Lecture 1: Introduction to Cryptography

Background on functions

Nargiza Tazabekova

SDU University

Cryptography course – Fall 2025

Why Functions in Cryptography?

- Cryptography relies on mathematical functions.
- Functions map inputs (domain) to outputs (codomain).
- Special classes of functions provide:
  - Security (one-wayness, trapdoor)
  - Efficiency
  - Predictable structure

Definition of a Function

Definition

A function $f : X \to Y$ is defined by two sets X and Y and a rule f which assigns to each element in X exactly one element in Y.

Definition of a Function

Definition

A function $f : X \to Y$ is defined by two sets X and Y and a rule f which assigns to each element in X exactly one element in Y.

- X: domain, Y: codomain.
- y is the image of x if $y = f(x)$.
- The set of all elements in Y which have at least one preimage is called the image of f and denoted $\mathrm{Im}(f)$.

Examples of Functions

Example

$f : \{a, b, c\} \to \{1, 2, 3, 4\}$ with $f(a) = 2, f(b) = 4, f(c) = 1.$

Examples of Functions

Example

$f : \{a, b, c\} \to \{1, 2, 3, 4\}$ with $f(a) = 2, f(b) = 4, f(c) = 1$.

Example

$f : \{1, 2, \ldots, 10\} \to \{0, 1, \ldots, 10\}$ defined by $f(x) = x^2 \bmod 11$.

Examples of Functions

Example

$f : \{a, b, c\} \to \{1, 2, 3, 4\}$ with $f(a) = 2, f(b) = 4, f(c) = 1$.

Example

$f : \{1, 2, \ldots, 10\} \to \{0, 1, \ldots, 10\}$ defined by $f(x) = x^2 \bmod 11$.

Explicitly:

$$\begin{array}{lllll} f(1) = 1, & f(2) = 4, & f(3) = 9, & f(4) = 5, & f(5) = 3, \\ f(6) = 3, & f(7) = 5, & f(8) = 9, & f(9) = 4, & f(10) = 1. \end{array}$$

$\mathrm{Im}(f) =$

Special Types of Functions

- **One-to-one (Injective):** Each element in the codomain Y is the image of at most one $x \in X$.

Special Types of Functions

- **One-to-one (Injective):** Each element in the codomain Y is the image of at most one $x \in X$.
- **Onto (Surjective):** Every element of Y is the image of at least one $x \in X$. Equivalently, $\mathrm{Im}(f) = Y$.

Special Types of Functions

- **One-to-one (Injective):** Each element in the codomain Y is the image of at most one $x \in X$.
- **Onto (Surjective):** Every element of Y is the image of at least one $x \in X$. Equivalently, $\mathrm{Im}(f) = Y$.
- **Bijection:** A function that is both injective and surjective. Bijective functions are invertible.

Bijection from Injectivity

Fact: If $f : X \to Y$ is one-to-one (injective), then

$$f : X \to \mathrm{Im}(f)$$

is a bijection.
In particular: If X and Y are finite sets of the same size and f is one-to-one, then f is bijective.

Inverse Functions

Definition

If $f : X \to Y$ is a bijection, then it is possible to define a bijection $g : Y \to X$ as follows: for each $y \in Y$ define

$$g(y) = x \quad \text{where } x \in X \text{ and } f(x) = y.$$

This function g obtained from f is called the **inverse function** of f and is denoted by

$$g = f^{-1}.$$

Inverse Functions

Example

Let

- $X = \{abc, acb, bac, bca, cab, cba\}$
- $Y = \{123, 132, 213, 231, 312, 321\}$

Define $f : X \to Y$ by:

$$\begin{aligned} f(abc) &= 123, \quad f(acb) = 132, \quad f(bac) = 213, \\ f(bca) &= 321, \quad f(cab) = 231, \quad f(cba) = 312. \end{aligned}$$

Since f is a bijection, we can define the inverse:

Inverse Functions

Example

Let

- $X = \{abc, acb, bac, bca, cab, cba\}$
- $Y = \{123, 132, 213, 231, 312, 321\}$

Define $f : X \to Y$ by:

$$f(abc) = 123, \quad f(acb) = 132, \quad f(bac) = 213,$$
$$f(bca) = 321, \quad f(cab) = 231, \quad f(cba) = 312.$$

Since f is a bijection, we can define the inverse:

$$f^{-1}(123) = abc, \quad f^{-1}(132) = acb, \quad f^{-1}(213) = bac, \ldots$$

Involution

Definition

Let S be a finite set and let f be a bijection from S to S (i.e., $f : S \to S$). The function f is called an **involution** if $f = f^{-1}$.
An equivalent way of stating this is

$$f(f(x)) = x \quad \text{for all } x \in S.$$

Example

Let $S = \{1, 2, 3, 4\}$ and define f as the permutation $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$.
Here, $f(1) = 2, f(2) = 1, f(3) = 4, f(4) = 3$. Applying f twice gives back the original element:

Involution

Definition

Let S be a finite set and let f be a bijection from S to S (i.e., $f : S \to S$).
The function f is called an **involution** if $f = f^{-1}$.
An equivalent way of stating this is

$$f(f(x)) = x \quad \text{for all } x \in S.$$

Example

Let $S = \{1, 2, 3, 4\}$ and define f as the permutation $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$.
Here, $f(1) = 2, f(2) = 1, f(3) = 4, f(4) = 3$. Applying f twice gives back the original element:

$$f(f(1)) = 1, \quad f(f(2)) = 2, \quad f(f(3)) = 3, \quad f(f(4)) = 4.$$

Thus f is an involution.

Bijections in Cryptography

In cryptography bijections are used as the tool for encrypting messages and the inverse transformations are used to decrypt.

Cryptographic Interpretation

- f = encryption function
- f^{-1} = decryption function

Every message has exactly one ciphertext, and every ciphertext maps back to a unique message.

Bijections in Cryptography

In cryptography bijections are used as the tool for encrypting messages and the inverse transformations are used to decrypt.

Cryptographic Interpretation

- f = encryption function
- f^{-1} = decryption function

Every message has exactly one ciphertext, and every ciphertext maps back to a unique message.

Example: Let $X = \{A, B, C\}$ (messages) and $Y = \{1, 2, 3\}$ (ciphertexts). Define f:

$$A \mapsto 2, \quad B \mapsto 3, \quad C \mapsto 1$$

Then the inverse f^{-1} is:

$$2 \mapsto A, \quad 3 \mapsto B, \quad 1 \mapsto C$$

Encryption: $B \to 3$ **Decryption:** $3 \to B$

One-Way Functions

Definition

A function $f : X \to Y$ is called a **one-way function** if

- $f(x)$ is "easy" to compute for all $x \in X$, but
- for "essentially all" elements $y \in \mathrm{Im}(f)$ it is "computationally infeasible" to find any $x \in X$ such that $f(x) = y$.

One-Way Functions

Definition

A function $f : X \to Y$ is called a **one-way function** if

- $f(x)$ is "easy" to compute for all $x \in X$, but
- for "essentially all" elements $y \in \mathrm{Im}(f)$ it is "computationally infeasible" to find any $x \in X$ such that $f(x) = y$.

For a *random* $y \in \mathrm{Im}(f)$ it is computationally infeasible to find $x \in X$ such that $f(x) = y$ means:

- Some outputs y might be easy to invert (special cases).
- But for almost all outputs, finding the preimage x is extremely hard.
- "Hard" means no efficient algorithm is known that works in reasonable time.

One-Way Functions

Example

Take $X = \{1, 2, 3, \ldots, 16\}$ and define

$$f(x) = r_x, \quad \text{where } r_x \text{ is the remainder of } 3^x \text{ divided by } 17.$$

One-Way Functions

Example

Take $X = \{1, 2, 3, \ldots, 16\}$ and define

$$f(x) = r_x, \quad \text{where } r_x \text{ is the remainder of } 3^x \text{ divided by } 17.$$

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$f(x)$	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

- Easy to compute $f(x)$ for a given x.
- Harder to invert: given $y = 7$, find x such that $f(x) = 7$.
  Only with the table we see $f(11) = 7$.

One-way Function

Example

Let $p = 48611$, $q = 53993$, and $n = pq = 2624653723$. Define a function on $X = \{1, 2, \dots, n-1\}$ by

$$f(x) = r_x, \quad r_x \equiv x^3 \pmod{n}.$$

- Computing $f(x)$ is straightforward: Example: $f(2489991) = 1981394214$.
- Reversing the process (given y, find x such that $x^3 \equiv y \pmod{n}$) is much harder.
- This is known as the **modular cube root problem**.

If the factors p and q are unknown, inversion is computationally infeasible. If p and q are known, the function can be inverted efficiently.

One-Way Functions Summary

- Easy to compute $y = f(x)$.
- Hard to find x given y.
- Example: $f(x) = 3^x \bmod 17$.
- Foundation for modern cryptography.

Trapdoor One-Way Functions

Definition

A *trapdoor one-way function* is a one-way function $f : X \to Y$ with the additional property that given some extra information (called the *trapdoor information*) it becomes feasible to find for any given $y \in \mathrm{Im}(f)$, an $x \in X$ such that $f(x) = y$.

Generators of Multiplicative Groups

Definition:

Let

$$p$$

be a prime. The set

$$\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$$

forms a multiplicative group modulo p. An element $g \in \mathbb{Z}_p^*$ is called a *generator* if its powers produce all elements of the group:

$$\{g^1 \bmod p, g^2 \bmod p, \ldots, g^{p-1} \bmod p\} = \mathbb{Z}_p^*.$$

Generators of Multiplicative Groups

Definition:

Let

$$p$$

be a prime. The set

$$\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$$

forms a multiplicative group modulo p. An element $g \in \mathbb{Z}_p^*$ is called a *generator* if its powers produce all elements of the group:

$$\{g^1 \bmod p, g^2 \bmod p, \ldots, g^{p-1} \bmod p\} = \mathbb{Z}_p^*.$$

Example:

For

$$p = 7$$

, the group is $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$. Take $g = 3$. Its powers are:

Groups

Definition:

A *group* is a set

$$G$$

together with a binary operation

$$\circ$$

such that:

1. **Closure:** For all

$$a, b \in G$$

,

$$a \circ b \in G$$

.

2. **Associativity:** For all

Trapdoor One-Way Function

Function:

$$f(x) = g^x \bmod p$$

where

$$g$$

is a generator of a multiplicative group modulo a large prime

$$p$$

.

- **Easy direction:** Given

  $$x$$

  , compute

  $$f(x)$$

  quickly.
- **Hard direction:** Given

  $$y$$

Trapdoor One-Way Functions

Function:

$$f(x) = x^e \bmod n$$

where

$$n = p \cdot q$$

is the product of two large primes.

- **Easy direction:** Given

  $$x$$

  , compute

  $$f(x)$$

  quickly.
- **Hard direction:** Given

  $$y = f(x)$$

  , finding

  $$x$$

  is hard without knowing the factors of

Trapdoor One-Way Functions

- One-way function with special **secret information** (trapdoor).
- With trapdoor: inversion becomes feasible.
- Example: RSA function $f(x) = x^e \bmod n$.
- Security relies on hardness of factoring $n = pq$.

Permutations

Definition

Let S be a finite set of elements. A **permutation** p on S is a bijection

$$p : S \longrightarrow S.$$

Example

Let $S = \{1, 2, 3, 4, 5\}$. A permutation $p : S \to S$ is defined as:

$$p(1) = 3,\ p(2) = 5,\ p(3) = 4,\ p(4) = 2,\ p(5) = 1.$$

Permutations as Arrays

A permutation can be written in array form:

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}.$$

Since permutations are bijections, they always have inverses. The inverse of p is:

Permutations as Arrays

A permutation can be written in array form:

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}.$$

Since permutations are bijections, they always have inverses. The inverse of p is:

$$p^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 3 & 2 \end{pmatrix}.$$

Any questions?