Common Key Cryptosystem

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. Common key cryptosystem

Common key cryptosystem

A chipher in which the key used for encryption and decryption are the same.
Also called secret key cryptography or symmetric key cryptography.

The encryption of a message(m) (plaintext) with a secret key(s) is reporesented as follows.

$$c = \mathrm{Enc}(s, m)$$

The decryption of a message with a secret key is represented as follows.

$$m = \mathrm{Dec}(s, c)$$

1 - 2. Type of common key cryptosystem

There are 2 types of common key cryptosystem.

1. Stream chipher
2. Block chipher

1 - 3. Stream chipher

1 - 4. Block chipher