SINGAPORE INSTITUTE OF TECHNOLOGY

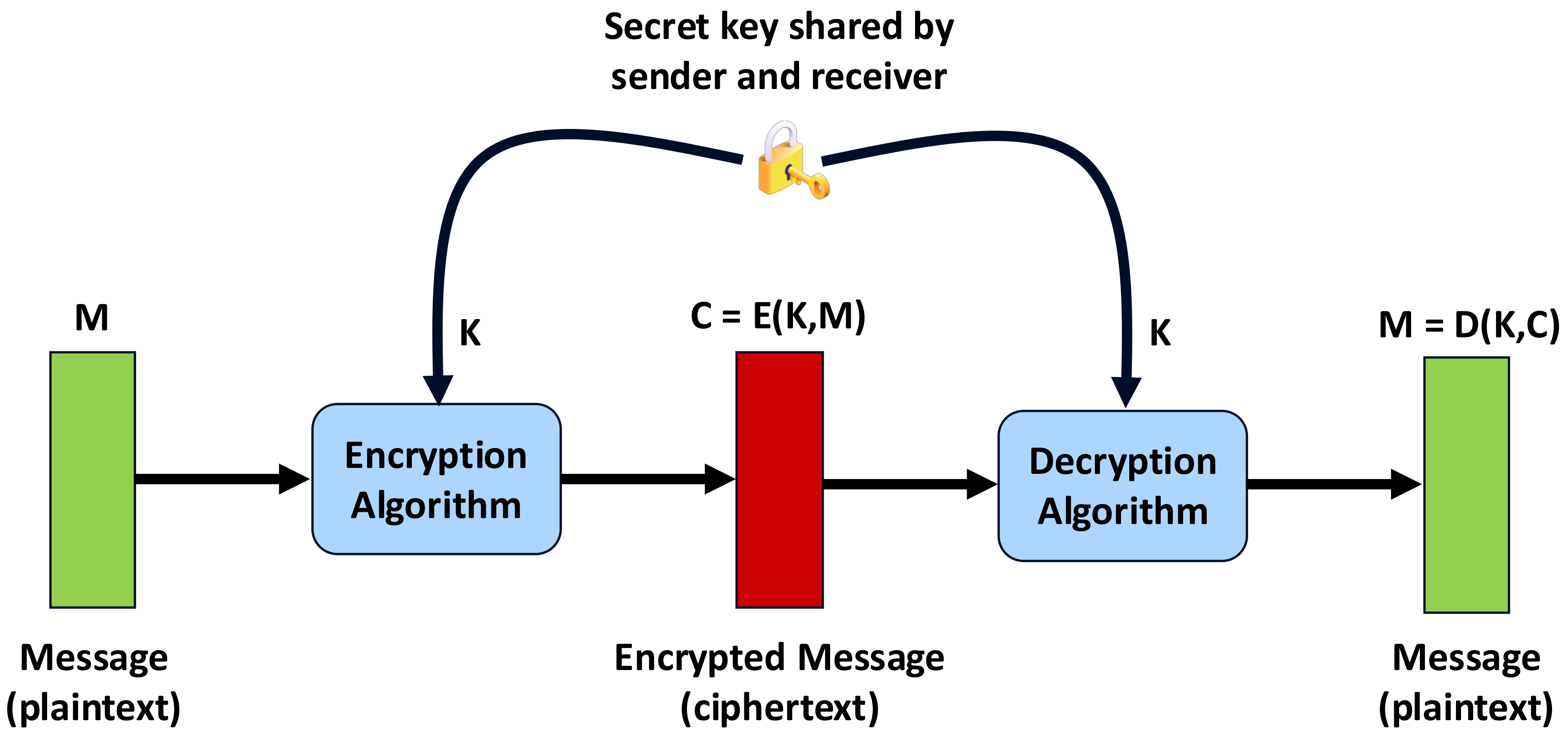
ICT2213 Applied Cryptography

Topic 1.1: Introduction

Learning outcomes

- Follow basic terminology
- Understand how cryptography can be used to secure systems
- List the different types of cryptographic algorithms
- Understand what constitutes a secure cryptographic algorithm

Symmetric encryption



What cryptography can offer

Confidentiality

Keeping information secret

Integrity

The receiver can verify that the message was not modified in transit

Authentication

The receiver of a message can verify its origin

Cryptographic algorithms

SINGAPORE INSTITUTE OF TECHNOLOGY

Symmetric algorithms

- The sender and receiver share the same key
- The key must be agreed upon before the parties can communicate securely
- Two categories: stream ciphers (operate on bytes) and block ciphers (operate on blocks, e.g., 16 bytes)

Public key algorithms

- Two different keys: public key (for encryption) and private key (for decryption)
- The public key can be shared with anyone to use
- The private key cannot be computed from the public key, given finite resources

Cryptanalysis vs. brute-force attacks

Cryptanalysis

- Relies on the characteristics of the algorithm and possibly some knowledge of the nature of the plaintext
- Objective is to deduce the key or, at least, a specific plaintext
- A cryptanalytic attack may also reveal some limited information about the key or plaintext (e.g., a few bits)

Brute-force attack

- The attacker tries every possible key on a ciphertext
- Eventually, this process will output an intelligible plaintext, which identifies the underlying key
- On average, a successful brute-force attack requires testing half of all possible keys

Cryptanalytic attack types

Attack type	Known to cryptanalyst
Ciphertext only	One or more messages (ciphertexts) encrypted with the same key
Known-plaintext	One or more plaintext-ciphertext pairs encrypted with the same key
Chosen-plaintext	The attacker chooses one or more plaintexts that get encrypted (with the same key) and has access to the resulting ciphertexts
Chosen-ciphertext	The attacker can choose different ciphertexts (encrypted with the same key) to be decrypted and has access to the decrypted plaintext. Primarily applicable to public key algorithms

Kerckhoffs' principle

Kerckhoffs' principle

- Secrecy must reside entirely in the key
- The cryptanalyst has complete details of the cryptographic algorithm
- The keyspace (all possible values of the key) must be very large

Security by obscurity

- Keeping the way the algorithm works secret
- Not adequate by today's standards

Security of algorithms

SINGAPORE INSTITUTE OF TECHNOLOGY

Unconditional security

- There is never enough information to recover the plaintext
- Also known as information-theoretic security
- Only the One-Time Pad is unbreakable, given infinite resources

Computational security

- The algorithm cannot be broken with available resources, either current or future
- Every algorithm is breakable in a ciphertext-only attack.
- For example, a brute-force attack on the key

Attack complexity

SINGAPORE INSTITUTE OF TECHNOLOGY

Measures

- **Processing complexity:** Time needed to perform the attack
- **Data complexity:** The amount of data needed as input to the attack
- **Storage complexity:** The amount of memory needed for the attack

Complexities are expressed as orders of magnitude (powers of 2)

Example

- Suppose we want to brute-force a 128-bit key
- In this case, the data and storage complexities are negligible
- The processing complexity is 2^{128}, i.e., the number of possible keys to test
- Suppose we have one million parallel CPUs, each capable of testing one million keys per second
- The attack will take over 10^{19} years