CS 442
Introduction to Cryptography

Lecture 4: Perfect Secrecy

Instructor: Aarushi Goel

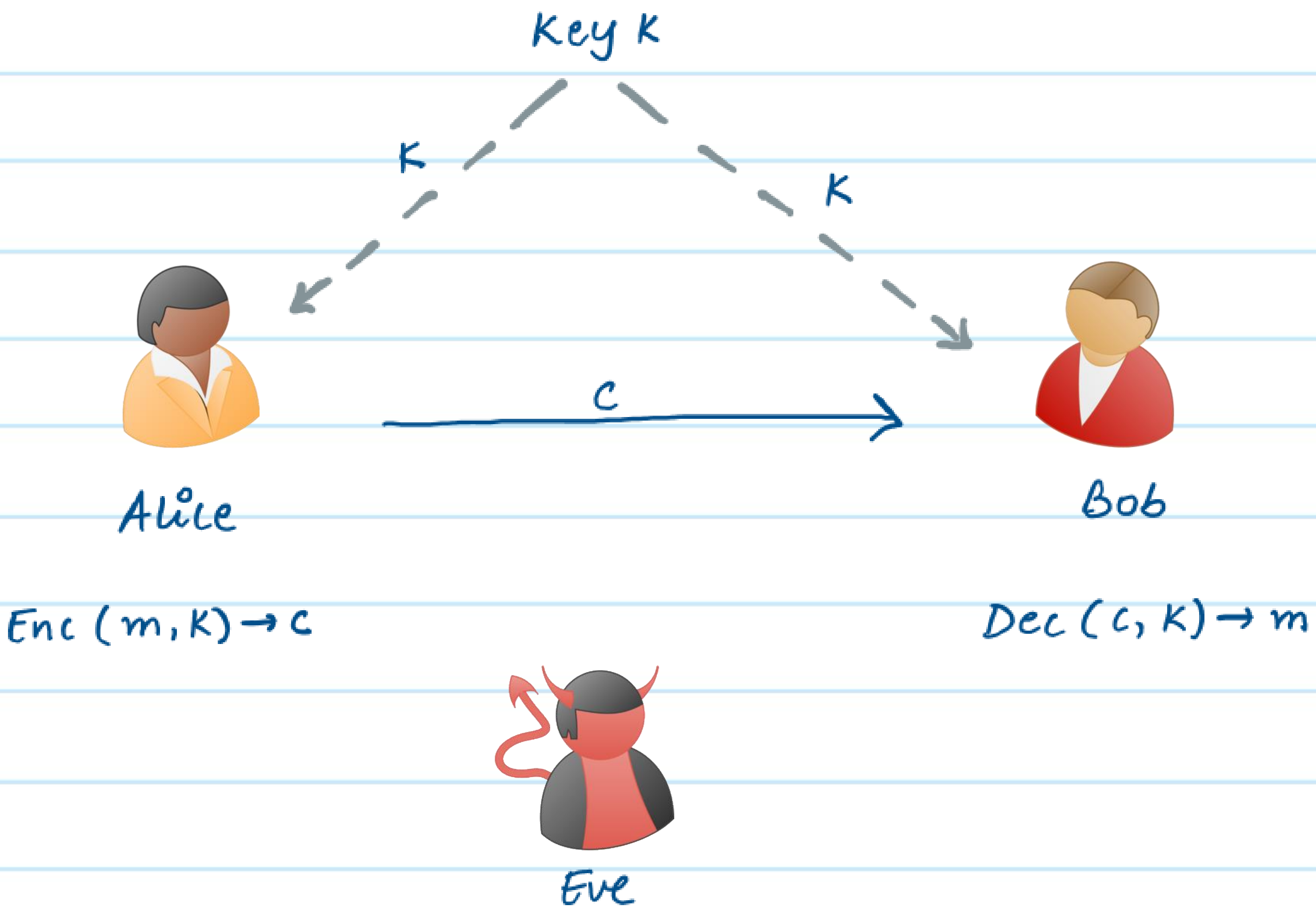
Spring 2026

Agenda

- → Defining perfectly secure encryption.
- → Examples of perfectly secure & insecure encryption schemes
- → Limitations of perfectly secure encryption

HW1 will be released today. Due on Feb 7.

Perfectly Secure Encryption



Perfectly Secure Encryption

→ **Correctness:**

* Alice and Bob share a common Key.
* Alice chooses a message, encrypts it using the Key and sends the resulting ciphertext to Bob.
* Bob should be able to use the Key to decrypt the ciphertext received from Alice to recover the message.

→ Key Generation

→ Encryption

→ Decryption

Perfectly Secure Encryption

→ **Secrecy:**

What does Eve Know?

* Eve Knows which encryption algorithm is being used. → Kerckhoff's Principle

* Eve Knows the probability distribution over messages

→ this is a pessimistic choice. If we can design an encryption scheme that is secure even when Eve Knows the probability distribution over messages, it will also remain secure in realistic scenarios where it may only have partial information about the messages

What do we want?

* After observing one ciphertext from Alice to Bob, Eve should not learn any more information about the encrypted message.

→ We are only aiming for 'one-time" security for now.

Perfectly Secure Encryption

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

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

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

→ Perfect Secrecy: If for every probability distribution over $\mathcal{M}$, $\forall m \in \mathcal{M}$, and $\forall c \in \mathcal{C}$ for which $\Pr[C = c] > 0$, it holds that:

$$\Pr[M = m \mid C = c] = \Pr[M = m]$$

Other Equivalent Formulations for Perfect Secrecy

$\Rightarrow \forall m \in \mathcal{M}, c \in \mathcal{C}, \quad Pr[M=m \mid C=c] = Pr[M=m]$

$\Rightarrow \forall m \in \mathcal{M}, c \in \mathcal{C}, \quad Pr[C=c \mid M=m] = Pr[C=c]$

$\Rightarrow \forall m \in \mathcal{M}, c \in \mathcal{C}, \quad Pr[C=c \cap M=m] = Pr[C=c] \times Pr[M=m]$

$\Rightarrow \forall m_1, m_2 \in \mathcal{M}, c \in \mathcal{C}, \quad Pr[C=c \mid M=m_1] = Pr[C=c \mid M=m_2]$

To prove that an encryption is perfectly secure, it suffices to prove any of these

Another Example of a Perfectly Secure Encryption

* Consider the following encryption scheme over the group $(\mathbb{Z}_{26}, + \bmod 26)$.

KeyGen : $K \xleftarrow{\$} \mathbb{Z}_{26}$

Enc$(K, m \in \mathbb{Z}_{26})$: $ct = (m + K) \bmod 26$

Dec(K, ct) : $m = (ct + (-K)) \bmod 26$

Q Prove that this is a perfectly secure encryption scheme

1 To prove correctness, show that $\forall K \in \mathbb{Z}_{26}, \forall m \in \mathbb{Z}_{26}$,

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

2. To prove security, show that $\forall m \in \mathbb{Z}_{26}, ct \in \mathbb{Z}_{26}$

$$\Pr[M = m \mid C = ct] = \Pr[M = m]$$

1 To prove correctness, show that $\forall K \in \mathbb{Z}_{26}$, $\forall m \in \mathbb{Z}_{26}$,

$$Pr[Dec(K, Enc(K, m)) = m] = 1$$

Proof:

$$Dec(K, Enc(K, m))$$
$$= Dec(K, (m + K) \bmod 26)$$
$$= (((m + K) \bmod 26) - K) \bmod 26$$
$$= m.$$

$$\therefore \quad Pr[Dec(K, Enc(K, m) = m] = 1$$

2. To prove security, show that $\forall\, m \in \mathbb{Z}_{26},\ ct \in \mathbb{Z}_{26}$

$$\Pr[M = m \mid C = ct] = \Pr[M = m]$$

Proof : $\Pr[M = m \mid C = ct] = \dfrac{\Pr[(M=m) \cap (C=ct)]}{\Pr[C = ct]}$

$$= \frac{\Pr[C = ct \mid M = m] \times \Pr[M = m]}{\Pr[C = ct]}$$

$\forall\, m \in \mathbb{Z}_{26}$:

$$\Pr[C = ct \mid M = m] = \Pr[\mathrm{Enc}(m, K) = ct]$$
$$= \Pr[(m + K) \bmod 26 = ct]$$
$$= \Pr[K = ct + (-K) \bmod 26]$$
$$= 1/26$$

$$= \sum_{m' \in \mathbb{Z}_{26}} \Pr[C = ct \mid M = m'] \times \Pr[M = m']$$

$$= \frac{1}{26} \times \sum_{m' \in \mathbb{Z}_{26}} \Pr[M = m'] = \frac{1}{26}$$

$$\therefore\ \Pr[M = m \mid C = ct] = \frac{1/26 \times \Pr[M = m]}{1/26} = \Pr[M = m]$$

Example of Insecure Encryption

Q Show that the following is not a perfectly secure encryption scheme.

* KeyGen : $K \xleftarrow{\$} \{0,1\}^n$

bit-wise AND

* Enc $(K, m \in \{0,1\}^n)$: $C = m \wedge K$

A 1) For some keys, there is no way to uniquely recover m.

counter example: if $K = 0^n$, the $c = m \wedge 0^n = 0^n$ for all $m \in \{0,1\}^n$.

$\Rightarrow$ correctness does not hold.

2) Also does not achieve perfect secrecy

We will show that $\exists\, m \in \{0,1\}^n$, such that $Pr[C = c \mid M = m] \neq Pr[C = c]$

counter example: Let $m = 0^n$

$$Pr[C = 0^n \mid m = 0^n] = 1 \neq Pr[C = c]$$

Limitations of Perfect Secrecy

If (KeyGen, Enc, Dec) is a perfectly secret encryption scheme with message space $\mathcal{M}$ and key space $\mathcal{K}$, then $|\mathcal{K}| \geq |\mathcal{M}|$.

Proof: We need to show that if $|\mathcal{K}| < |\mathcal{M}|$, then the scheme cannot be perfectly secure.

* Let us assume for the sake of contradiction that $|\mathcal{K}| < |\mathcal{M}|$.
* Let $c \in \mathcal{C}$ be a ciphertext that occurs with non-zero probability.

* Let $\mathcal{M}(c)$ be the set of all possible messages that are possible decryptions of c. i.e., $\mathcal{M}(c) = \{ m \mid \exists k \in \mathcal{K}, \text{ such that } Dec(k, c) = \quad \}$

$$\Rightarrow |\mathcal{M}(c)| \leq |\mathcal{K}|$$

However, if $|\mathcal{K}| < |\mathcal{M}|$, $|\mathcal{M}(c)| \leq |\mathcal{K}| < |\mathcal{M}| \Rightarrow |\mathcal{M}(c)| < |\mathcal{M}|$

$\Rightarrow$ there is some $m' \in \mathcal{M}$, such that $m' \notin \mathcal{M}(c)$.

$$\Pr[C = c \,|\, M = m'] = 0$$

But we know that $\forall\, m^* \in \mathcal{M}(c)$, $\Pr[C = c \,|\, M = m^*] \neq 0$

$\Rightarrow$ $\exists\, m', m^* \in \mathcal{M}$, $\exists\, c \in \mathcal{C}$, such that

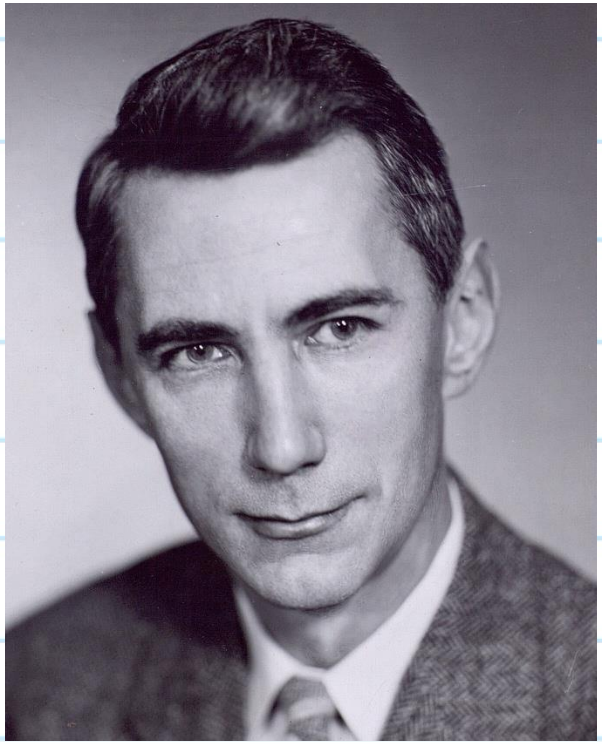
$$\Pr[C = c \,|\, M = m'] \neq \Pr[C = c \,|\, M = m^*]$$

$\Rightarrow$ The scheme is not perfectly secure.

$\therefore$ Our assumption is wrong, a perfectly secure encryption scheme must be such that $|\mathcal{K}| \geq |\mathcal{M}|$.

Shannon's Theorem

* Shannon provided a characterization of perfectly secure encryption schemes.



Claude Shannon

Theorem: Let (KeyGen, Enc, Dec) be an encryption scheme, where $|\mathcal{M}| = |\mathcal{C}| = |\mathcal{K}|$. This scheme is perfectly secure if and only if:

1. Every key $k \in \mathcal{K}$ is chosen with (equal) probability $1/|\mathcal{K}|$ by algorithm KeyGen.
2. For every $m \in \mathcal{M}$ and every $c \in \mathcal{C}$, $\exists$ a unique key $k \in \mathcal{K}$ such that $\text{Enc}(k, m) = c$.