CSCI 1515 Applied Cryptography

This Lecture:

- Block Cipher Modes of Operation
- Public Key Infrastructure (PKI)

Block Cipher Modes of Operation

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

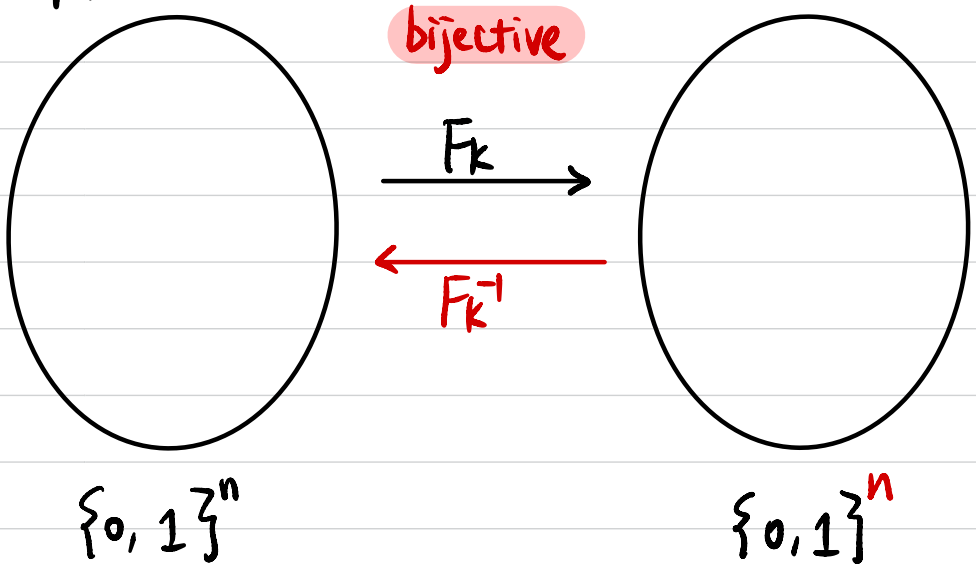
Assumed to be a **pseudorandom permutation (PRP)**.

Goal: Construct a **symmetric-key encryption (SKE) scheme** for **arbitrary-length messages** with **chosen-plaintext Attack (CPA) security**.

- $k \xleftarrow{\$} \{0,1\}^\lambda$
- $\text{Enc}_k(m)$ $|m| = \alpha \cdot \lambda$ (If not, pad it to a multiple of λ)
- $\text{Dec}_k(c)$

Pseudorandom Permutation (PRP)

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



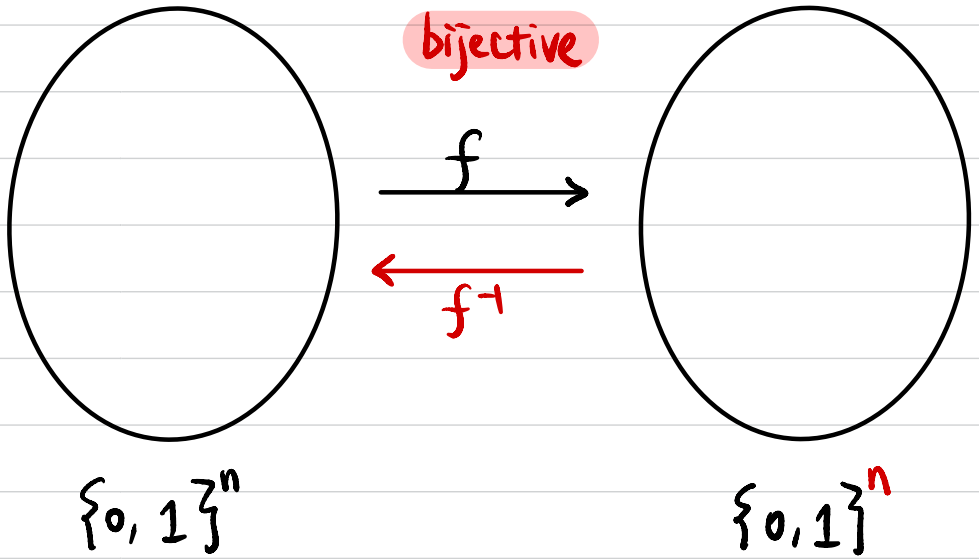
How many possible F_k's ?

2^λ

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

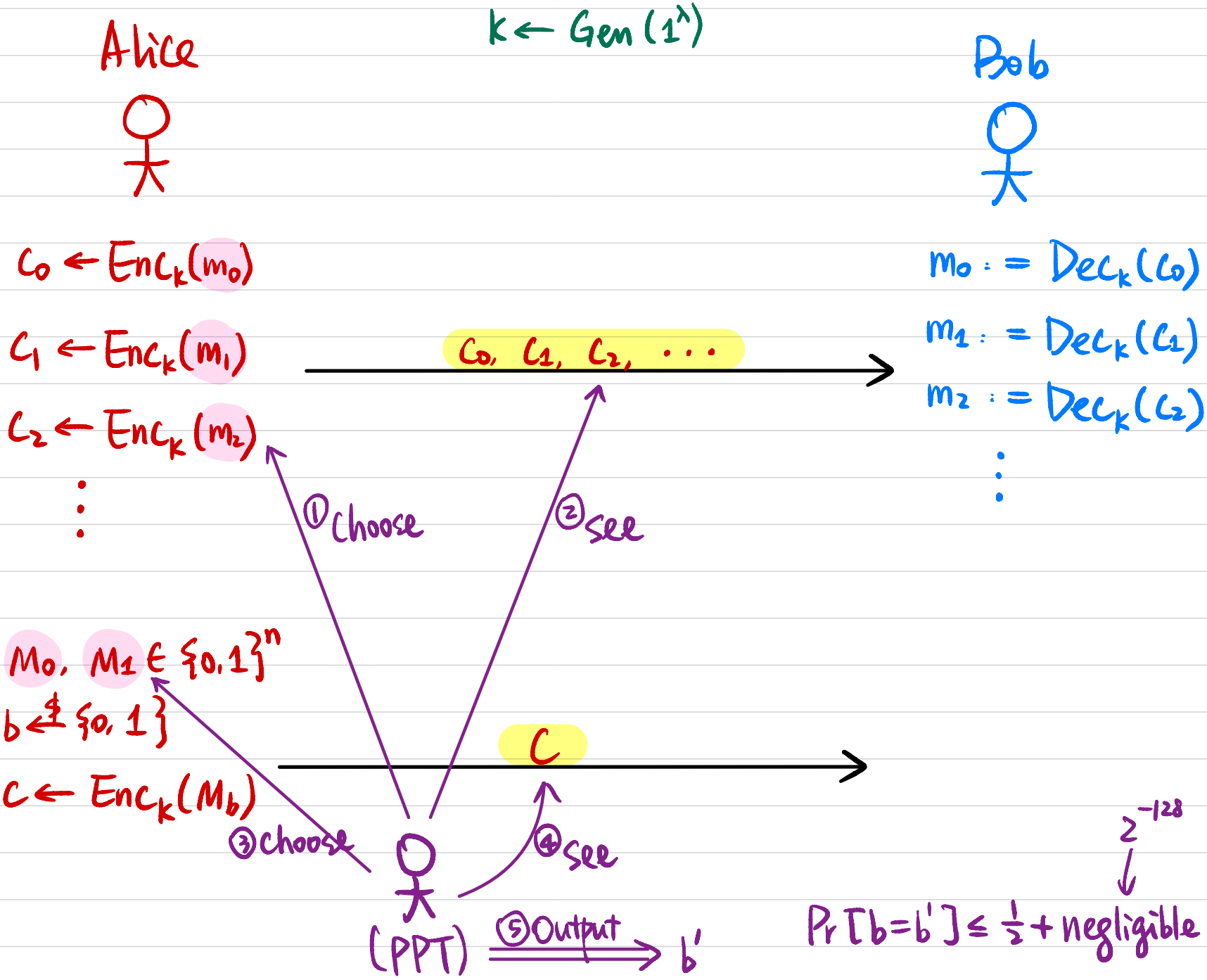
$f \xleftarrow{\$} \{ F \mid F: \{0,1\}^n \to \{0,1\}^n,$
F is bijective $\}$

$2^n!$ $\quad f:$

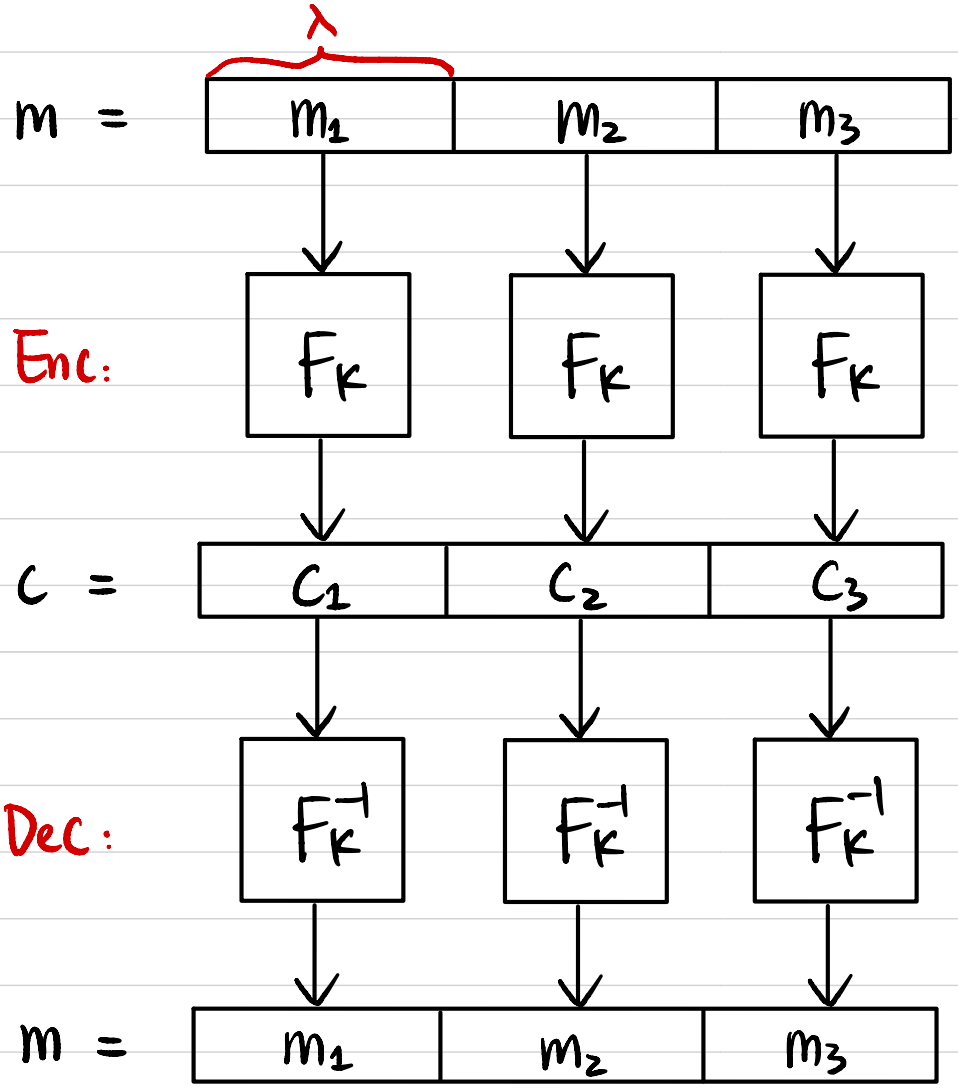


How many possible f's ?

Chosen-Plaintext Attack (CPA) Security

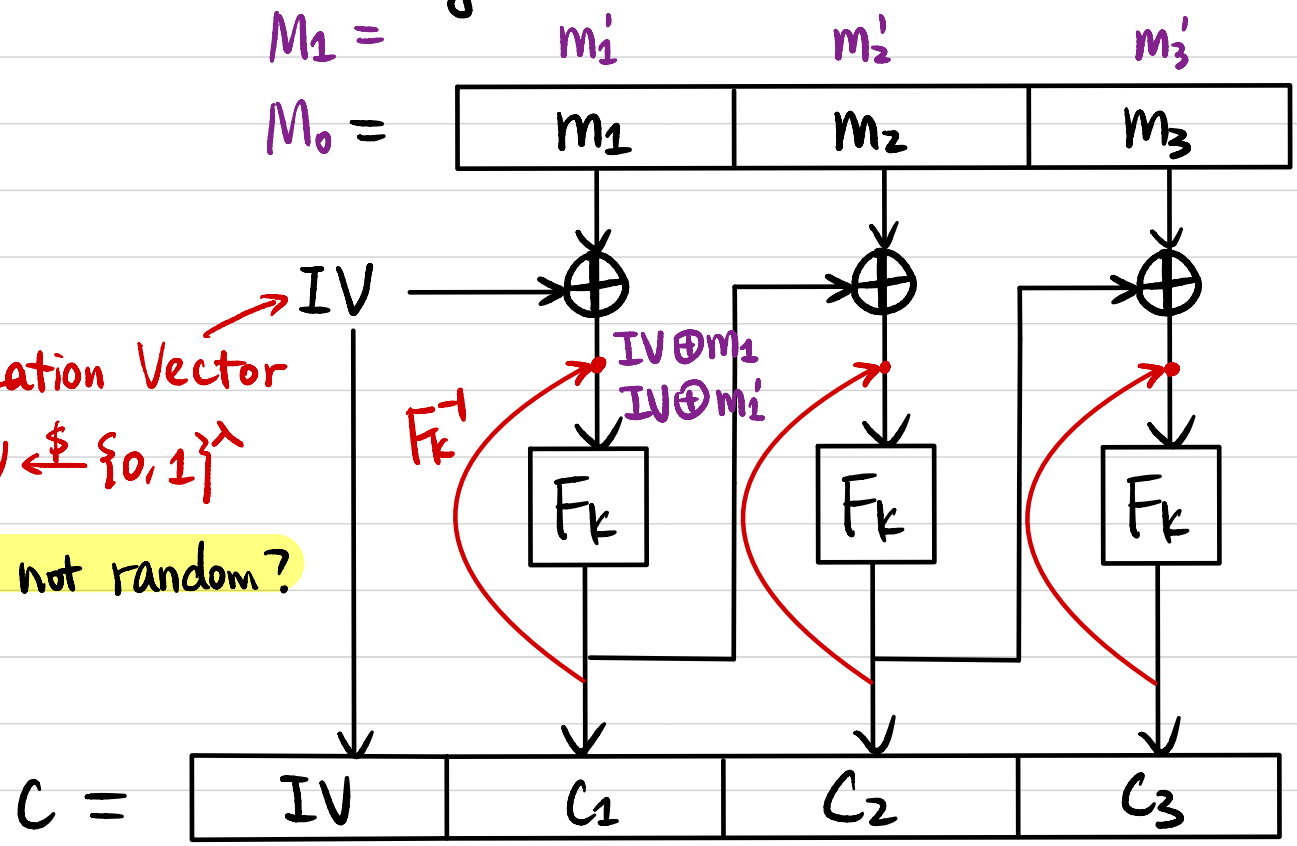


Electronic Code Book (ECB) Mode



CPA Secure? NO!

Cipher Block Chaining (CBC) Mode

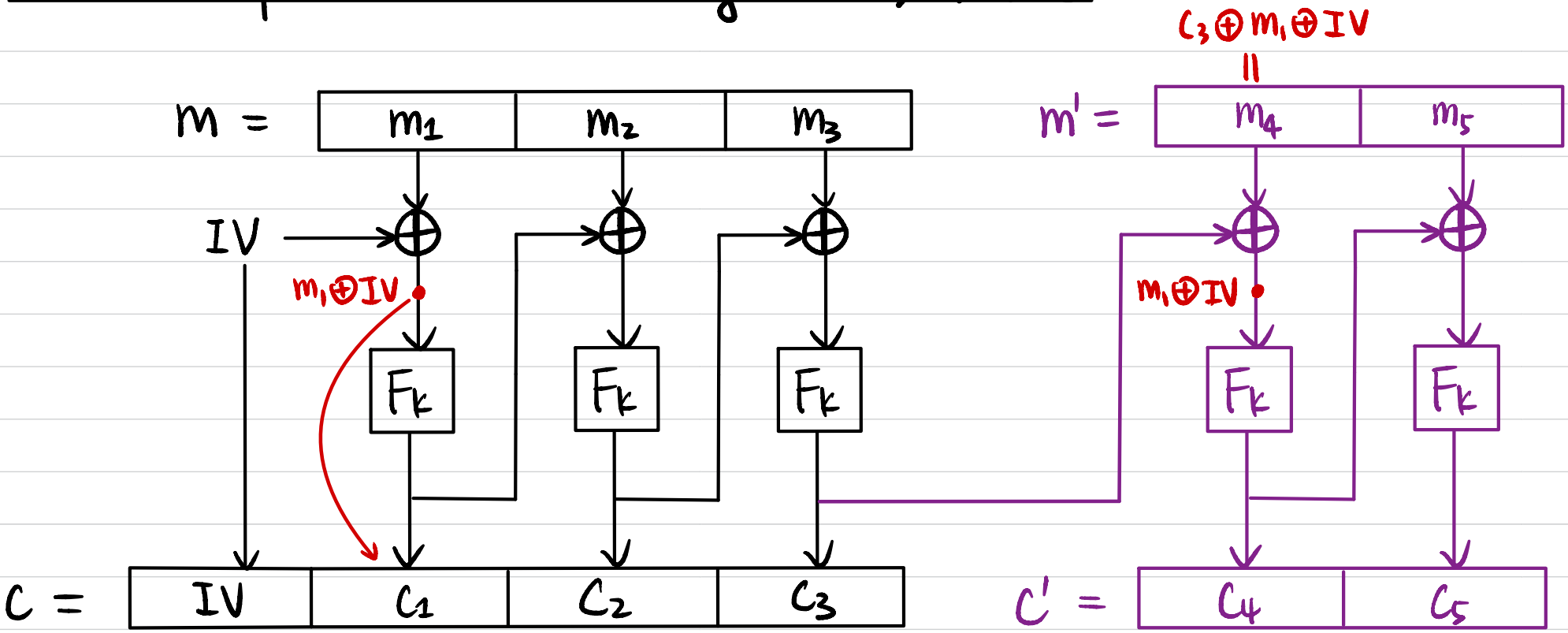


How to decrypt?

CPA secure? YES!

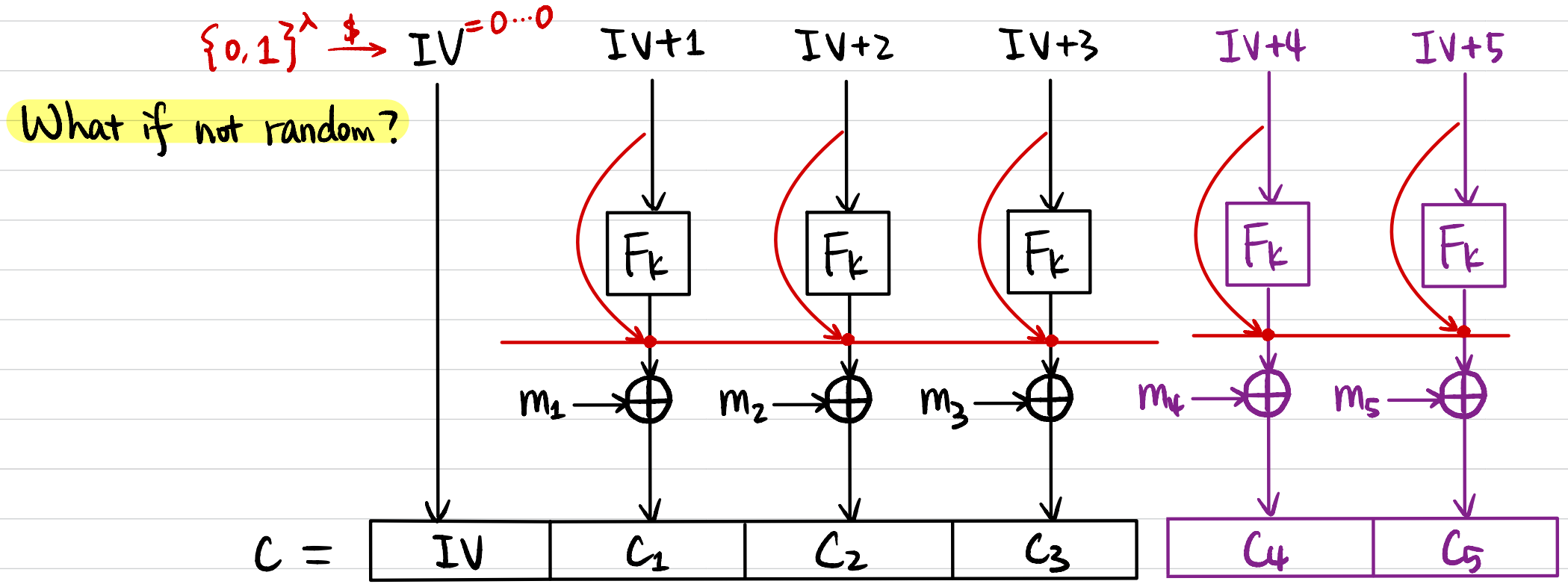
Can we parallelize the computation? NO for Enc
YES for Dec

Chained Cipher Block Chaining (CBC) Mode



CPA secure? No!

Counter (CTR) Mode



What if not random?

How to decrypt?

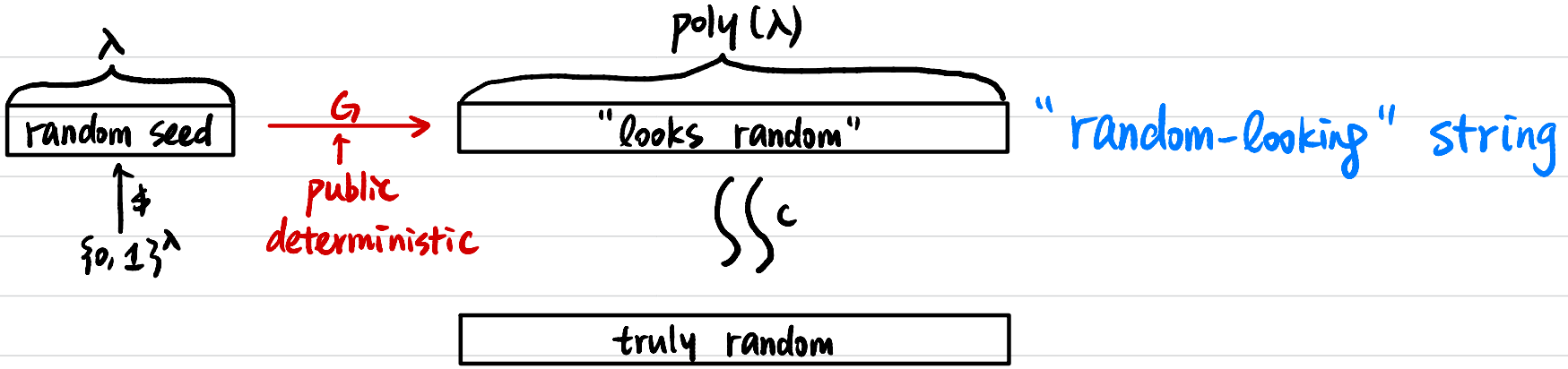
CPA secure? YES!

"Stateful" CTR Mode? YES!

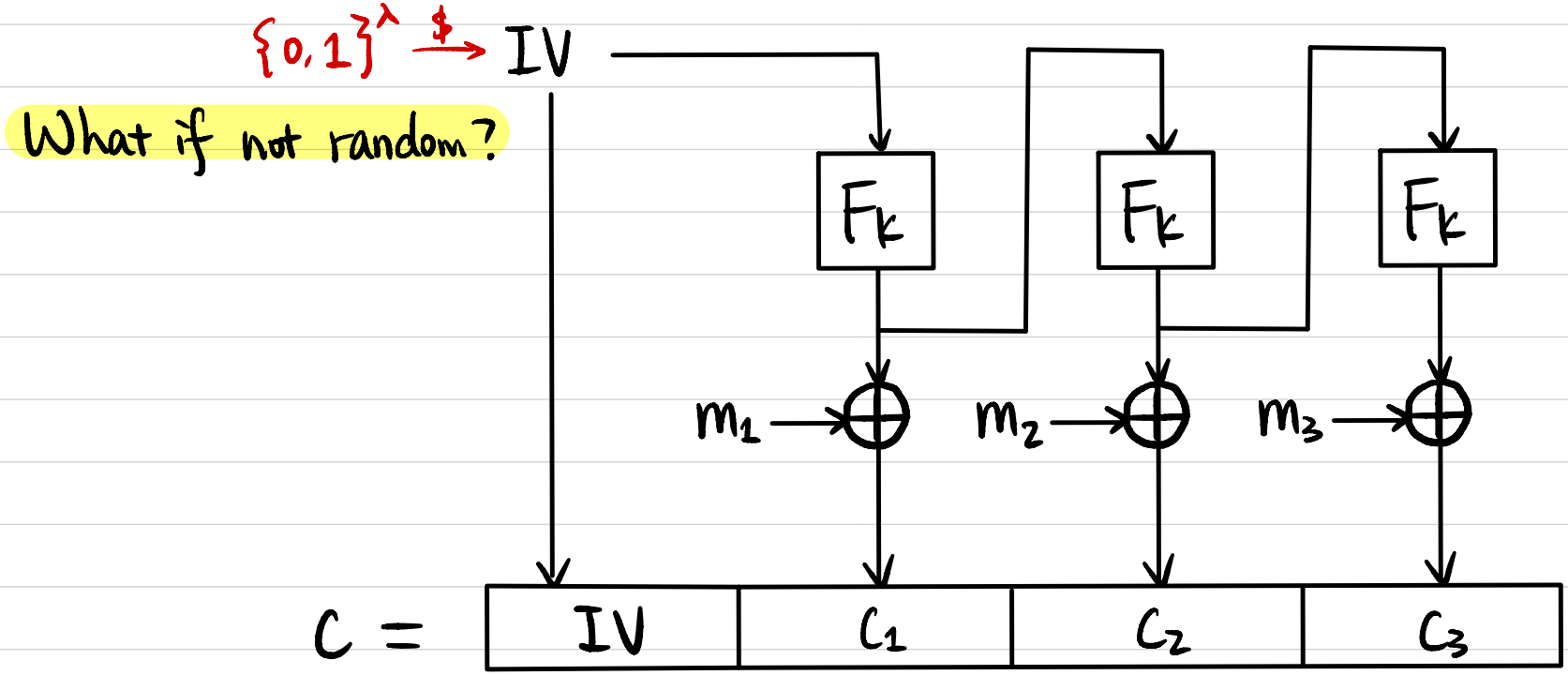
Can we parallelize the computation? YES!

PRG from PRF

Pseudorandom Generator (PRG)



Output Feedback (OFB) Mode



How to decrypt?

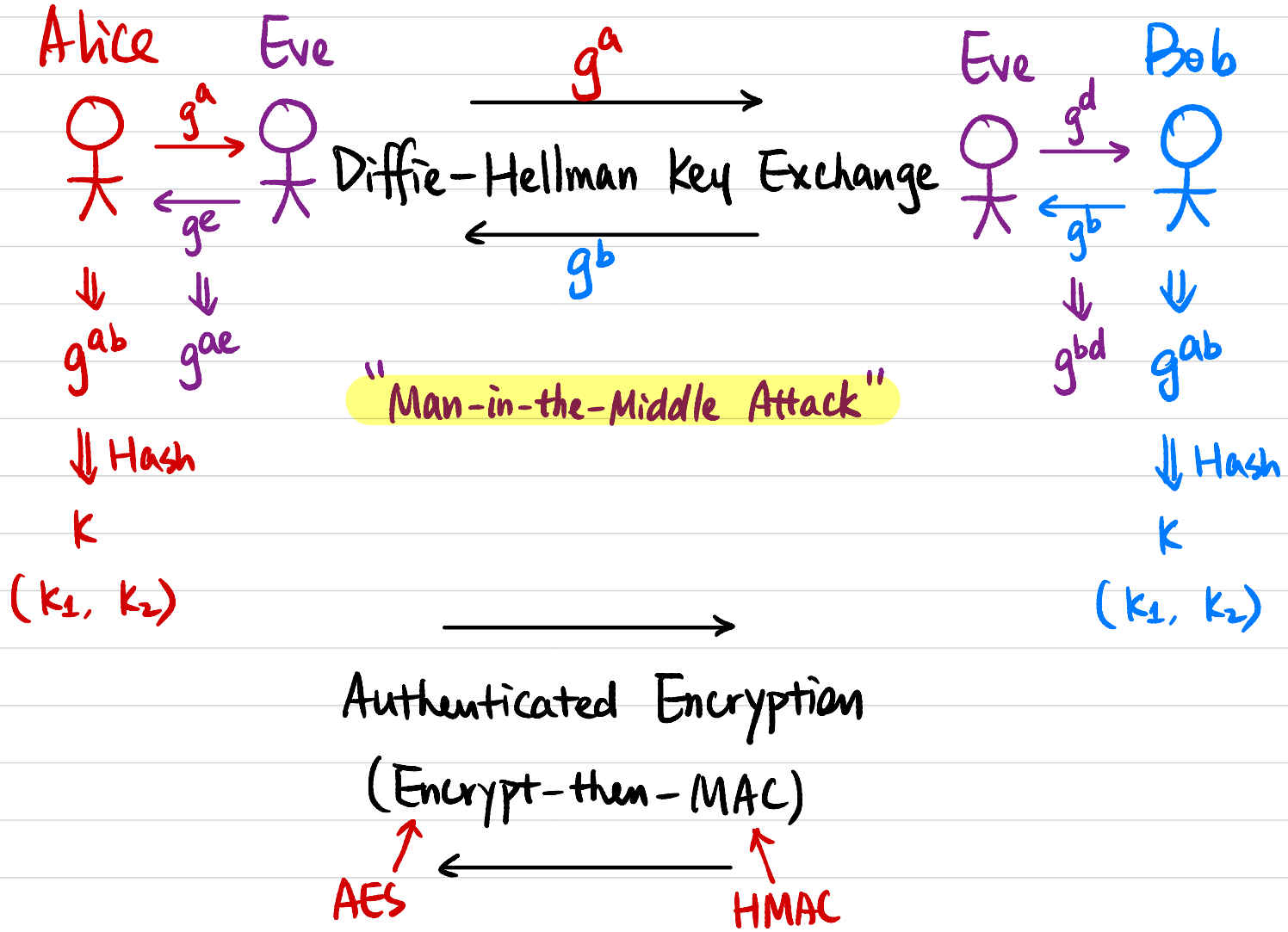
CPA secure?

"Stateful" OFB Mode?

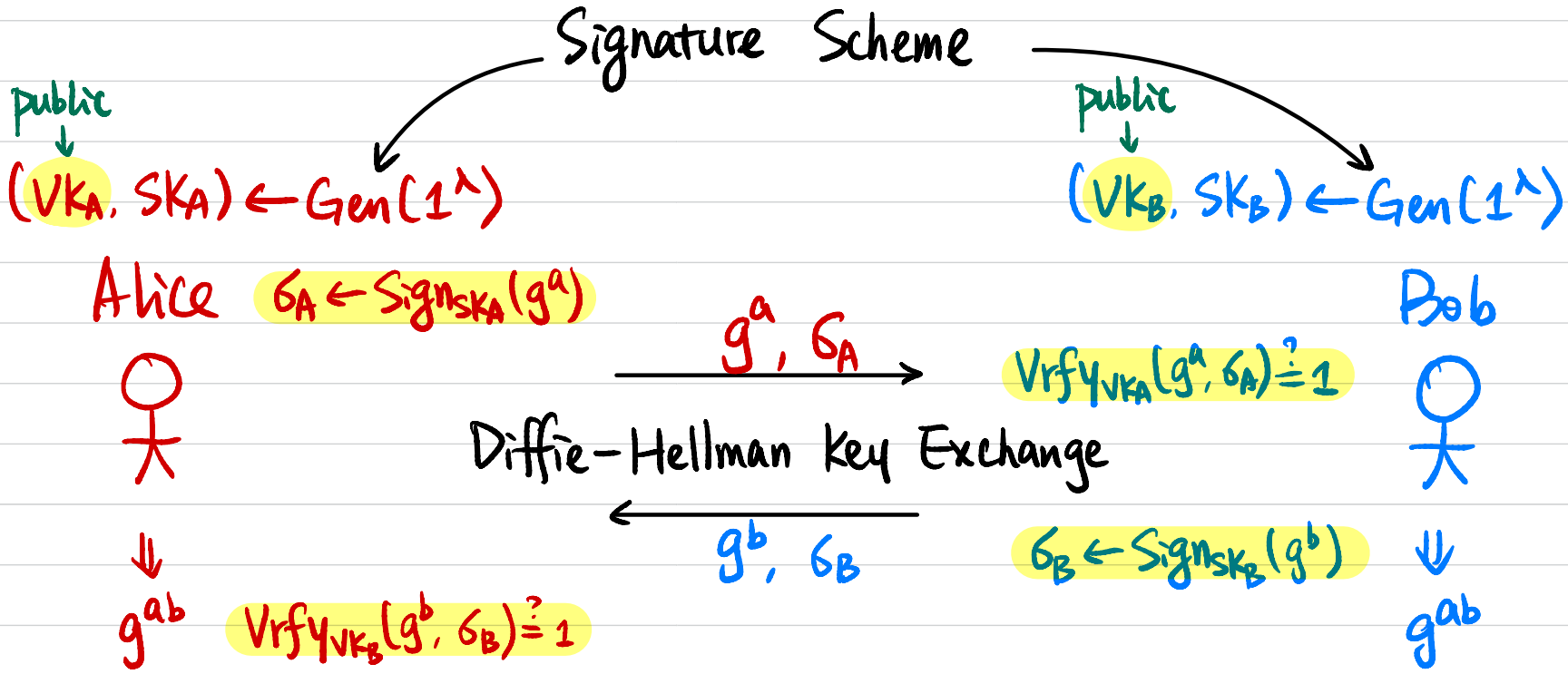
Can we parallelize the computation?

PRG from PRF

Putting it All Together: Secure Communication



Authenticated Key Exchange

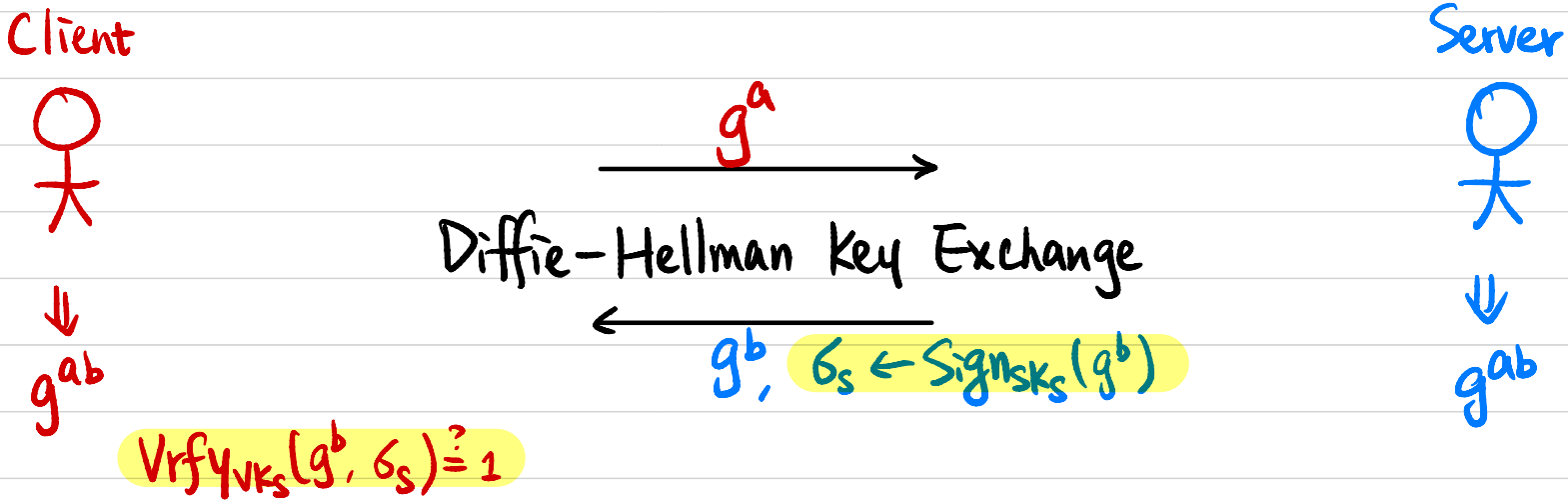


Can we prevent Man-in-the-Middle Attack ?

One-Sided Secure Authentication

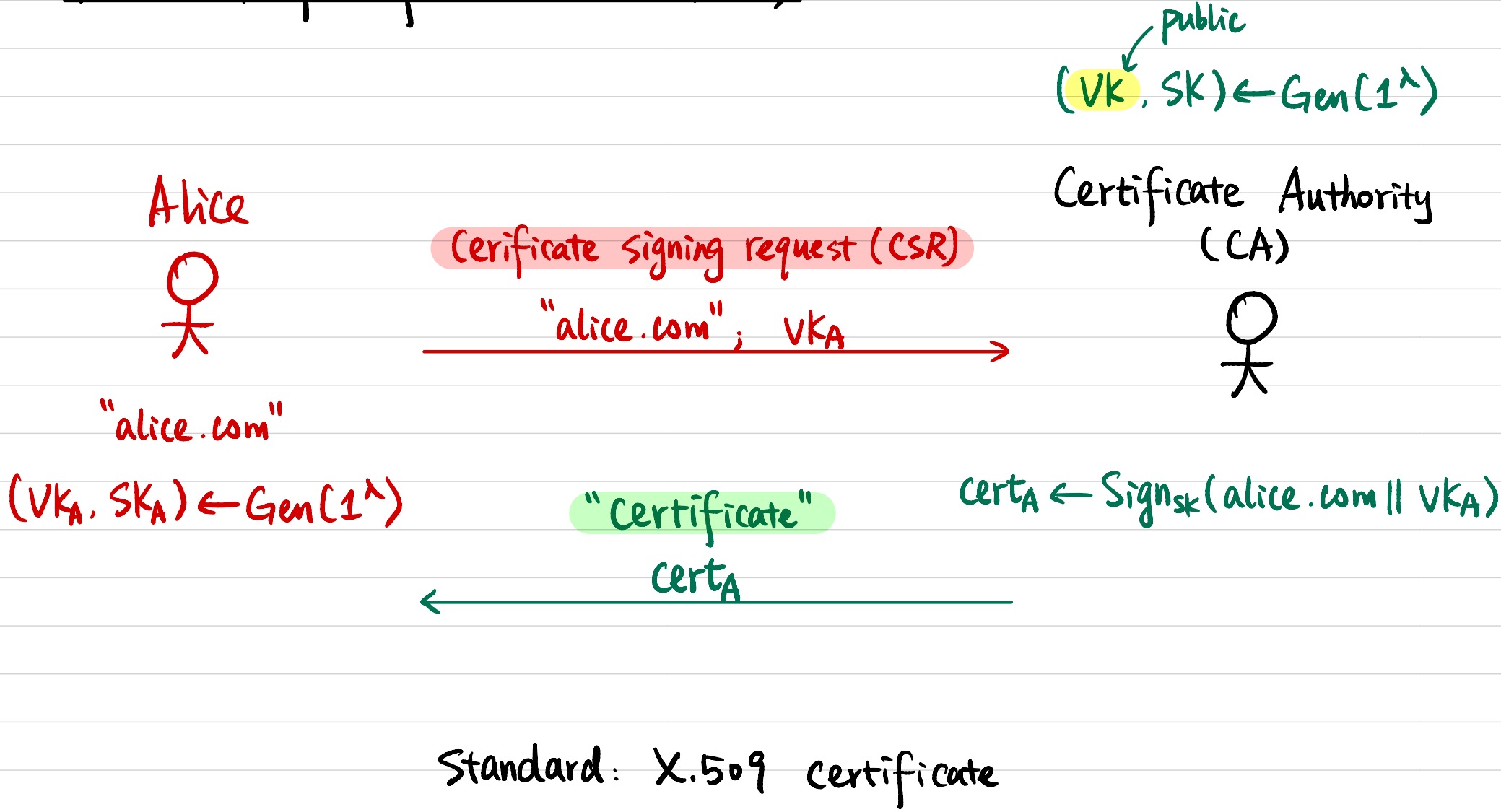
public — Where does it come from?

$(vk_S, sk_S) \leftarrow Gen(1^\lambda)$



Can we prevent Man-in-the-Middle Attack?

Public Key Infrastructure (PKI)



Standard: X.509 certificate

Public Key Infrastructure (PKI)