Cryptography

Cunsheng DING, HKUST

COMP3631

Lecture 01: Functions

Outline of This Lecture

1. To recall sets.
2. To recall functions.
3. To explain why functions are important in security systems.

Definition of Sets

Definition: A set is a collection of (distinct) objects.

Example: $A = \{x, y, z\}$.

Example: $B = \{1, 2\}$.

Example: $C = \{1, 2, x\}$.

Example: Z the set of all integers.

Example: $S = \{x \in Z : x > 0\}$.

Membership: We write $a \in A$ if a is an element of A.

The Number of Elements in a Set

Example: $|A| = |\{x, y, z\}| = 3$

Example: $|B| = |\{1, 2\}| = 2$.

Example: $|C| = |\{1, 2, x\}| = 3$.

Cardinality of a set A: the number of elements in A.

Cartesian Product of Sets (I)

Definition: The Cartesian product of two sets A and B is defined as

$$A \times B = \{(a, b) : a \in A,\ b \in B\}.$$

Example: Let $A = \{x, y, z\}$ and $B = \{1, 2\}$. Then

$$A \times B = \{(x, 1), (x, 2), (y, 1), (y, 2), (z, 1), (z, 2)\}.$$

Question: For the sets A and B above, what is $B \times A$?

Question: For the set A above, what is $A^2 := A \times A$?

Cartesian Product of Sets (II)

Definition: The n-ary Cartesian product over n sets $A_1, \ldots, A_n$:

$$A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) : a_i \in A_i \text{ for very } i \in \{1, \ldots, n\}\}.$$

Definition: The n-ary Cartesian power of A:

$$A^n := A \times \cdots \times A := \{(a_1, \ldots, a_n) : a_i \in A \text{ for very } i \in \{1, \ldots, n\}\}.$$

Alphabets and A Set Notation

Definition: An **alphabet** A is a finite set. Every element of A is called a **letter** or **character**.

Example: The English alphabet, the German alphabet, the Chinese alphabet, $A = \{0, 1\}$.

Definition: For a finite set A, define

$$A^* := \{a_1 a_2 \dots a_t : a_i \in A \text{ for each } i \text{ and } t \text{ is a positive integer}\},$$

that is, A^* consists of all finite strings of letters from A.

Remark: This set notation A^* is often used in this course.

Definition of Functions

Definition: A function f from A to B is a *mapping* (i.e., a set $A \times B'$, where $B' \subseteq B$) such that f maps each element $a \in A$ to a **unique** element, denoted $f(a)$, in B.

Example: Let $A = \{x, y, z\}$ and $B = \{1, 2\}$. Is the mapping

$$x \mapsto 1,\ x \mapsto 2,\ y \mapsto 2,\ z \mapsto 2$$

a function from A to B? Why?

Example: Let $A = \{x, y, z\}$ and $B = \{1, 2\}$. Is the mapping

$$x \mapsto 2,\ y \mapsto 2,\ z \mapsto 2$$

a function from A to B? Why?

Some Basic Concepts of Functions

Domain and range: Let f be a function from A to B. Then A is called the **domain** of f and the **range** of f is defined to be

$$f(A) := \{f(a) : a \in A\} \subseteq B.$$

Image and preimage: Let f be a function from A to B and $f(a) = b$, where $a \in A$ and $b \in B$. Then b is said to be the **image** of a under f and a is called a **preimage** of b under f.

The Number of Functions from A to B

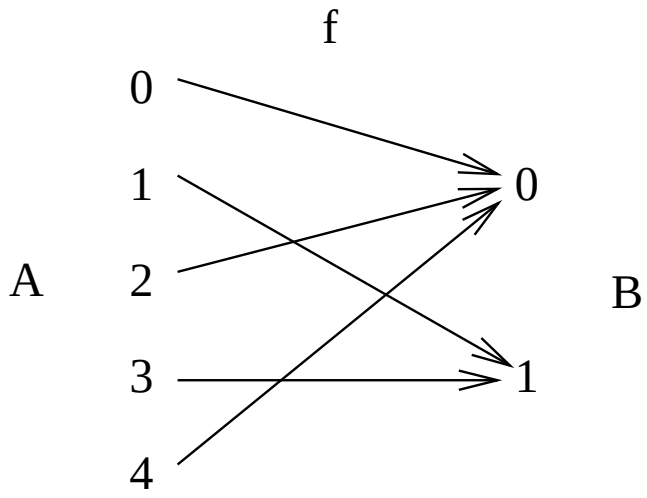
Question: Let $|A| = m$ and $|B| = n$. What is the total number of functions from A to B?

How to Describe Functions

Formula Description: Let $A = \{0, 1, 2, 3, 4\}$ and $B = \{0, 1\}$. Define

$$f(x) = x \bmod 2$$

Pictorial Description: For the f above,



Remark: These are school approaches. There are other approaches.

Onto Functions (Surjections)

Definition: A function f from A to B is *onto (surjective)* if there is at least one $a \in A$ such that $f(a) = b$ for every $b \in B$.

Example: Let $A = \{0, 1, 2, 3, 4\}$ and $B = \{0, 1\}$. Is the function

$$f(x) = x \bmod 2$$

onto? Why?

Example: Let $A = \{x, y, z\}$ and $B = \{1, 2\}$. Is the function

$$x \mapsto 2,\ y \mapsto 2,\ z \mapsto 2$$

onto? Why?

Onto Functions

Question: Let $|A| = m$ and $|B| = n$, where $m \geq n$. What is the total number of onto functions from A to B?

Onto Functions

Question: Let $|A| = m$ and $|B| = n$, where $m \geq n$. What is the total number of onto functions from A to B?

Solution: It is

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m.$$

You may use an inclusion-exclusion argument to prove this result.

Remark: You are not required to prove this result.

The Inclusion-Exclusion Principle: $|D \cup E| = |D| + |E| - |D \cap E|$.

One-to-one Functions (Injections)

Definition: A function f from A to B is *one-to-one (injective)* if $f(a_1) \neq f(a_2)$ for every pair (a_1, a_2) of distinct elements in A.

Example: Let $A = \{0, 1, 2, 3, 4\}$ and $B = \{0, 1\}$. Is the function

$$f(x) = x \bmod 2$$

one-to-one? Why?

Example: Let $A = \{x, y\}$ and $B = \{1, 2\}$. Is the function

$$x \mapsto 1, \quad y \mapsto 2$$

one-to-one? Why?

Question: Let $|A| = m$ and $|B| = n$, where $m \leq n$. What is the total number of one-to-one functions from A to B?

One-to-one Functions (Injections)

Question: Let $|A| = m$ and $|B| = n$, where $m \leq n$. What is the total number of one-to-one functions from A to B?

Answer: It is

$$m!\binom{n}{m} = \frac{n!}{(n-m)!} = n(n-1)(n-2)\cdots(n-(m-1)).$$

Remark: This question has an important cryptographic meaning, which will be explained later.

One-to-one Correspondences (Bijections)

Definition: A function f from A to B is a *one-to-one correspondence (bijection)* if it is both onto and one-to-one.

Example: Let $A = \{0, 1, 2, 3, 4\}$ and $B = \{0, 1\}$. Is the function

$$f(x) = x \bmod 2$$

a one-to-one correspondence? Why?

Example: Let $A = \{x, y\}$ and $B = \{1, 2\}$. Is the function

$$x \mapsto 1, \quad y \mapsto 2$$

a one-to-one correspondence? Why?

Inverse Functions

Definition: Let f be a one-to-one correspondence from A to B. The inverse of f, denoted by f^{-1}, is defined by

$$f^{-1}(b) = a \text{ if and only if } f(a) = b.$$

Conclusion: f^{-1} is a one-to-one correspondence from B to A.

Example: Let $A = \{x, y\}$ and $B = \{1, 2\}$ and

$$f : x \mapsto 1,\ y \mapsto 2.$$

Then

$$f^{-1} : 1 \mapsto x,\ 2 \mapsto y.$$

The Identity Function

Definition: The *identity function* I_A from A to A is defined by

$$I_A(a) = a \text{ for every element } a \in A.$$

Conclusion: I_A is a one-to-one correspondence from A to A.

Example: Let $A = \{x, y\}$.

$$I_A : x \mapsto x,\ y \mapsto y.$$

Conclusion: The inverse of I_A is itself.

Function Composition

Definition: Let f be a function from A to B, and g a function from B to C. The *composition* of g and f or *composition* of g after f denoted by $g \circ f$, is a function from A to C defined as

$$(g \circ f)(a) := g(f(a))$$

for all $a \in A$

Example: Let $A = \{x, y\}$, $B = \{1, 2\}$, $C = \{u, v\}$,

$$f : x \mapsto 1,\ y \mapsto 2$$

$$g : 1 \mapsto u,\ 2 \mapsto u.$$

Then

$$g \circ f : x \mapsto u,\ y \mapsto u.$$

Function Composition - ctd.

Definition: Let f be a function from A to B, and g a function from B to C. The *composition* of g and f or *composition* of g after f denoted by $g \circ f$, is a function from A to C defined as

$$(g \circ f)(a) := g(f(a))$$

for all $a \in A$

Remark: Although $g \circ f$ is well defined, $f \circ g$ may not be well defined, as the image of g may not be a subset of the domain of f. See the example in the previous page.

Remark: Even if both $g \circ f$ and $f \circ g$ are well defined (e.g., when $A = B = C$), they may be different functions! See the example in the next page.

Function Composition - ctd.

Question: Let $A = B = C$, be the set of integers.

$$f(x) = x + 1 \text{ and } g(x) = x^2 + x.$$

What is $g \circ f$? What is $f \circ g$?

Conclusion: Let f be a one-to-one correspondence from A to B. Then

$$f^{-1} \circ f = I_A \text{ and } f \circ f^{-1} = I_B.$$

The cryptographic meaning of the first equality will be explained later.

Permutations

Definition: A *permutation* f of A is a one-to-one correspondence from A to A.

Example: Let $A = \{0, 1, 2\}$ and $f(x) = (x + 1) \bmod 3$.

Conclusion: Every permutation f of A has the inverse f^{-1}. Clearly f^{-1} is also a permutation of A.

Example: Let $A = \{0, 1, 2\}$ and f be the same as above. Then

$$f^{-1}(x) = (x + 2) \bmod 3.$$

Question: What is the total number of permutations of A with n elements?

The Importance of Functions in Security Systems

Summary:

- Almost every building block in a cryptographic system is a function.
- A bijection may be used for encrypting a piece of data, and its inverse function will be used for decrypting the received data.
- Function composition is an important operation in many cryptographic systems.