ICT Course: Introduction to Information Security

Nguyen Minh Huong

ICT Department, USTH

December 12, 2022

Session 1: Introduction

1. Introduction
   - Security concerns
   - Information Security aspects
     - Cryptology
     - Access Control
     - Protocols
     - Software
2. Modular Arithmetic

What is "Information System"?

Example: Homework submission system

What is an Information system comprised of?

What is Information Security?

What is Information Security?

- **Information system** is an organized system for the **collection**, **organization**, **storage** and **communication** of information.
- Information system's components: hardware, software, data, people, procedures, and networks.
- **Information security**: is the protection of information assets that **use**, **store**, or **transmit** information from risk through the application of policy, education, and **technology**.

Main question

How to use, store and transmit the information securely?

What does "securely" mean?

Alice wants to send a love letter to Bob. What may happen to the letter that Alice may afraid of?

What does "securely" mean?

- Information is kept secret
- Information is protected from being manipulated
- Services are available
- Identification of the user is true
- Restriction on actions of authenticated users

Security Concerns

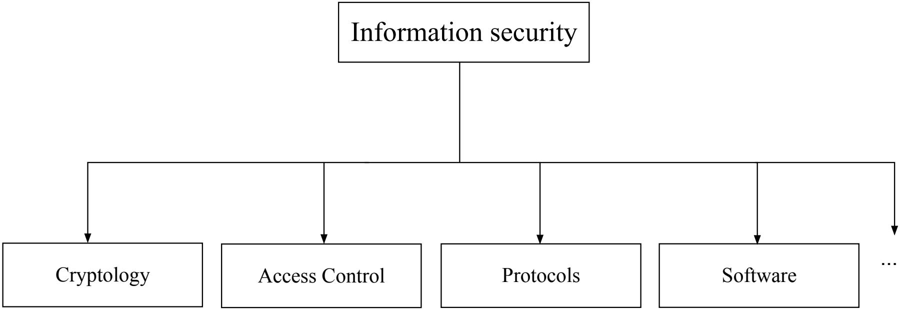
- Confidentiality
- Integrity
- Availability
- Authentication
- Authorization

How to guarantee the information security?

How to guarantee the information security?

- **What** information is exchanged **securely**?
- **How** to exchange information **securely**?
- **Who** are allowed to access to information?
- How each participants can do with the information?

Information Security Aspects


Information security

Cryptology

Access Control

Protocols

Software

...

Course Description

- 3 credits
- References:
  1. Paar, Christof, and Jan Pelzl. Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media, 2009.
  2. Stamp, Mark. Information security: principles and practice. John Wiley & Sons, 2011.
  3. M. Bishop, Computer Security: Art and Science, Addison Wesley, 2003.
- Assessment:

Attendance	Mid-term	Active	Final Exam
10 %	35%	5%	50%

Modular Arithmetic

Why do we need to study modular arithmetic?[1]

- Extremely important for asymmetric cryptography (RSA, elliptic curves etc.)
- Some historical ciphers can be elegantly described with modular arithmetic (cf. Caesar and affine cipher later on).

[1] Understanding Cryptography by Christof Parr and JanPelzl

Introduction to Modular Arithmetic

- Modular Arithmetic is a system of arithmetic of integers, which considers the remainder
- Definition:

Modulus Operation

Let a, r, m be integers and $m > 0$. We write

$$a \equiv r\ mod\ m$$

if $(r - a)$ is divisible by m.

- m is called the modulus
- r is called the remainder

- Example:

$$15 \equiv 3\ (mod\ 6)$$

$$21 \equiv 3(mod\ 6)$$

- The remainder is not unique:
  Examples:

$$12 \equiv \ 3 \ (mod \ 9)$$

$$12 \equiv \ 21 \ (mod \ 9)$$

- Which remainder do we choose?
  By convention, we usually agree the smallest positive integer r as remainder:

$$a = q.m + r \ where \ 0 \leq r \leq m - 1 \ , \ q : quotient$$

Congruence

- Two integers *a* and *b* are congruent modulo N if they have the same remainder upon division by N

$$a \equiv b\ (mod\ N)\ \leftrightarrow b \equiv a\ (mod\ N)$$

Addition

- If $a + b = c$, then $a + b \ \equiv c \ (mod \ N)$
- If $a \equiv b(mod \ N)$, then $a + k \equiv b + k \ (mod \ N)$
- If $a \equiv b(mod \ N)$ and $c \equiv d(mod \ N)$, then $a + c \equiv b + d(mod \ N)$
- If $a \equiv b(mod \ N)$, then $-a \equiv -b(mod \ N)$

Multiplication

- If $a * b = c$, then $a * b \equiv c(mod\ N)$
- If $a \equiv b(mod\ N)$, then $k * a \equiv k * b(mod\ N), \forall k \in \mathbb{Z}$
- If $a \equiv b(mod\ N)$, and $c \equiv d(mod\ N)$, then $a * c \equiv b * d(mod\ N)$

Exponentiation

- If $a \equiv b(mod\ N)$, then $a^k \equiv b^k(mod\ N), \forall k \in \mathbb{Z}, k > 0$

Division

- If $gcd(k, N) = 1$ (k and N are coprime) and $k * a \equiv k * b (mod\ N)$, then $a \equiv b (mod\ N)$

Multiplicative inverse

- If $gcd(a, N) = 1$, $\exists x \in \mathbb{Z}$ such that $a * x \equiv 1(mod\ N)$
- x is called the multiplicative inverse of a modulo N

$$x \equiv a^{-1}(mod\ N)$$

Equivalent Classes

- Equivalent class is a set of numbers that have the same remainder for modulus m
- With a fixed modulus, we are free to choose the class element that results in the easiest computation
- Example:

$$3^8 = 6567 \equiv 2\, mod\, 7$$

$$3^8 = 3^4 * 3^4 = 81 * 81$$

$$81 \equiv 4\, mod\, 7,\ then\ 81 * 81 \equiv 4 * 4\, mod\, 7\ =\ 2\, mod\, 7$$

Exercises

Ex 1: Compute the result without a calculator:

- $15 * 29\ mod\ 13$
- $2 * 29\ mod\ 13$
- $2 * 3\ mod\ 13$
- $-11 * 3\ mod\ 13$

1. Ex2: Compute x as far as possible without a calculator:
    - $x = 3^2\ mod\ 13$
    - $x = 7^2\ mod\ 13$
    - $x = 3^{10}\ mod\ 13$
    - $x = 7^{100}\ mod\ 13$
    - $7^x = 11\ mod\ 13$

Euler's phi function

- Euler's phi function, $\Phi(m)$ is the number of positive integers less than m that are relatively prime to m.
- Example: What is $\Phi(m)$ for $m = 3, 4, 5, 9, 26$?