CS 442
Introduction to Cryptography

Lecture 3: Groups/Fields and One-Time Pads

Instructor: Aarushi Goel

Spring 2026

Agenda

* Groups , Fields
* One-time Pad
* Perfect Secrecy

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 $a \circ (-a) = e$

Groups

bit-wise XOR

Verify that $(\{0,1\}^n, \oplus)$ is a group.

* Closure and Associativity is easy to verify
* Show that $\underbrace{00\ldots0}_{n\text{-times}}$ is the identity
* Show that for $a \in \{0,1\}^n$, the inverse of a is a itself.

Groups

* Groups can have infinite size

<u>Example</u>: $(\mathbb{Z},+)$, where $\mathbb{Z}$ is the set of integers and $+$ is integer addition

verify that it satisfies all properties of a group.

* Groups can have finite size

<u>Example</u>: $(\mathbb{Z}_n,+)$, where $\mathbb{Z}_n = \{0, \ldots, n-1\}$ and $+$ is integer addition mod n, is a group.

verify that it satisfies all properties of a group.

Groups

Following are NOT groups. Find which rule is violated.

* $(\mathbb{Z}, \times)$, where $\times$ is integer multiplication

  → does not satisfy inverse

* $(\mathbb{Z}^*, \times)$, where $\mathbb{Z}^*$ is the set of all non-zero integers and $\times$ is integer multiplication

  → still does not satisfy inverse

* $(\mathbb{Q}, \times)$, where $\mathbb{Q}$ is the set of all rationals and $\times$ is rational multiplication

  → No inverse for 0.

But $(\mathbb{Q}^*, \times)$, where $\mathbb{Q}^*$ is the set of all non-zero rationals and $\times$ is rational multiplication, is a group!

Fields

Definition: A field is defined by a set of elements $\mathbb{F}$, and two operators $+$ and $\cdot$. The field $(\mathbb{F}, +, \cdot)$ satisfies the following properties:

* Closure: $\forall\, a, b \in \mathbb{F}$, we have $a+b \in \mathbb{F}$ and $a \cdot b \in \mathbb{F}$
* Commutativity: $\forall\, a, b \in \mathbb{F}$, we have $a+b = b+a$ and $a \cdot b = b \cdot a$
* Associativity: $\forall\, a, b, c \in \mathbb{F}$, we have $(a+b)+c = a+(b+c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
* Additive & Multiplicative Identities: $\exists$ elements $0 \in \mathbb{F}$ and $1 \in \mathbb{F}$ such that $\forall\, a \in \mathbb{F}$, we have $a+0 = a$ and $a \cdot 1 = a$.
* Additive Inverse: $\forall\, a \in \mathbb{F}$, $\exists\, (-a) \in \mathbb{F}$ such that $a + (-a) = 0$
* Multiplicative Inverse: $\forall\, 0 \neq a \in \mathbb{F}$, $\exists\, a^{-1} \in \mathbb{F}$ such that $a \cdot (a^{-1}) = 1$
* Distributivity: $\forall\, a, b, c \in \mathbb{F}$, we have $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$

Fields

* Fields can have finite size

Example: $(\mathbb{Z}_p, +, \times)$ is a field when p is a prime, $+$ is integer addition mod p, $\times$ is integer multiplication mod p.

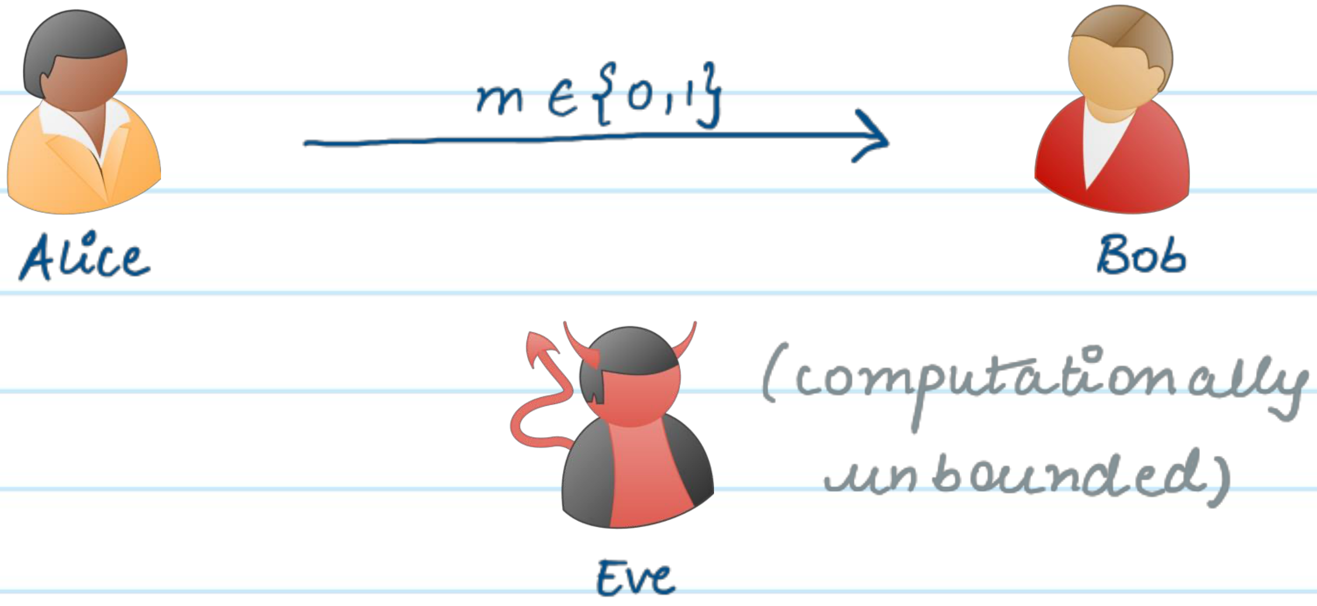
Verify that it satisfies all properties of a field.

* Fields can have infinite size

Example: $(\mathbb{Q}, +, \times)$

Verify that it satisfies all properties of a field

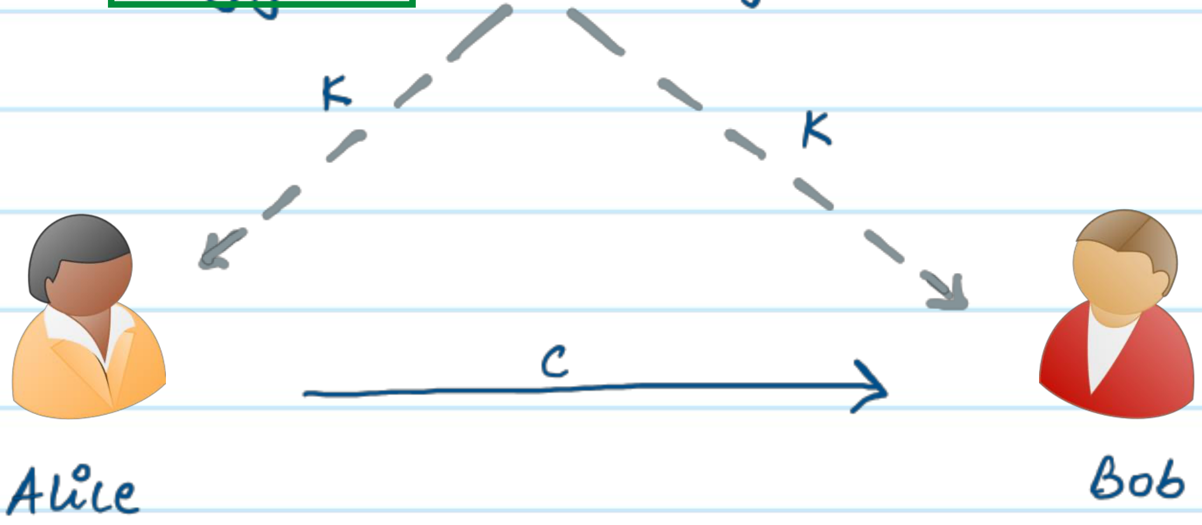
Private Communication



How can Alice send m to Bob, while keeping it hidden from an evesdropper Eve?

One-Time Pad

$\boxed{\text{Keygen:}}$ $K \xleftarrow{\$} \{0,1\}$ randomly sampling



$\text{Enc}(m,K): c = m \oplus K$

$\text{Dec}(c,K): m = c \oplus K$

One-Time Pad

Let $m=0$. What are the possible values of c?

prob	K	$c = m \oplus K$
$1/2$	0	0
$1/2$	1	1

$\Rightarrow$ whatever $\boxed{\text{Eve sees i.e., } c}$ is independent of m

also called the "view" of the adversary

Perfect Secrecy

* Is the message m really secret?

* Eve could have easily guessed m with probability $\frac{1}{2}$

  In fact if they already knew something about m, they can do even better.

  NOTE: we did not claim that m is random

* But Eve could have learnt this without looking at c.

  This means c does not leak any additional information about m.

Perfect Secrecy

Typical goal in Cryptography :

PRESERVE SECRECY !!

Intuitively speaking, this is what we want :

$$\boxed{\text{What Eve learns about } m \text{ after seeing } c \text{, is the same as what they alredy knew about } m.}$$

Formalizing Perfect Secrecy

Setting 1: What did Eve already know about the message?

→ probability distribution over m

→ i.e., $\forall m$, $\Pr[msg = m]$

Setting 2: What does Eve learn after seeing c?

→ New distribution $\Pr[msg = m \mid view = c]$

$$\boxed{\begin{array}{c}\text{What do we want for Secrecy?}\\ \text{Eve's knowledge in Setting 1}\\ =\\ \text{Eve's knowledge in Setting 2}\end{array}}$$

Formalizing Perfect Secrecy

$\Rightarrow$ $\forall m, \forall c, \quad Pr[msg = m \mid view = c] = Pr[msg = m]$

view is independent of msg

$\Rightarrow$ $\forall m, \forall c, \quad Pr[view = c \mid msg = m] = Pr[view = c]$

for all possible values of the msg, the view is identically distributed.

$\Rightarrow$ $\forall c, \forall m_1, m_2, \quad Pr[view = c \mid msg = m_1] = Pr[view = c \mid msg = m_2]$

Formalizing Perfect Secrecy (Summary)

These are equivalent formulations:

$\Rightarrow$ $\forall m, \forall c, \quad Pr[msg = m \mid view = c] = Pr[msg = m]$

$\Rightarrow$ $\forall m, \forall c, \quad Pr[view = c \mid msg = m] = Pr[view = c]$

$\Rightarrow$ $\forall m, \forall c, \quad Pr[msg = m, view = c] = Pr[msg = m] \times Pr[view = c]$

$\Rightarrow$ $\forall c, \forall m_1, m_2, \quad Pr[view = c \mid msg = m_1] = Pr[view = c \mid msg = m_2]$

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

One-time Pad Encryption has perfect Secrecy

To Prove: $\forall\, m \in \{0,1\}, ct \in \{0,1\}$, show that

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

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

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

$\forall\, m \in \{0,1\}$

$$\boxed{\begin{aligned} Pr[C=ct \mid M=m] &= Pr[Enc(m,K)=ct] \\ &= Pr[(m \oplus K)=ct] \\ &= Pr[K = ct \oplus m] \\ &= 1/2 \end{aligned}}$$

$$\boxed{\begin{aligned} &= \sum_{m' \in \{0,1\}} Pr[C=ct \mid M=m'] \times Pr[M=m'] \\ &= \frac{1}{2} \times \sum_{m' \in \{0,1\}} Pr[M=m'] = \frac{1}{2} \end{aligned}}$$

Reflection #1

Is $Pr[msg = m_1 \mid view = v] = Pr[msg = m_2 \mid view = v]$?

why / why not ?

This is only true if the msg is uniformly distributed.

$\Rightarrow$ a good encryption scheme should be perfectly secret for any distribution of messages in the message space.

Reflection #2

In this construction of one-time pad encryption scheme, can we use the same key to encrypt two different msgs?

Why / why Not?

Let $c_1 = m_1 \oplus k$ and $c_2 = m_2 \oplus k$

if Eve sees c_1, c_2, it can compute

$$\underline{m_1 \oplus m_2} = c_1 \oplus c_2$$

this leaks more information about m_1, m_2 than Eve had before seeing c_1, c_2.

⇒ This is an example of a "one-time" encryption.

Reflection #3

Is it sufficient for an encryption scheme to only have perfect secrecy?

If so, is the following a good encryption?
$Enc(K, m) = 0$, i.e., the encryption of any message m,
using any key K is 0?

No, because Bob cannot correctly recover the original message m with certainty.

⇒ An encryption scheme should have both correctness and privacy.

Next Class

* Formally define a one-time perfectly secure encryption scheme.
* See other examples