CS 442
Introduction to Cryptography

Lecture 5: Perfect Secrecy - II

Instructor: Aarushi Goel

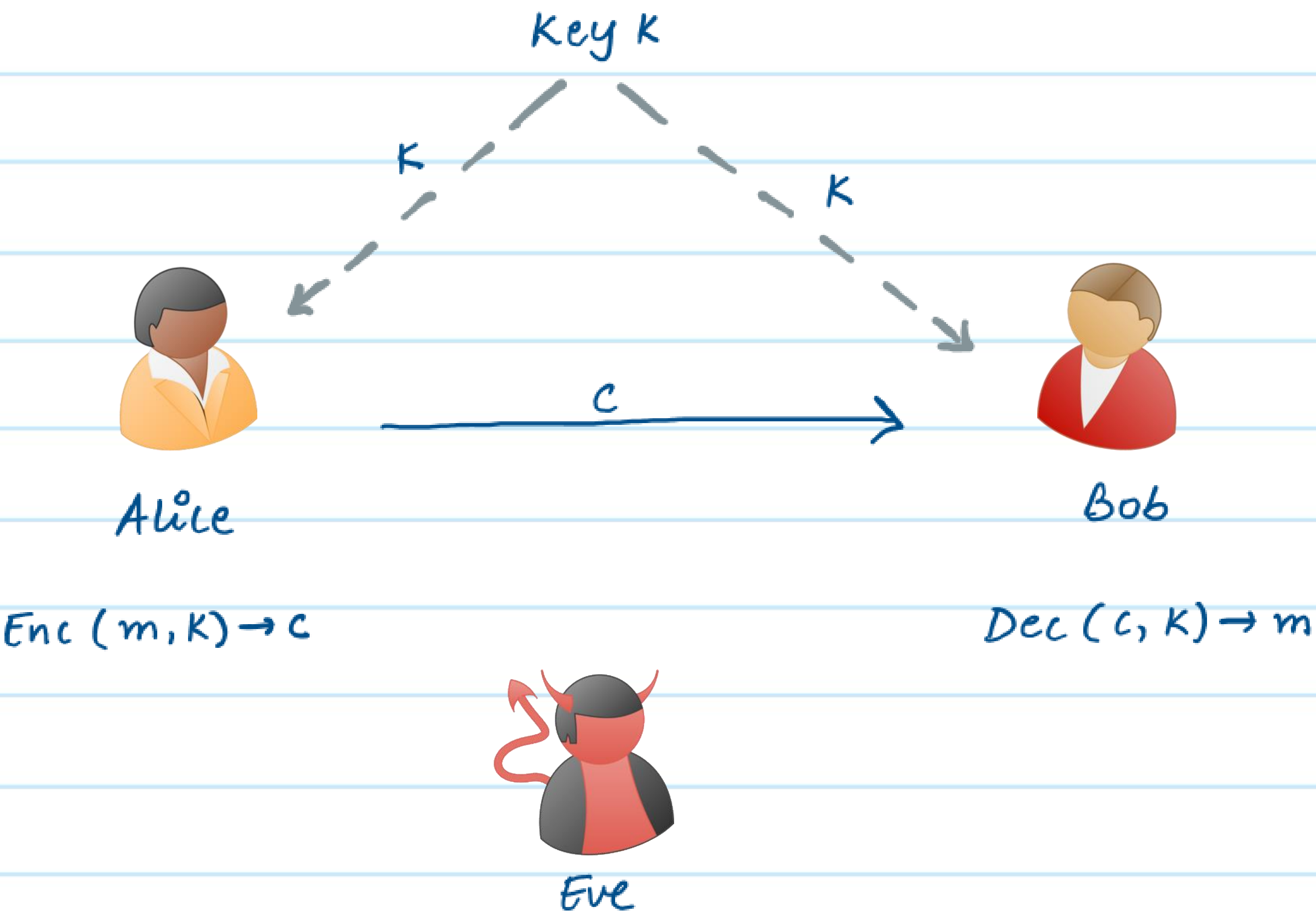
Spring 2026

Agenda

* Proof of Shannon's Theorem.
* Game-based definition of Perfect secrecy
* Computational Security.

- HW1 is due on Feb 7.
- Midterm will be in class on Mar 5

Perfectly Secure Encryption



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:

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

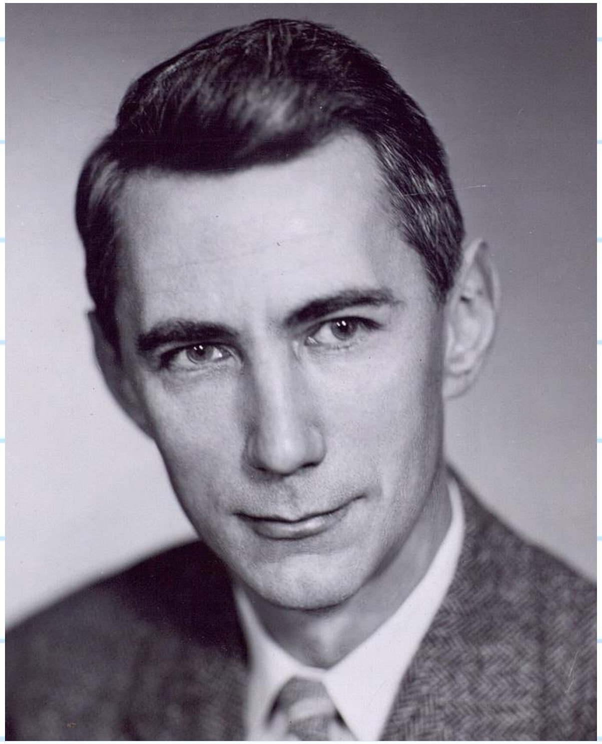
$$\Pr[\mathrm{Dec}(K, \mathrm{Enc}(K, m)) = m] = 1$$

→ 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:

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

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 $\mathrm{Enc}(k, m) = c$.

Proof of Shannon's Theory

when $|M| = |K| = |C|$. perfect secrecy $\Longrightarrow$ conditions 1 and 2.

Condition 2:

Let's assume for the sake of contradiction that $\exists i \in |\mathcal{M}|, \exists k_{i,1}, k_{i,2} \in \mathcal{K}$ such that $Enc(k_{i,1}, m_i) = Enc(k_{i,2}, m_i) = ct^*$

- But we also know that if a scheme is perfectly secure, then $\forall m_i, m_j \in \mathcal{M}$ & $ct \in C$, $Pr[C = ct \mid M = m_i] = Pr[C = ct \mid M = m_j]$
- Since the decryption algorithm is deterministic, $\exists k_j \neq k_{i,1} \neq k_{i,2}$ such that $Enc(k_j, m_j) = ct^*$. Infact such a unique key should exist for all $j \neq i$
- This would imply there are $|\mathcal{M}|+1$ keys, which is a contradiction.

$\Rightarrow$ our assumption is incorrect. $\forall m, c, \exists$ a unique key k, such that $Enc(m, k) = c$.

Condition 1:

- We know that $|\mathcal{K}| = |\mathcal{M}|$.
- Since the scheme has perfect secrecy, $\forall\, m_i, m_j \in \mathcal{M}$, it holds that

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

$$\Rightarrow \Pr[\mathrm{Enc}(K, m_i) = c] = \Pr[\mathrm{Enc}(K, m_j) = c]$$

- Also from condition 2, we know that $\exists$ unique $k_i \in \mathcal{K}$, for every $m_i \in \mathcal{M}$, $c \in \mathcal{C}$, such that $\mathrm{Enc}(k_i, m_i) = c$.

$$\Rightarrow \Pr[\mathrm{Enc}(K, m_i) = c] = \Pr[K = k_i]$$

$$= \Pr[\mathrm{Enc}(K, m_j) = c] = \Pr[K = k_j]$$

$$\Rightarrow \forall i, j, \quad \Pr[K = k_i] = \Pr[K = k_j]$$

$\Rightarrow$ each key is picked with equal probability $1/|\mathcal{K}|$.

Conditions 1 & 2 $\Rightarrow$ the given scheme has perfect secrecy

Given some $m \in \mathcal{M}$ & $c \in \mathcal{C}$, let $k \in \mathcal{K}$ be the unique key guaranteed from condition 2, such that, $\mathrm{Enc}(k, m) = c$

Then $Pr[C = c \mid M = m] = Pr[K = k]$

from condition 1, we know that $Pr[K = k] = 1/|\mathcal{K}|$

$$\Rightarrow Pr[C = c] = \sum_{m \in \mathcal{M}} Pr[C = c \mid M = m] \cdot Pr[M = m] = \sum_{m \in \mathcal{M}} Pr[K = k] \cdot Pr[M = m]$$

$$= Pr[K = k] \cdot \sum_{m \in \mathcal{M}} Pr[M = m]$$

$$= 1/|\mathcal{K}| \cdot 1.$$

$$\Rightarrow Pr[C = c \mid M = m] = Pr[C = c] = 1/|\mathcal{K}|$$

Alternate Way of Thinking About Perfect Secrecy
(Game-based definition)

* Recall that for perfect secrecy, we want $\forall m_1, m_2 \in \mathcal{M}$ & $\forall c \in \mathcal{C}$,

$$\Pr[C=c \mid M=m_1] = \Pr[C=c \mid M=m_2]$$

* This can be modeled as an interactive game between Eve & a challenger

Since the above equation must hold for $\forall m_1, m_2$ we can let Eve choose a pair of messages

Eve

$$\xrightarrow{m_1, m_2 \in \mathcal{M}}$$

Challenger

$$\xleftarrow{c = \mathrm{Enc}(K, m_b)}$$

$\mathrm{KeyGen} \rightarrow K$

$b \xleftarrow{\$} \{1, 2\}$

$$\xrightarrow{b'}$$

Eve guesses which message was encrypted

* Eve wins the game if $b' = b$
* For perfect secrecy we want Eve's advantage in correctly guessing b after seeing the ciphertext to be as much as its advantage in guessing without looking at the ciphertext.
* Eve's best strategy to correctly predict b without looking at the ciphertext is to randomly guess b.

$$\Rightarrow \Pr[b = b'] = 1/2$$

This gives us another definition of perfect secrecy.

Game-based Definition of perfect Secrecy

Definition: An encryption scheme (KeyGen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secure if it satisfies correctness (as defined previously) and if for *every* Eve, the following holds in the game below.

$$\Pr[b = b'] = 1/2$$

Eve

$\xrightarrow{m_1, m_2 \in \mathcal{M}}$

$\xleftarrow{c = \mathrm{Enc}(K, m_b)}$

$\xrightarrow{b'}$

Challenger

$\mathrm{KeyGen} \rightarrow K$

$b \xleftarrow{\$} \{1, 2\}$

Relaxing Security Requirements

What if the ciphertext is not exactly independent of the message?

Next Best Thing:

The distribution of ciphertexts is close to a distribution that is independent of the message.

Statistical Closeness

Computational Closeness

Computational Security vs Perfect Security

* For perfect secrecy, we want security against *every* Eve/Adversary.
* However, this may be an overkill.
* As we discussed earlier, there are also limitations of perfectly secure encryption schemes.
* In practice, it might be sufficient to security against computationally feasible attacks as opposed to all possible attacks

John Nash

"It doesn't really matter whether attacks are impossible, only whether attacks are computationally infeasible"

* Modern cryptography is based on this principle *

Cost of Computation

It can be helpful to think of cost of computation or the cost of attack in terms of monetary value. Following costs are approximated using the pricing model of Amazon EC2

clock cycles	approx cost	reference
2^{50}	\$3.50	cup of coffee
2^{55}	\$100	decent tickets to a Portland Trailblazers game
2^{65}	\$130,000	median home price in Oshkosh, WI
2^{75}	\$130 million	budget of one of the Harry Potter movies
2^{85}	\$140 billion	GDP of Hungary
2^{92}	\$20 trillion	GDP of the United States
2^{99}	\$2 quadrillion	all of human economic activity since 300,000 BC[4]
2^{128}	really a lot	a billion human civilizations' worth of effort

Basic Group Theory

Recall the definition of groups.

Definition: A group, represented by $(G, \circ)$, is defined by a set G and a binary operator $\circ$ that satisfies the following properties:

* **Closure:** $\forall\ a, b \in G$, we have $a \circ b \in G$
* **Associativity:** $\forall\ a, b, c \in G$, we have $(a \circ b) \circ c = a \circ (b \circ c)$
* **Identity:** $\exists$ an element $e \in G$, such that $\forall\ a \in G$, we have $a \circ e = a$
* **Inverse:** $\forall$ elements $a \in G$, $\exists$ an element $(-a) \in G$, such that $a \circ (-a) = e$

Basic Group Theory

* Group exponentiation: For a group $(G, \cdot)$. and group elements $g, h \in G$

$$g^m = \overbrace{g \cdot g \cdots g}^{m}, \quad g^0 = e, \quad g^{-m} = (g^{-1})^m$$

$$g^{m_1} \cdot g^{m_2} = g^{m_1 + m_2}, \quad (g^{m_1})^{m_2} = g^{m_1 \cdot m_2}, \quad g^m \cdot h^m = (g \cdot h)^m$$

* For a finite group, we use $|G|$ to denote its order (# of elements)
* Let G be a group of order q.
* G is a cyclic group if $\exists g \in G$, s.t. $\{g^0, g^1, \ldots, g^{q-1}\} = G$.

  g is called the generator of G.