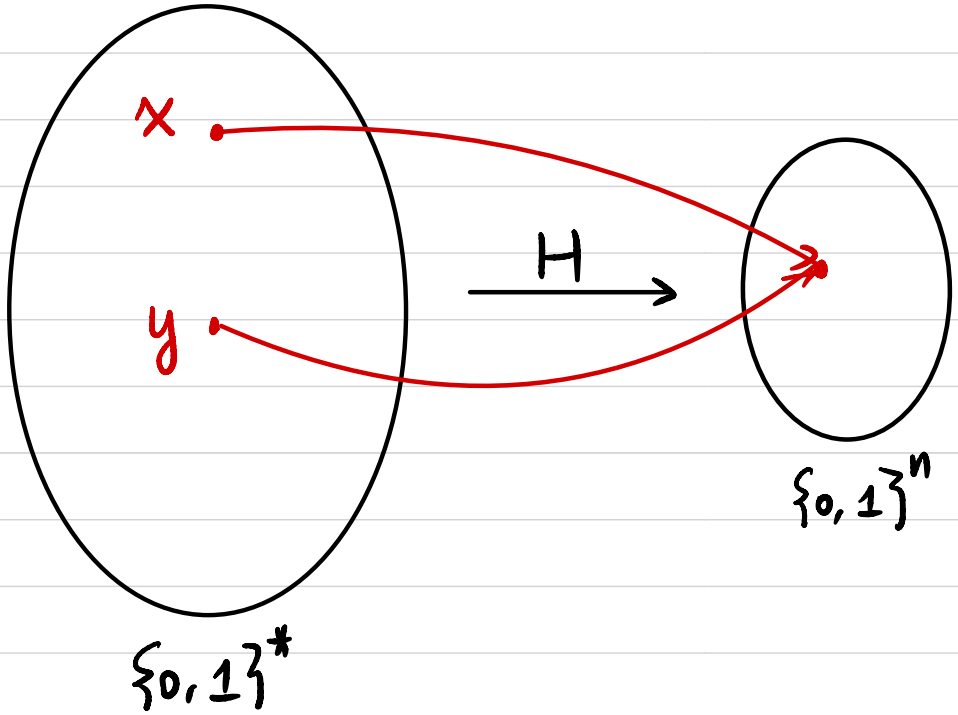
This Lecture:

- Applications of Hash Functions
- Putting it Together: Secure Communication
- Pseudorandom Generator (PRG)
  Pseudorandom Function (PRF)
  Pseudorandom Permutation (PRP)
- Block Cipher and Modes of Operation

Hash Function

$\lambda = 128$
$n = 256$

$H: \{0,1\}^* \longrightarrow \{0,1\}^n$



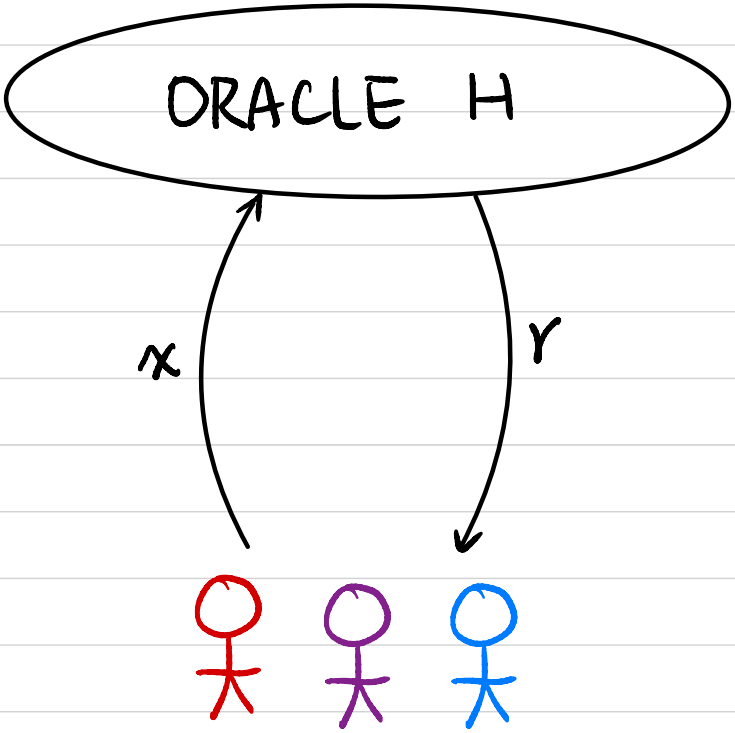
Collision-Resistant Hash Function (CRHF):

It's computationally hard to find $x, y \in \{0,1\}^*$ s.t.

$x \neq y, \quad H(x) = H(y)$ (collision)

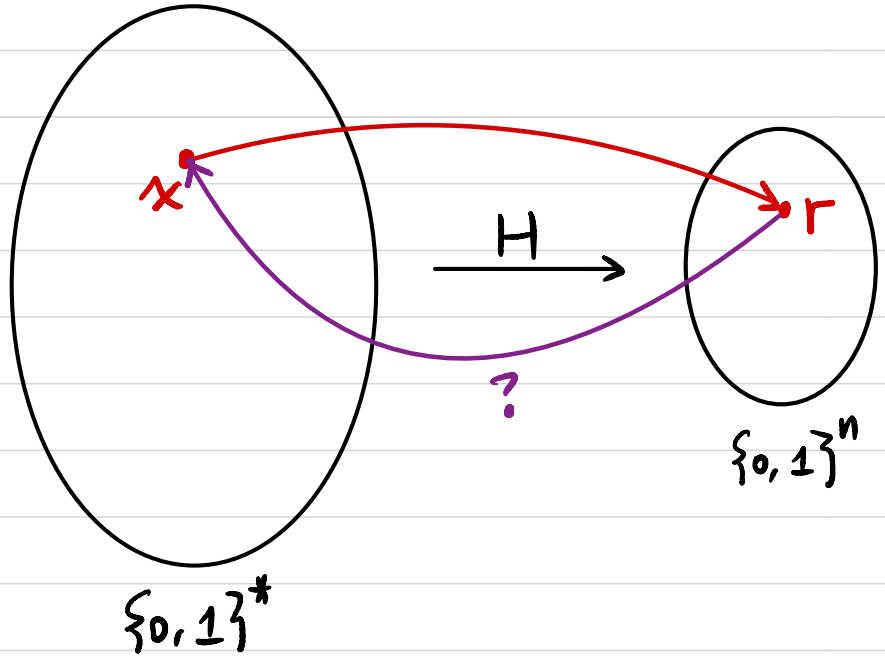
Random Oracle Model

$H: \{0,1\}^* \longrightarrow \{0,1\}^n$



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

$H(x) := r$



Constructions for 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

Applications of Hash Functions

- **HMAC**

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

$Mac_k(m) = H(k \| m)$

$Mac_k(m) = H(k \| H(k \| m))$

$HMAC_k(m) = H(k_1 \| H(k_2 \| m))$

$k_1 = k \oplus opad$ (public)

$k_2 = k \oplus ipad$ (public)

- **Hash-and-Sign**: $Sign_{sk}(H(m))$

RSA Signature: $Sign_{sk}(m) = H(m)^d \bmod N$

- **Password-based Authentication**

username, $H(password)$

Applications of Hash Functions

- **Deduplication**

$H(D_1) \rightarrow h_1$

$H(D_2) \rightarrow h_2$

unique identifier

If $h_1 \neq h_2 \Rightarrow D_1 \neq D_2$

If $h_1 = h_2 \Rightarrow D_1 = D_2$ (why?)

Virus Scan $H(F) \stackrel{?}{=} H(F^*)$

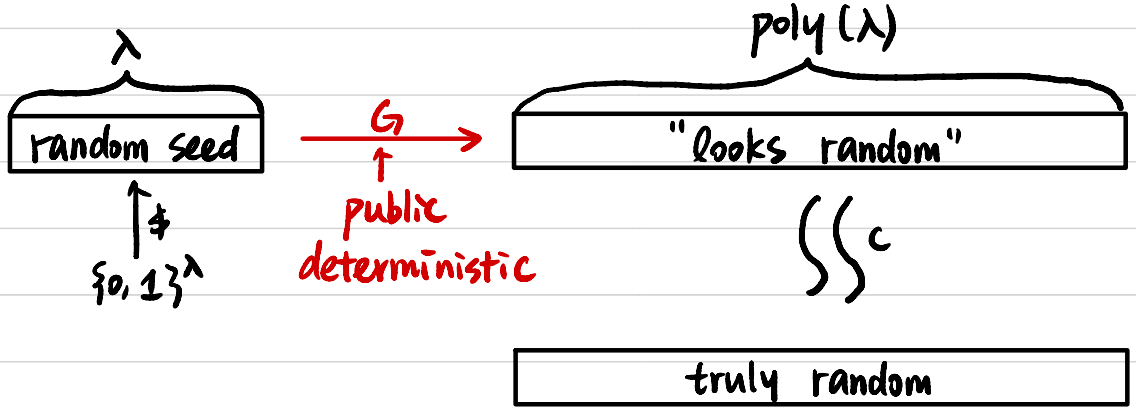
Video Deduplication $H(V_1) \stackrel{?}{=} H(V_2)$

Applications of Hash Functions

- **HKDF (Key Derivation Function)**:

  $HMAC(g^{ab}, salt)$

Pseudorandom Generator (PRG)



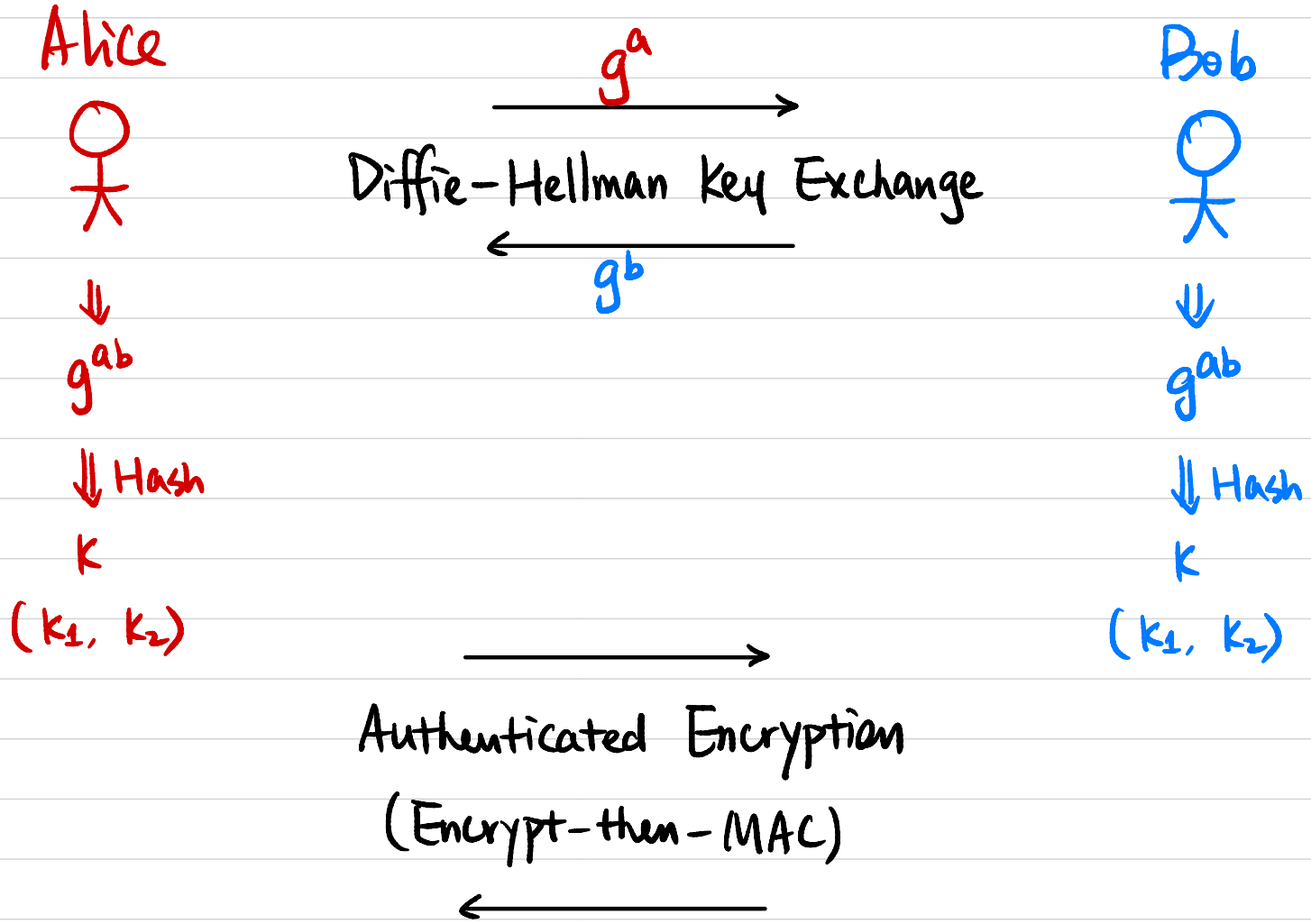
- Fast Membership Proof (Merkle Tree) → blockchain

- SKE Scheme ?

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

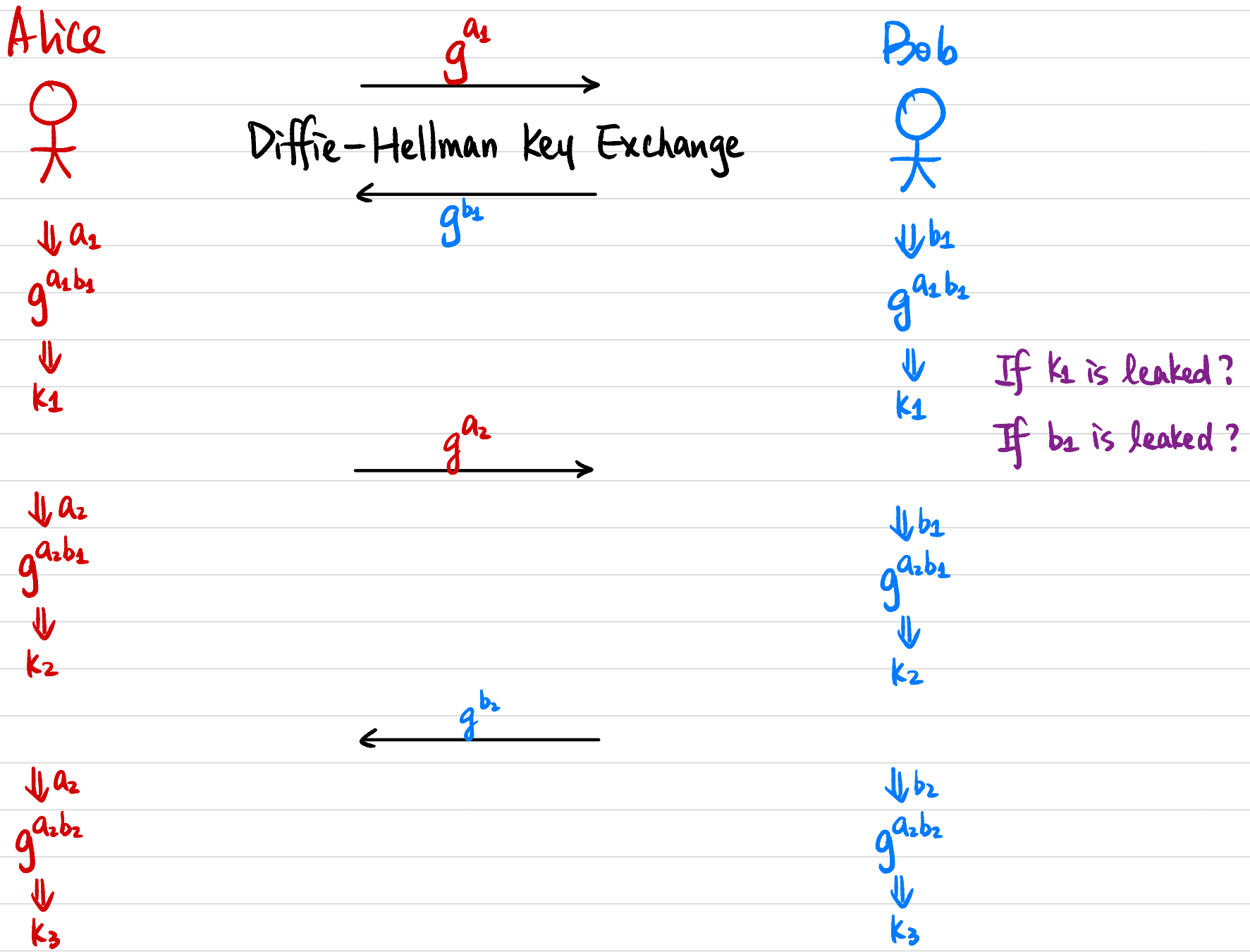
  $Enc_k(m) = H(k \| m)$?

Putting it Together: Secure Communication



Any security issue?

Signal: Diffie-Hellman Ratchet

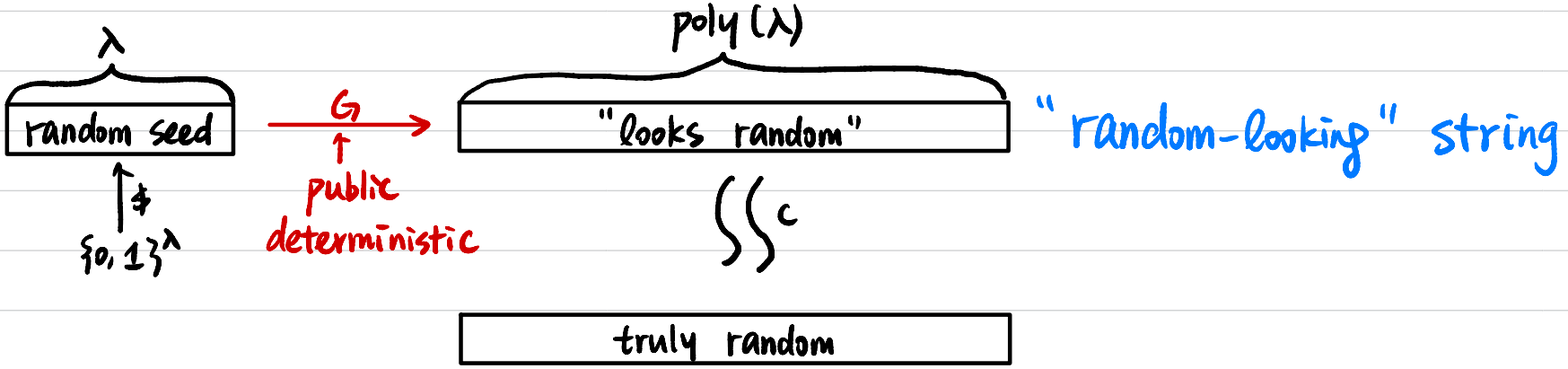


Summary

	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)



"random-looking" string

Pseudorandom Function (PRF):

"random-looking" function

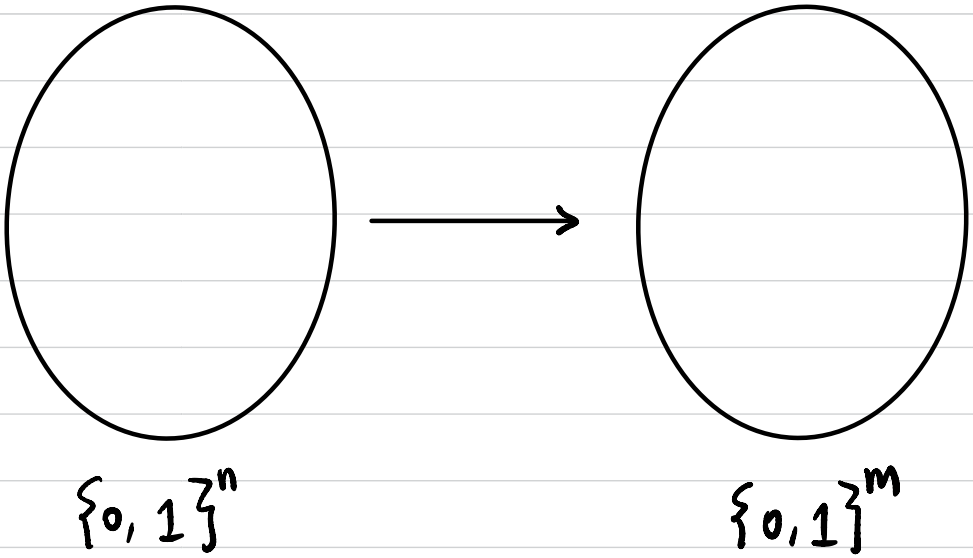
Pseudorandom Function (PRF)

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

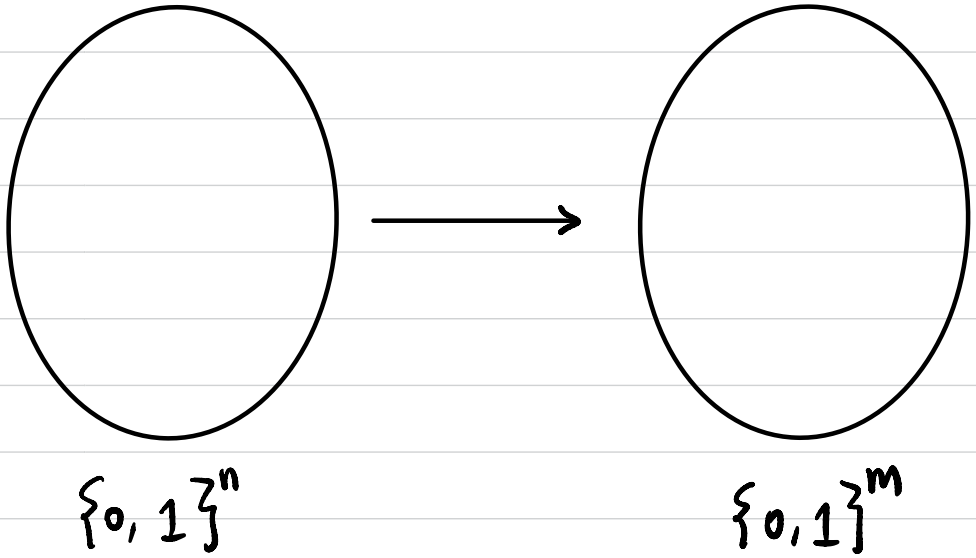
$k \xleftarrow{\$} \{0,1\}^\lambda$ $\quad F_k:$



"looks like a random function"

Pseudorandom Function (PRF)

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

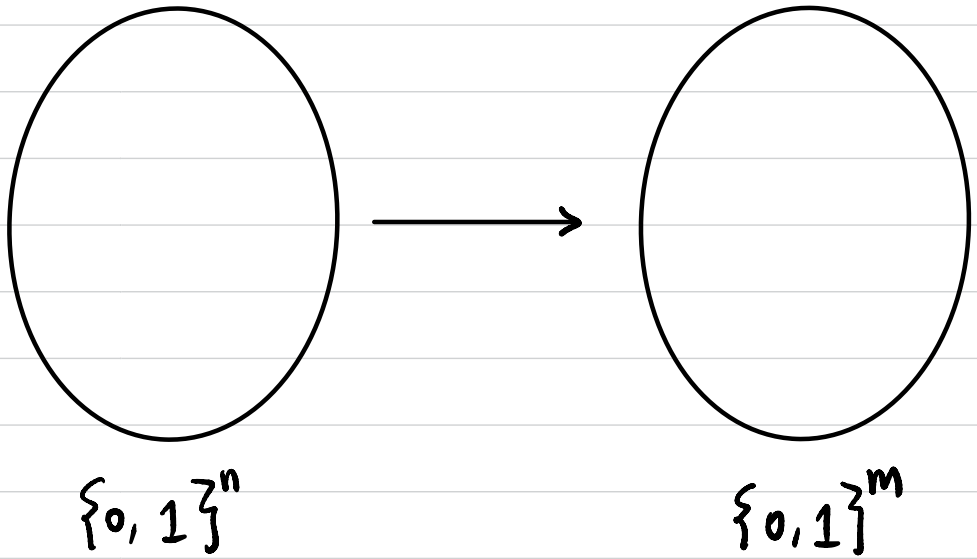


How many possible F_k's ?

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

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

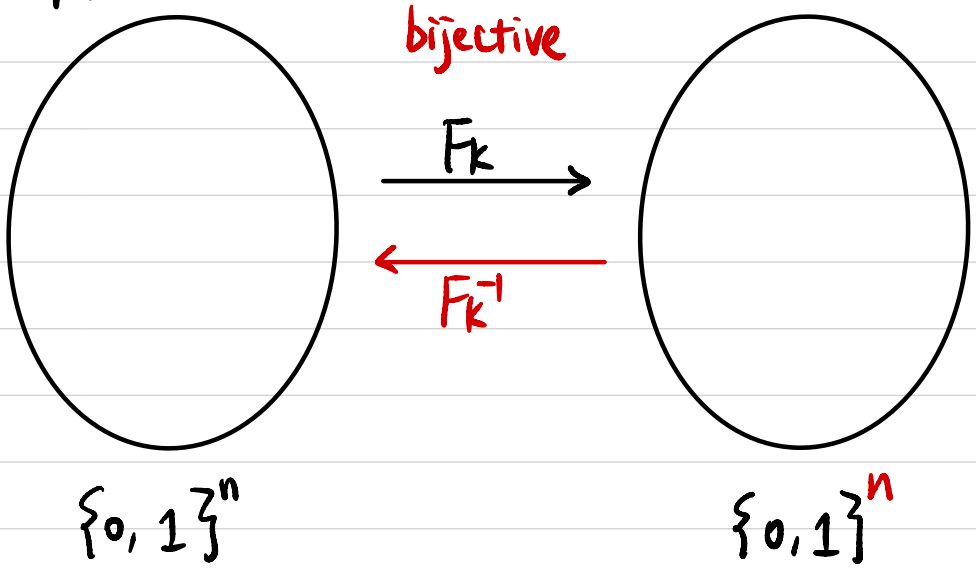
$f :$



How many possible f's ?

Pseudorandom Permutation (PRP)

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

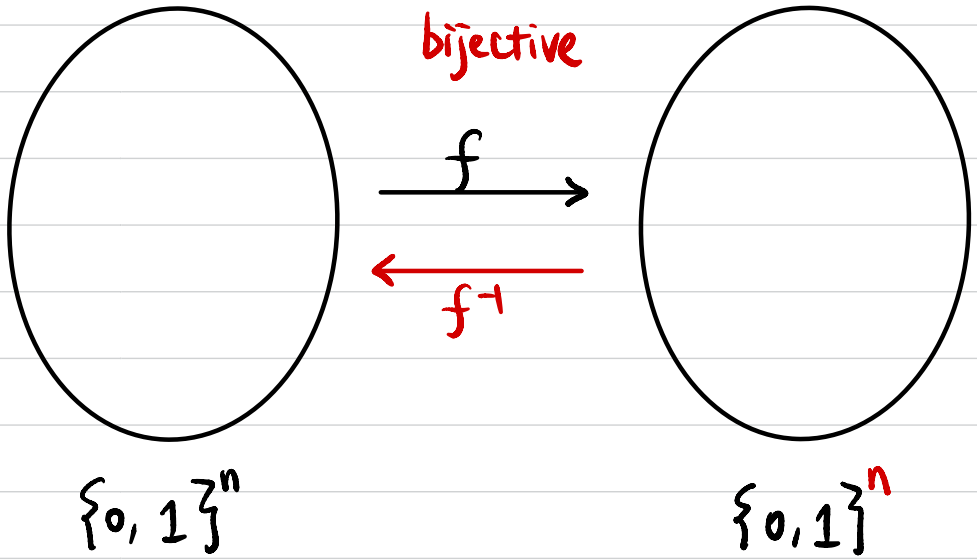


How many possible F_k's ?

$\{\!\{ c \}\!\}$ (not knowing k)

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

$f :$



How many possible f's ?

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)

- $\lambda = n = 128$
- Standardized by NIST in 2001
- Competition 1997-2000

Before AES: Data Encryption Standard (DES)

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

Block Cipher Modes of Operation

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

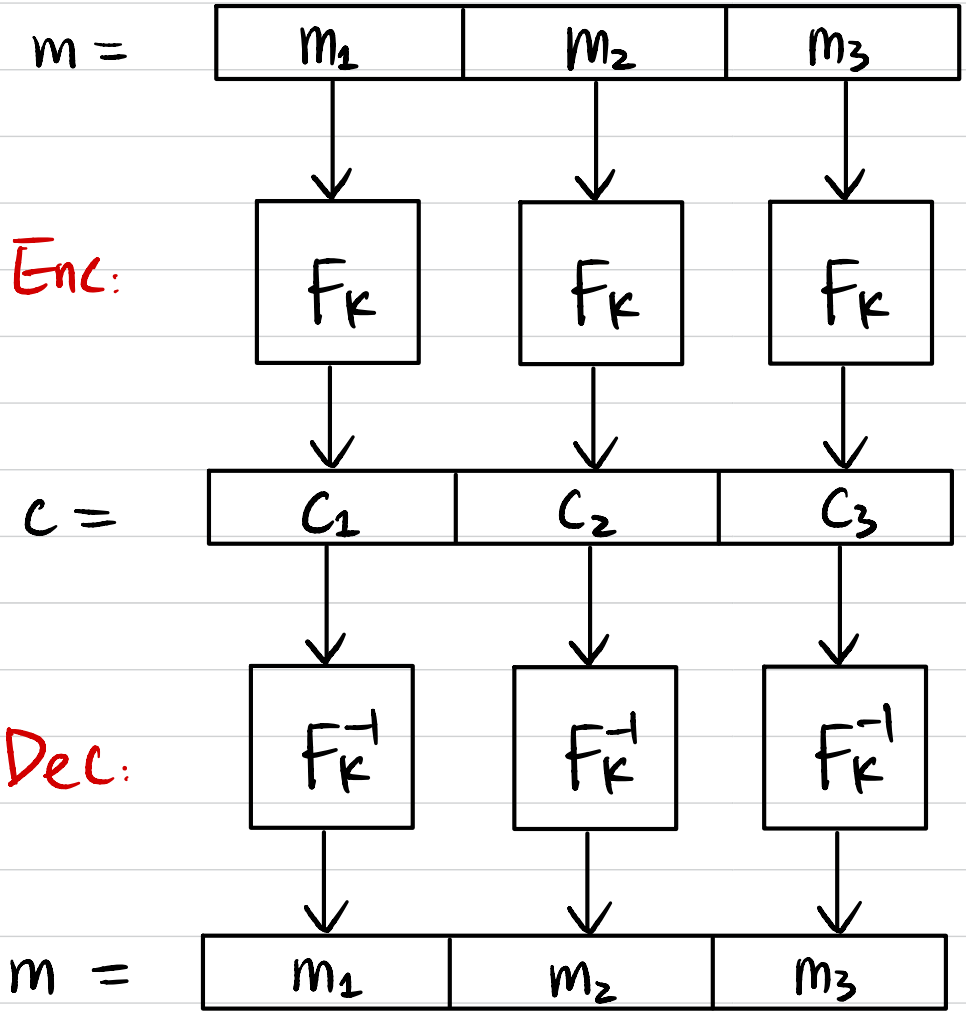
Construct an SKE scheme from F for arbitrary-length messages.

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

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

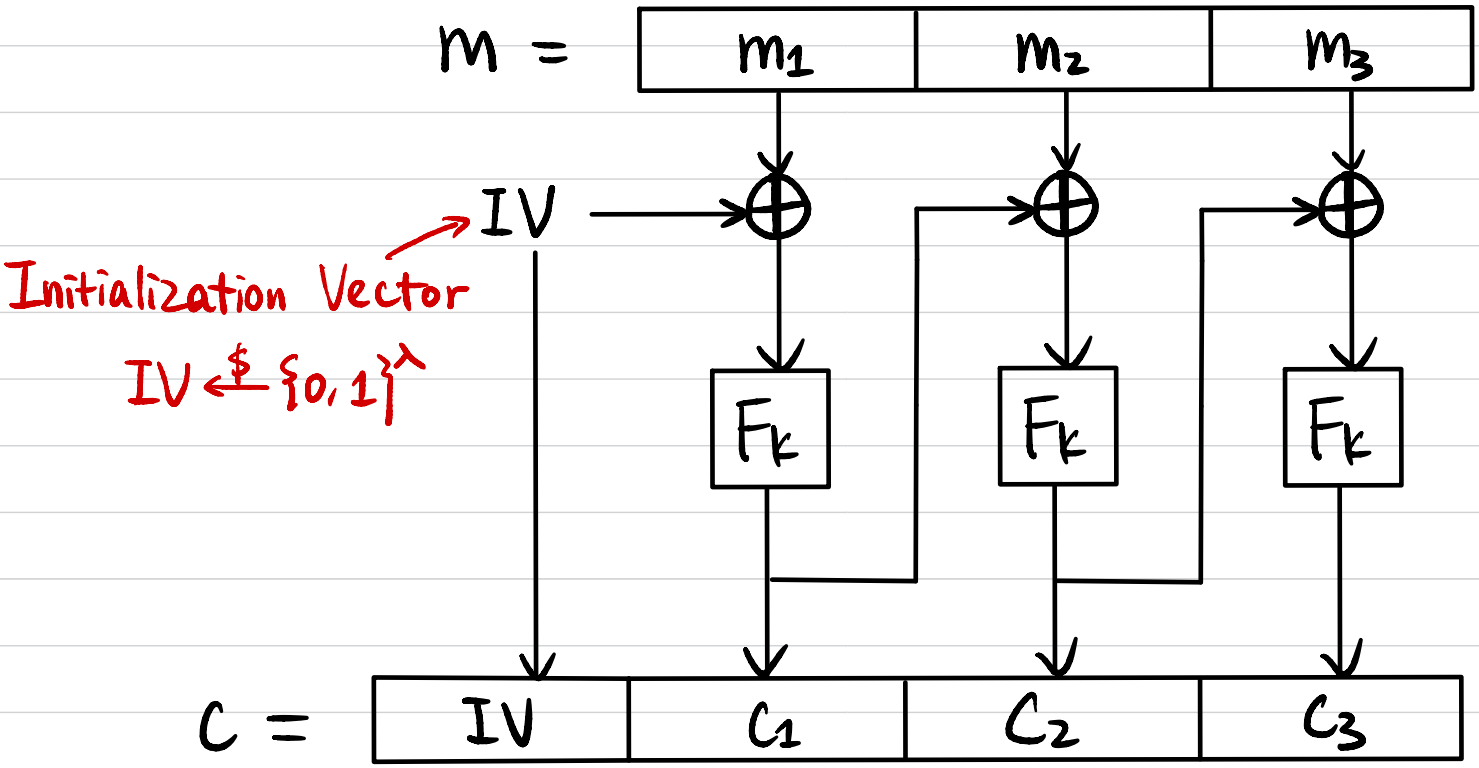
Goal: CPA (Chosen Plaintext Attack) Security

Electronic Code Book (ECB) Mode



CPA secure?

Cipher Block Chaining (CBC) Mode

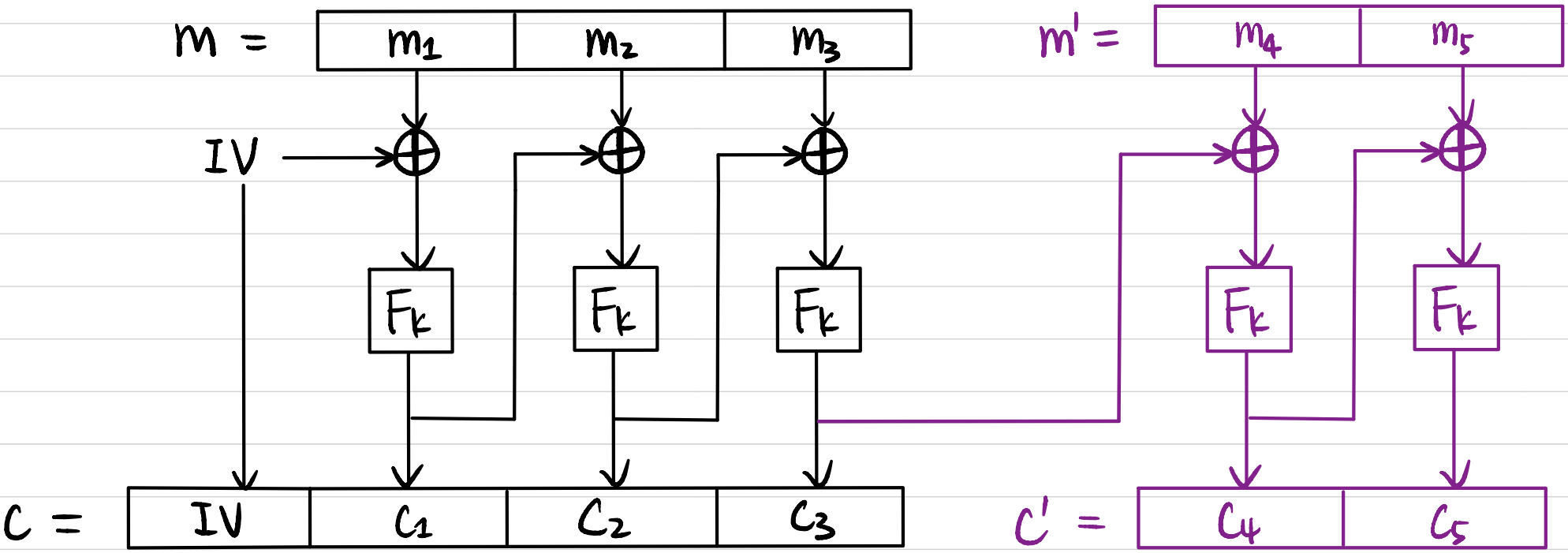


How to decrypt?

CPA secure?

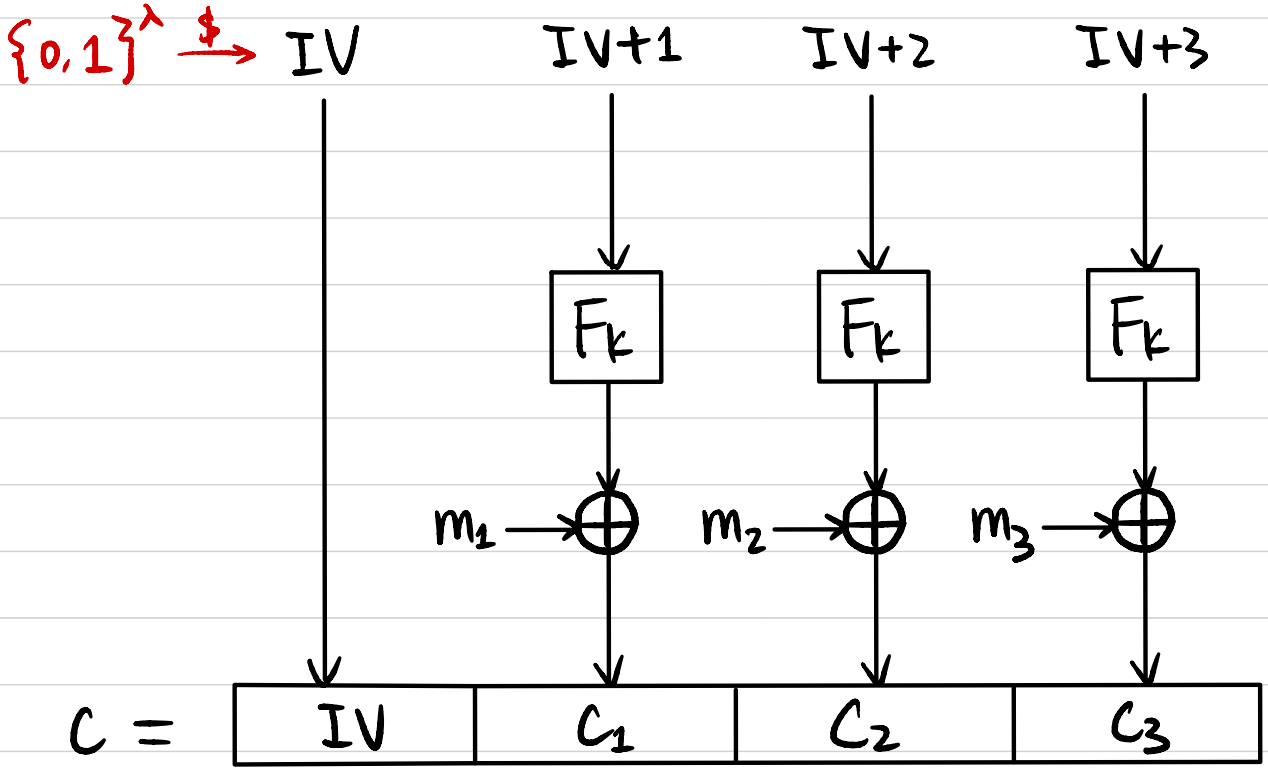
Can we parallelize the computation?

Chained Cipher Block Chaining (CBC) Mode



CPA secure?

Counter (CTR) Mode



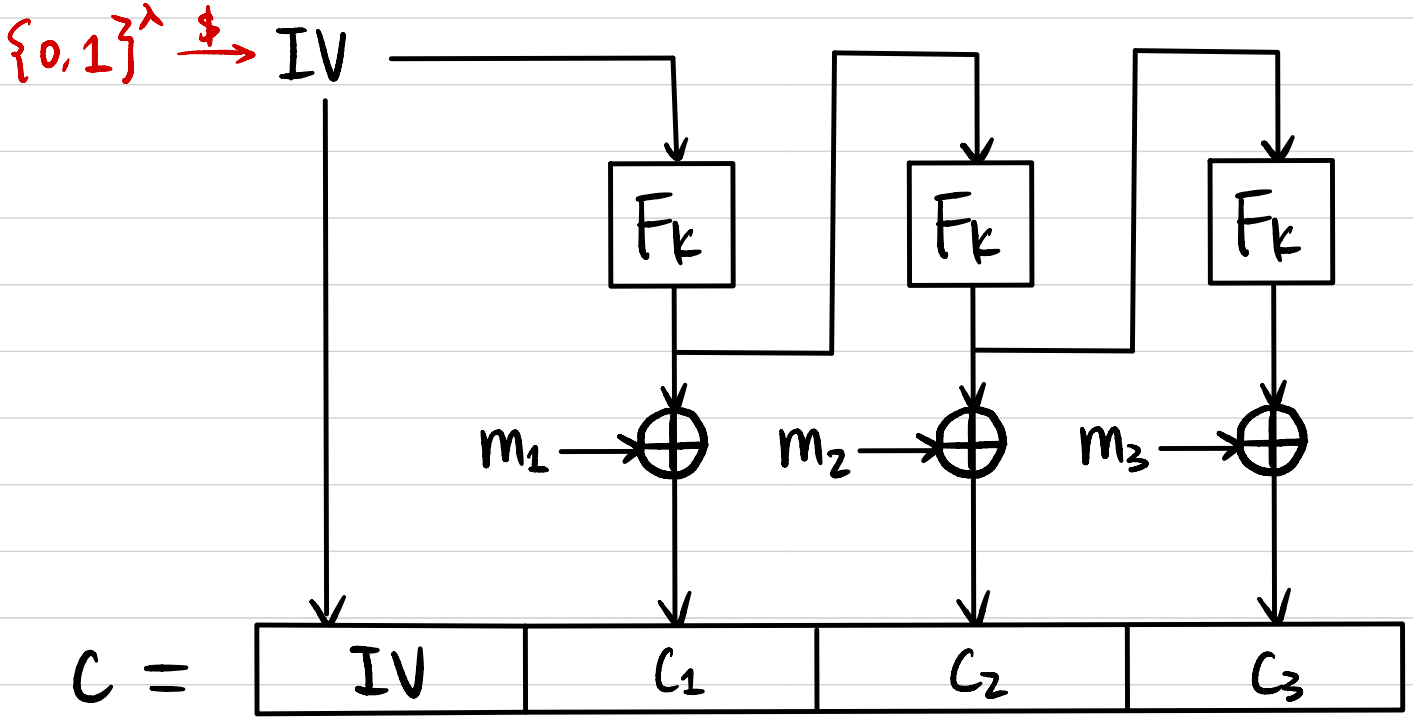
How to decrypt?

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