Cryptography Basics

Cryptography And Authentication

MIZOGUCHI Koki *

Kochi University of Technology

September 7, 2022

KOCHI UNIVERSITY OF TECHNOLOGY

*Infromation Security System Lab.

Table of Contents

1 - 1. Three elements of information security

The following three are called the "three elements if information security"

- Confidentiality
- Integrity
- Availability

1 - 1. Three elements of information security

Confidentiality

Unauthorized persons should not have access to the information.

Integrity

Information remains accurate and unaltered or erased.

Availability

Authorized persons should be able to access information whenever they want.

1 - 1. Three elements of information security

Requirement	Characteristics required	Cryptography
Confidentiality	Data Privacy	Encryption, Authentication
Integrity	Data Accuracy	message authentication, signature
Availability	Ease of access to data	secret sharing

1 - 2. Definition of Information Security

Information security is defined in *JIS Q 27000* [a].

[a] JIS(Japanese Industrial Standards) is national standard of Japan for standardization of Japanese industry.

JIS Q 27000 states that "Information security is the maintenance of confidentiality, integrity, and availability of information".

1 - 3. Additional Requirements

When handling more sensitive information, the following requirements should be considered in addition to the three elements of information security.

- Authenticity
- Accoutability
- Non-repudiation
- Reliability

1 - 3. Additional Requirements

Authenticity

The user or system is really the person and system, and no imposters are mixed in.

Accountability

When a system behaves strangely or is attacked, it should be possible to trace what happened and why.

1 - 3. Additional Requirements

Non-repudiation

Transactins, registrations, and other operations should not be later pretended to be something they are not.

Reliability

The system is operating correctly and without any defects.

1. Infomation security
   - Three elements of information security
   - Definition of Information Security
   - Additional Requirements

2. Encryption
   - What is Cryptography?
   - Decoding

3. Authentication
   - Password Authentication
   - Password Attack Techniques
   - Authentication Classification
   - Authorization
   - OAuth

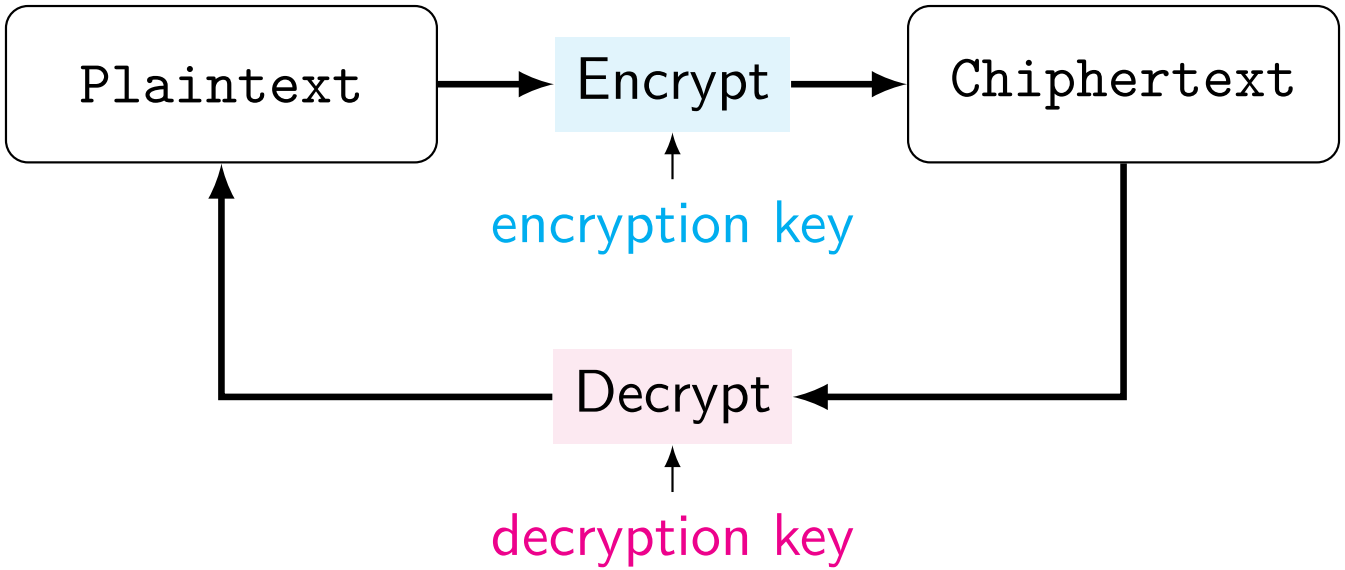
2 - 1. What is Cryptography?

Encrypt

The information should be in a form that cannot seen by a third party.

Decrypt

Converting chiphertext back to plaintext.



2 - 2. Decoding

Decoding

Obtaining plaintext information in a way that was not intended by the chipher developer, without following a legitimate decryption process.

1. Infomation security
   - Three elements of information security
   - Definition of Information Security
   - Additional Requirements
2. Encryption
   - What is Cryptography?
   - Decoding
3. Authentication
   - Password Authentication
   - Password Attack Techniques
   - Authentication Classification
   - Authorization
   - OAuth

3 - 1. Password Authentication

Authentication

A process by which a person confirms to another person that he or she is indeed that person.

Password or Passphrases

Passphrase is more strong.

System	Pattern example	Number of combinations	example
Password	8 characters	62^8	`P1kAIMiG`
Passphrase	4 words *	4000^4	`we map as ps`

[a] from 4000 words

3 - 2. Password Attack Techniques

The following are the main password attack techniques.

- Dictionary attack
- Brute-force attack
- Reverse burute-force attack
- Password spray attack
- Password list attack

3 - 2. Password Attack Techniques

Dictionary attack

Obtain a list of popular passwords and try them one after the other.

Blute-force attack

Fix the ID of a user and try passwords in order.

Reverse blute-force attack

Fix the password and try ID in order.

Password spray attack

Based on a large number of ID information, for each ID, try the same password in order.

3 - 2. Password Attack Techniques

Password list attack

When one service is attacked and the password is leaked, the other service may also be attacked by password reuse.

Password Manager

It is difficult to remember passwords for many services, each with a different password.
There is a management tool called **Password Manager**.

The password manager itself can also be attacked.Consideration should be given when using it.

3 - 3. Authentication Classification

The following is a standard authentication method.

- Knowledge authentication [a]
- Biometrics [b]
- One-Time password maker [c]
- Propety authentication [d]

[a] Use knowledge known the person.
[b] Use biometrics information such as finger points and veins.
[c] Use a temporary password generated.
[d] Use something that only the person has.

Client certificate

When security is important to service provider, a digital certificate called a *client certificate* is issued for each other.

3 - 3. Authentication Classification

Types and characteristics authentication

Types	Memory	Risk of loss	Costs	Measures
Knowledge	Necessary	Have	Low	Easy
Biometrics	Not Necessary	Have	High	Difficulty
Propety	Not Necessary	Have	High	Easy

Multi-Factor authentication

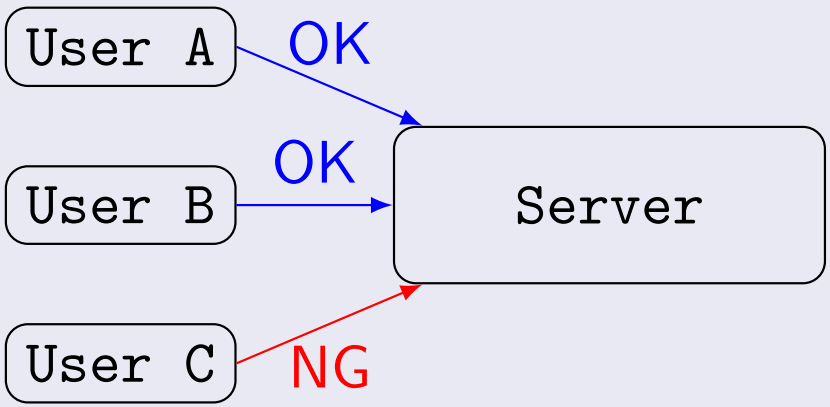
A number of several authentication methods.

3 - 4. Authorization

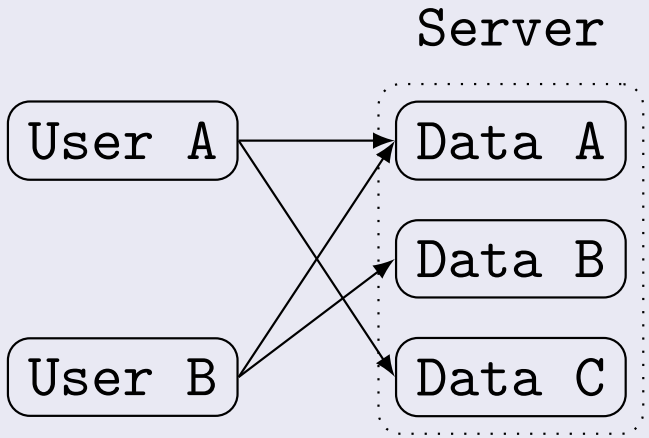
Authorization

After authentication, the user is given accses right to the system according to user propeties.

Authentication

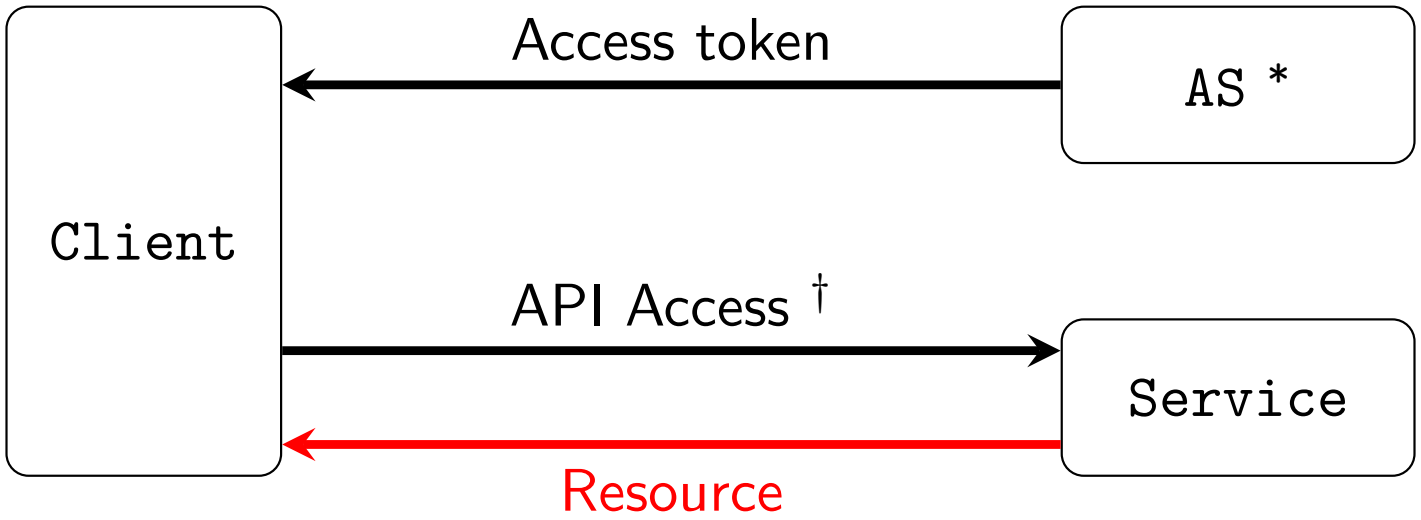


Authorization



OAuth

OAuth(Open Authorization) is system used to allow multiple web services to work together.



*AS : Authorization Server

†With an access token.

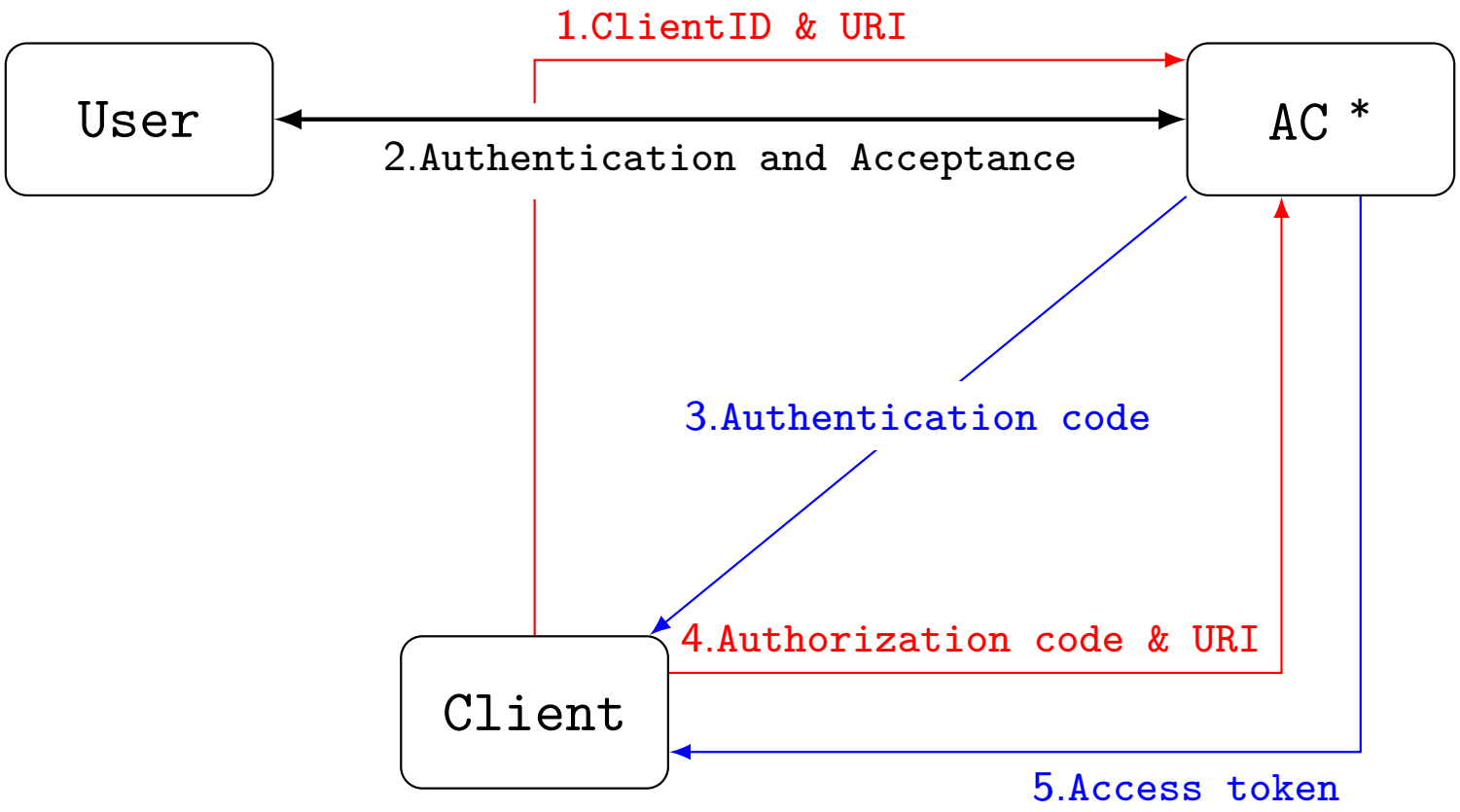
3 - 5. OAuth

Access token issuance procedure

1. The client sends an authorization request to authorization server via web browser, together with a client ID and a URI to redirect.
2. The authorization server authenticates the user via a browser and outputs a "permission" acceptance screen.
3. If the user allows it, the authorization server redirects the browser and sends authorization code to the client.
4. The client server sends the authorization code and redirect URI to the authorization server.
5. The authorization server authenticates the client, verifies the authorization code and redirect URI, and sends access token to the client.

3 - 5. OAuth

OAuth 2.0 Authorization code ground



*AC : Authentication Server