

Cryptography L1



Cryptograph
y L1

Introduction to Cryptography
Background on functions

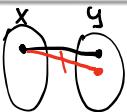
Nargiza Tazabekova
SDU University
Lecture 1 – Fall 2025

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 $f : X \rightarrow Y$ 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 $f : X \rightarrow Y$ 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 $\text{Im}(f)$.

Examples of Functions

Example

ff

private key (one key)
key $\rightarrow [E] \rightarrow \text{ciphertext}$

ciphertext $\rightarrow [D] \rightarrow \text{plaintext}$
 \uparrow
key

public key (2 keys)

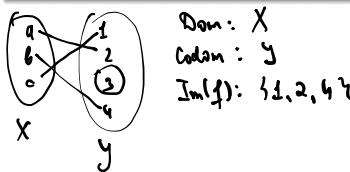
$k_1 \rightarrow [E] \rightarrow C$

$k_2 \rightarrow [D] \rightarrow P$
 \uparrow
C

k_1 - encr. key public.
RSA

DES, Caesar

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



Nargiza Tazibekova

4 / 20

Examples of Functions

Example

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

Example

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

$$\begin{aligned}f(1) &= 1^2 \bmod 11 = 1 & f(5) &= 25 \% 11 = 3 \\f(2) &= 2^2 \bmod 11 = 4 & \\f(3) &= 9 \\f(4) &= 4^2 \bmod 11 = 16 \% 11 = 5\end{aligned}$$

Nargiza Tazibekova

4 / 20

Examples of Functions

Example

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

Example

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

Explicitly:

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

$$\text{Im}(f) = \{1, 3, 4, 5, 9\}$$

Nargiza Tazibekova

4 / 20

Special Types of Functions

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

Nargiza Tazibekova

5 / 20

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, $\text{Im}(f) = Y$.



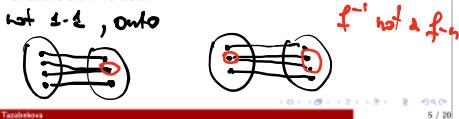
Nargiza Tazibekova

5 / 20

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, $\text{Im}(f) = Y$.
- **Bijection:** A function that is both injective and surjective. Bijective functions are invertible.



Nargiza Tatsibekova

5 / 20

Bijection from Injectivity

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

$$f : X \rightarrow \text{Im}(f) \Rightarrow |X| = |\text{Im}(f)|$$

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.

$$\begin{aligned} f: \{1, 2, 3, 4\} &\rightarrow \{1, 2, 3, 4\} \quad f(x) = x^2 \\ f(1) = 1 & \quad f: \{1, 2, 3, 4\} \rightarrow \{1, 2, 3, 4\} \text{ is a bijection} \\ f(2) = 4 & \quad f: \{1, 2, 3, 4\} \rightarrow \{1, 2, 3, 4\} - \{1, 4\} \\ f(3) = 9 & \end{aligned}$$

Nargiza Tatsibekova

6 / 20

Inverse Functions

Definition

If $f : X \rightarrow Y$ is a bijection, then it is possible to define a bijection $g : Y \rightarrow X$ 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

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

Nargiza Tatsibekova

7 / 20

Inverse Functions

Example

Let

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

Define $f : X \rightarrow Y$ by:

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

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

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

Nargiza Tatsibekova

8 / 20

Inverse Functions

Example

Let

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

Define $f : X \rightarrow Y$ by:

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

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

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

Nargiza Tatsibekova

8 / 20

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

f^{-1} = decryption function

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

Nargiza Tatsibekova

9 / 20

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: $B \rightarrow 3$ **Decryption:** $3 \rightarrow B$

Nargiza Tatsibekova

9 / 20

One-Way Functions

Definition

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

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

Nargiza Tatsibekova

10 / 20

One-Way Functions

Definition

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

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

For a random $y \in \text{Im}(f)$ 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.

Nargiza Tatsibekova

10 / 20

One-Way Functions

Example

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

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

$$f(1) = 3$$

$$f(2) = 9$$

$$f(3) = 3^3 \% 17 = 10$$

Nargiza Tatsibekova

11 / 20

One-Way Functions

Example

Take $X = \{1, 2, 3, \dots, 16\}$ 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 $f(11) = 7$.

Nargiza Tazibekova 11 / 20

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:
 $f(248991) = 1981394214$.
 - 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.

Nargiza Tazibekova 12 / 20

One-Way Functions Summary

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

Nargiza Tazibekova 13 / 20

Trapdoor One-Way Functions

Definition

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

Nargiza Tazibekova 14 / 20

Generators of Multiplicative Groups

Definition:

Let p be a prime. The set

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

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:

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

Nargiza Tazibekova 15 / 20

Generators of Multiplicative Groups

Definition:

Let p be a prime. The set

$$\begin{aligned} g &= 3 \\ 3^3 &\pmod{7} = 6 \end{aligned}$$

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

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:

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

Example:

For $p = 7$, the group is $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$. Take $g = 3$. Its powers are:

$$3^1 \equiv 3, \quad 3^2 \equiv 2, \quad 3^3 \equiv 6, \quad 3^4 \equiv 4, \quad 3^5 \equiv 5, \quad 3^6 \equiv 1 \pmod{7}.$$

Since all nonzero elements appear, $g = 3$ is a generator of \mathbb{Z}_7^* .

Nargiza Tazibekova

15 / 20

Groups

Definition:

A group is a set G together with a binary operation \circ such that:

- **Closure:** For all $a, b \in G$, $a \circ b \in G$.
- **Associativity:** For all $a, b, c \in G$, $(a \circ b) \circ c = a \circ (b \circ c)$.
- **Identity:** There exists an element $e \in G$ such that for all $a \in G$, $a \circ e = e \circ a = a$.
- **Inverses:** For every $a \in G$, there exists $a^{-1} \in G$ such that $a \circ a^{-1} = a^{-1} \circ a = e$.

Example: $(\mathbb{Z}, +)$ is a group:

- Closure: sum of integers is an integer.
- Associativity: $(a + b) + c = a + (b + c)$.
- Identity: 0.
- Inverse: $-a$ for each a .

Nargiza Tazibekova

16 / 20

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 $y = f(x)$, finding x (the discrete log) is hard.
- **Trapdoor:** With extra hidden structure (in some systems), inversion becomes feasible.

Basis for Diffie-Hellman key exchange and ElGamal encryption.

Nargiza Tazibekova

17 / 20

Trapdoor One-Way Functions

Function:

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

RSA
e - public key

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 n .
- **Trapdoor:** If you know p and q , you can compute the private key d and invert:

$$x = y^d \bmod n \quad d \text{ depends on } p, q$$

Used in RSA encryption/decryption.

$$\phi = (p-1)(q-1)$$

Nargiza Tazibekova

18 / 20

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 $n = pq$.

Nargiza Tazibekova

19 / 20

Any questions?