CS 442
Introduction to Cryptography

Lecture 13: CPA Secure Encryption

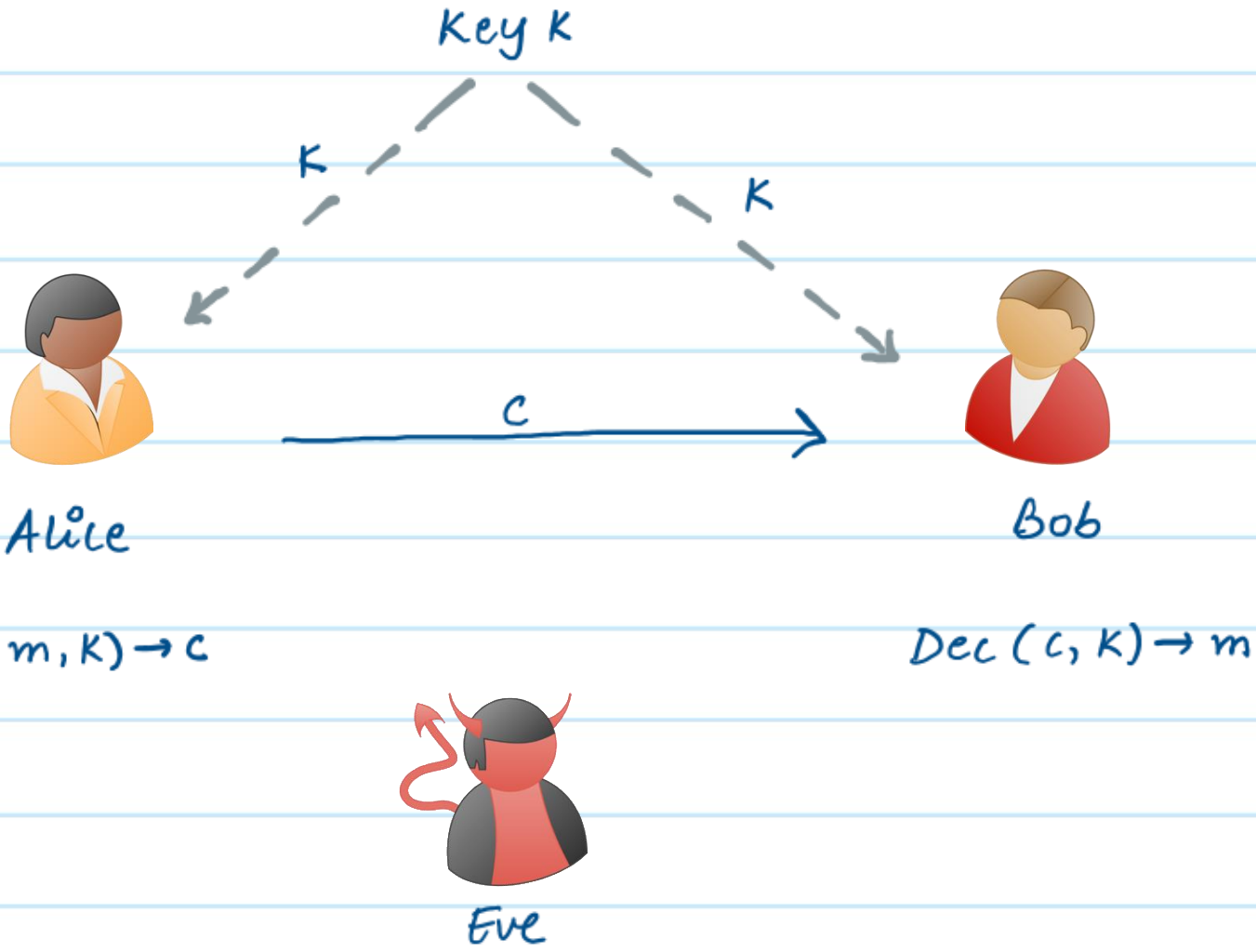
Instructor: Aarushi Goel

Spring 2026

Agenda

* Midterm Solutions
* Defining CPA-Secure Encryption
* CPA-Secure encryption scheme from PRFs.

Ciphertext Only Attack



Ciphertext Only Attack

* Eve can evesdrop on the ciphertext that Alice sends to Bob and tries to deduce information about the underlying message.
* This type of attack is called *ciphertext Only Attack*.
* In the encryption schemes that we have seen so far, the goal was to defend against such attacks.
* In other words:

  In the encryption schemes that we have discussed so far, the goal was to ensure that this ciphertext does not reveal any more information about the message, that Eve did not already have prior to seeing this ciphertext.

Ciphertext Only Attack (COA)

Definition: A COA-secure encryption scheme with message space $\mathcal{M}$, key space $\mathcal{K}$, ciphertext space $\mathcal{C}$, comprises of the following algorithms:

* $\text{KeyGen} \longrightarrow K$: This algorithm samples a key $K \in \mathcal{K}$.
* $\text{Enc}(K, m) \rightarrow c$: On input a key $K \in \mathcal{K}$ and a message $m \in \mathcal{M}$, it outputs ciphertext $c \in \mathcal{C}$.
* $\text{Dec}(K, c) \rightarrow m$: On input a key $K \in \mathcal{K}$ and a ciphertext $c \in \mathcal{C}$, it outputs message $m \in \mathcal{M}$.

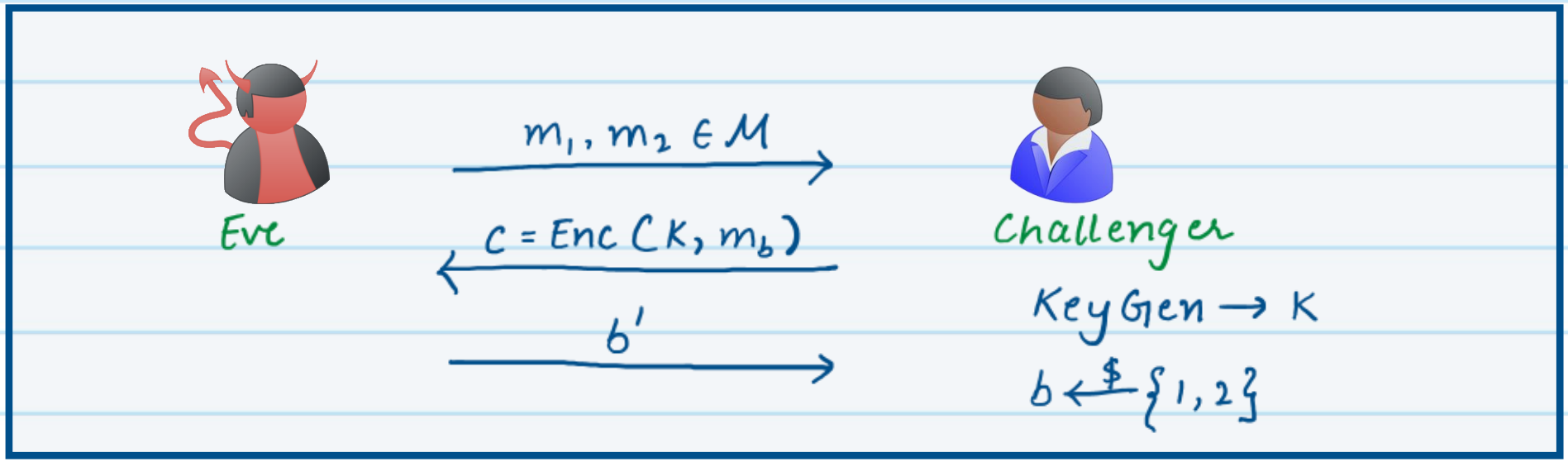
These algorithms must satisfy the following:

→ **Correctness:** $\forall K \in \mathcal{K}$, $\forall m \in \mathcal{M}$, it holds that:

$$Pr[\text{Dec}(K, \text{Enc}(K, m)) = m] = 1$$

→ **COA-Security:** For every PPT Eve, $\exists$ a negligible function $\nu(.)$, such that the following holds in the game below:

$$Pr[b = b'] \leq \frac{1}{2} + \nu(|K|)$$


Eve
$m_1, m_2 \in \mathcal{M}$
$c = Enc(K, m_b)$
b'
Challenger
KeyGen → K
$b \xleftarrow{\$} \{1, 2\}$

Encrypting Multiple Messages

* Now, we will shift focus on encryption schemes where the same key can be used to encrypt multiple messages.
* This means that Eve will have an opportunity to see multiple ciphertexts computed using the same key.
* This could potentially give Eve more help in deducing information about the underlying messages.
* Such attacks are called *chosen plaintext attacks*
* Our goal will now be to prevent against such attacks.

Chosen Plaintext Attack Security (CPA Security)

* We want to design encryption schemes where even if an eavesdropper sees multiple ciphertexts computed using the same key, they should not learn any more information about the underlying messages than they already had prior to seeing these ciphertexts

* To formalize this notion of security, we will allow Eve to have some extra power.
* In particular, we will allow Eve to obtain encryptions of polynomially many messages of his choice. After that, we test how much advantage Eve has in gaining more information about a message encrypted under a new ciphertext.

CPA Secure Encryption (Also called multi-message secure encryption)

Definition: A CPA-secure encryption scheme with message space $\mathcal{M}$, key space $\mathcal{K}$, ciphertext space $\mathcal{C}$, comprises of the following algorithms:

* $\text{KeyGen} \longrightarrow K$: This algorithm samples a key $K \in \mathcal{K}$.
* $\text{Enc}(K, m) \rightarrow c$: On input a key $K \in \mathcal{K}$ and a message $m \in \mathcal{M}$, it outputs ciphertext $c \in \mathcal{C}$.
* $\text{Dec}(K, c) \rightarrow m$: On input a key $K \in \mathcal{K}$ and a ciphertext $c \in \mathcal{C}$, it outputs message $m \in \mathcal{M}$.

These algorithms must satisfy the following:

→ Correctness: $\forall K \in \mathcal{K}$, $\forall m \in \mathcal{M}$, it holds that:

$$Pr[\text{Dec}(K, \text{Enc}(K, m)) = m] = 1$$

→ CPA-Security: For all PPT adversaries, there exists a negligible function $\nu(\cdot)$ such that the following holds in the game below:

$$Pr[b = b'] \leq \frac{1}{2} + \nu(|K|)$$

Adversary

Challenger

KeyGen → K

query polynomial no. of times { $m \rightarrow$, $\leftarrow c$ } Enc(K, .)

can include previously queried messages

$m_0, m_1 \in \mathcal{M}$ →

$\leftarrow c_b = Enc(K, m_b)$

$b \xleftarrow{\$} \{0,1\}$

query polynomial no. of times { $m \rightarrow$, $\leftarrow c$ } Enc(K, .)

$b' \rightarrow$

Necessity of Randomized Encryption

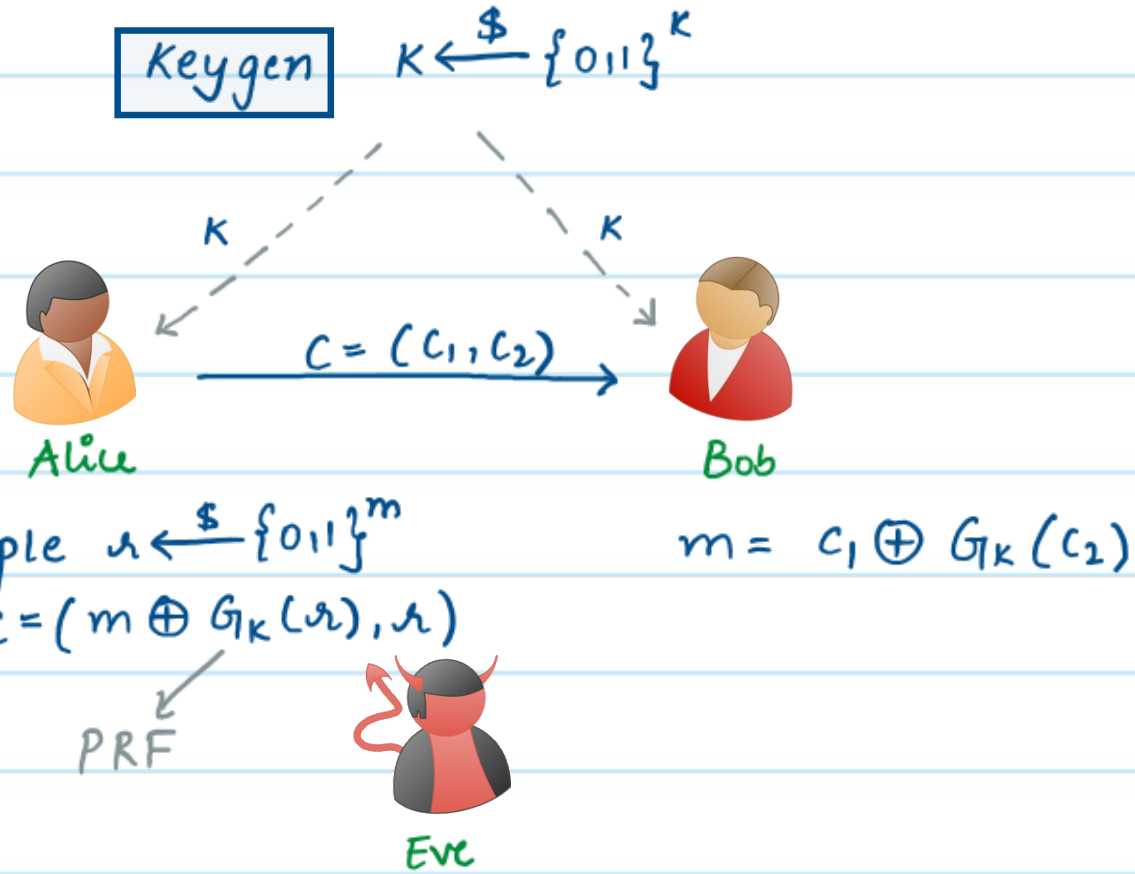
A CPA-secure (or multi-message secure) encryption cannot be deterministic

* In other words, the Enc algorithm must be a randomised algorithm or equivalently, it must take an additional random value as input.

Why??

* If the encryption algorithm is deterministic, then given a key, there will be a unique ciphertext corresponding to each message.
* A PPT adversary in this case will easily be able to win in the game we just discussed.

CPA Secure Encryption from PRFs



Think: why is this CPA-Secure?