# Chapter 2-1

## Conventional Encryption Message Confidentiality

# Outline

- Conventional Encryption Principles
- Conventional Encryption Algorithms
- Cipher Block Modes of Operation
- Location of Encryption Devices
- Key Distribution

# Conventional Encryption Principles

- An encryption scheme has five ingredients:
  - Plaintext
  - Encryption algorithm
  - Secret Key
  - Ciphertext
  - Decryption algorithm
- Security depends on the secrecy of the key, not the secrecy of the algorithm

# Conventional Encryption Principles

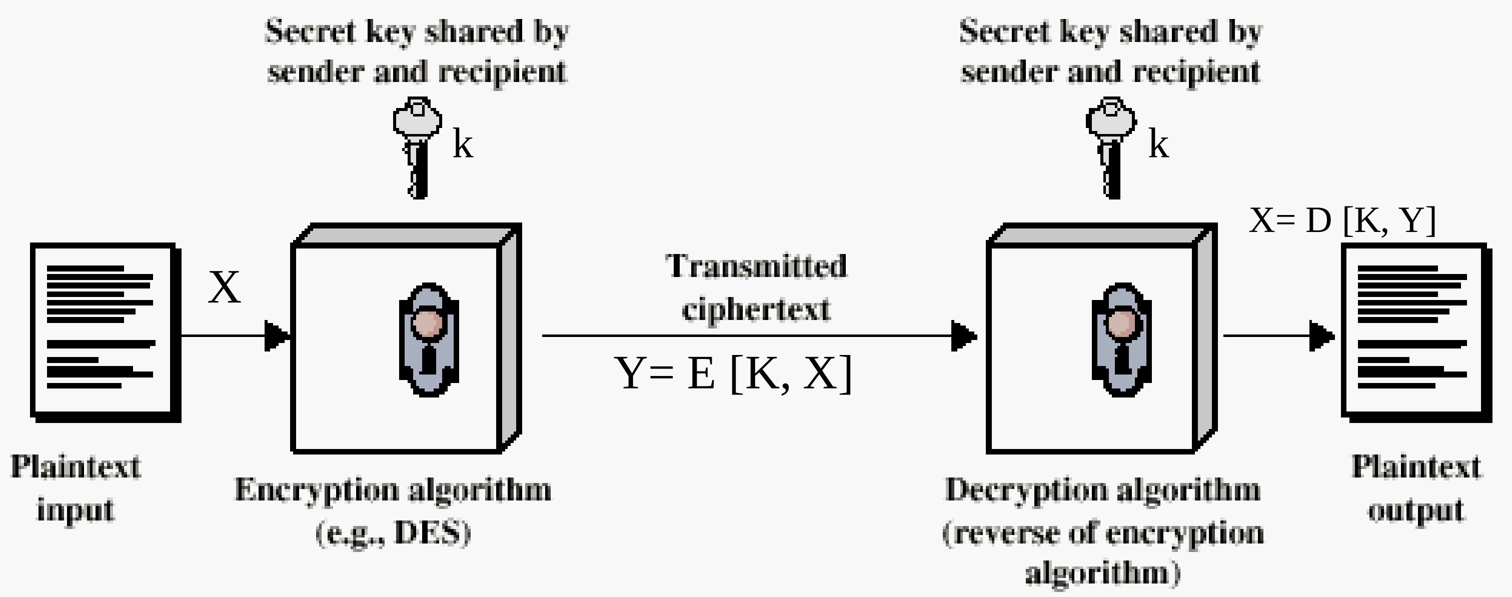



Figure 2.1 Simplified Model of Conventional Encryption

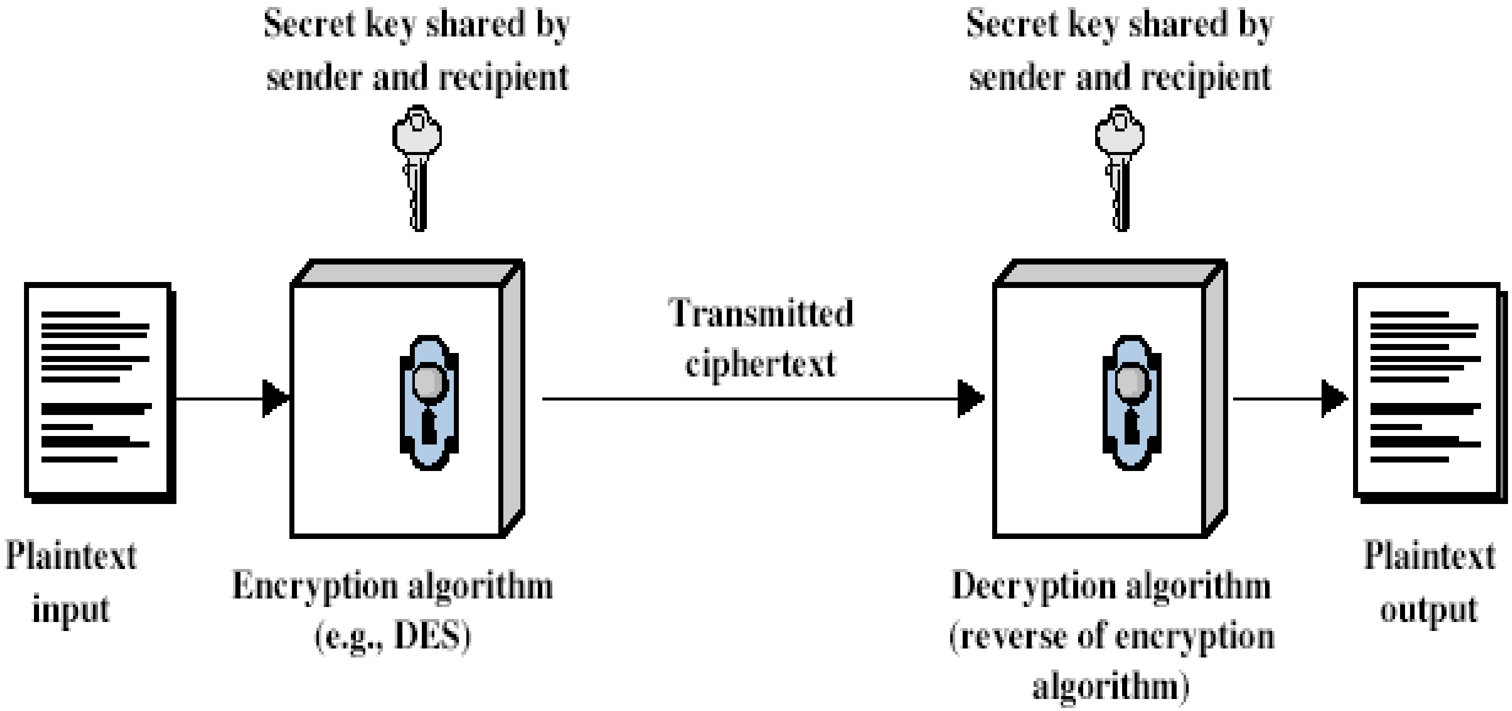
# Symmetric Encryption

- or conventional / secret-key / single-key
- sender and recipient share a common key
- was the only type of cryptography, prior to invention of public-key in 1970's

# Basic Terminology

- **plaintext** - the original message
- **ciphertext** - the coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - information used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering ciphertext from plaintext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - the study of principles/ methods of deciphering ciphertext *without* knowing key
- **cryptology** - the field of both cryptography and cryptanalysis

# Symmetric Cipher Model



# Requirements

- Two requirements for secure use of symmetric encryption:
  - a strong encryption algorithm
  - a secret key known only to sender / receiver

    $Y = E_K(X)$

    $X = D_K(Y)$
- assume encryption algorithm is known
- implies a secure channel to distribute key

# Cryptography

- can be characterized by:
  - The type of operations used for transforming plaintext to ciphertext
    - substitution / transposition / product
  - The number of keys used
    - symmetric (single key)
    - asymmetric (two-keys, or public-key encryption)
  - way in which plaintext is processed
    - block / stream

# Types of Cryptanalytic Attacks

- **ciphertext only**
  - only known algorithm / ciphertext, statistically, can identify plaintext
- **known plaintext**
  - known algorithm/ plaintext & ciphertext  pairs to attack cipher
- **chosen plaintext**
  - known algorithm/ ciphertext to be decoded/chosen plaintext/its corresponding ciphertext
- **chosen ciphertext**
  - known algorithm / purported ciphertext chosen/its corresponding decrypted plaintext
- **chosen text**

**- chosen plaintext** + Purported ciphertext chosen + corresponding decrypted plaintext by generated by secret key

# Average time required for exhaustive key search (brute force approach)

| Key Size (bits) | Number of Alternative Keys | Time required at 1 encription/us | Time required at $10^6$ Decryption/µs |
|---|---|---|---|
| 32 | $2^{32} = 4.3 \times 10^9$ | $2^{31}$ us = 35.8 minutes | 2.15 milliseconds |
| 56 | $2^{56} = 7.2 \times 10^{16}$ | $2^{55}$ us = 1142 years | 10.01 hours |
| 128 | $2^{128} = 3.4 \times 10^{38}$ | $2^{127}$ us = $5.4 \times 10^{24}$ years | $5.4 \times 10^{18}$ years |
| 168 | $2^{168} = 3.7 \times 10^{50}$ | $2^{167}$ us = $5.9 \times 10^{36}$ years | $5.9 \times 10^{30}$ years |
| 26 characters | $26! = 4 \times 10^{26}$ | $2 \times 10^{26}$ us = $6.4 \times 10^{12}$ years | $6.4 \times 10^6$ years |

# More Definitions

- **unconditional security**
  - no matter how much computer power is available, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext
- **computational security**
  - given limited computing resources (e.g., time needed for calculations is greater than age of universe), the cipher cannot be broken

# Computationally Secure

- The cost of breaking the cipher exceeds the value of the encrypted information

- The time required to break the cipher exceeds the useful lifetime of the information

# Types of Ciphers

- *Substitution(대체)* ciphers
- *Permutation* (or *transposition: 치환*) ciphers
- Product ciphers (or product system : 생성시스템)

# Classical Substitution Ciphers

- where letters of plaintext are replaced by other letters or by numbers or symbols
- or if plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns

# Caesar Cipher

- earliest known substitution cipher by Julius Caesar (?)
- first attested use in military affairs
- replaces each letter by 3rd letter on
- example:

```
meet me after the toga party
PHHW PH DIWHU WKH WRJD SDUWB
```

- What's the key?

# Caesar Cipher

- can define transformation as:

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |

- mathematically give each letter a number

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | b | c | d | e | f | g | h | i | j | k | l | m |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| n | o | p | q | r | s | t | u | v | w | x | y | Z |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

- then have Caesar cipher (using modular arithmetic) as:

$$C = \mathrm{E}(p) = (p + k) \bmod (26)$$

$$p = \mathrm{D}(\mathrm{C}) = (\mathrm{C} - k) \bmod (26)$$

| Decryption shift | Candidate plaintext |
|---|---|
| 0 | exxegoexsrgi |
| 1 | dwwdfndwrqfh |
| 2 | cvvcemcvqpeg |
| 3 | buubdlbupodf |
| 4 | attackatonce |
| 5 | zsszbjzsnmbd |
| 6 | yrryaiyrmlac |
| ... | |
| 23 | haahjrhavujl |
| 24 | gzzgiqgzutik |
| 25 | fyyfhpfytshj |

# Cryptanalysis of Caesar Cipher

- only have 26 possible ciphers
  - A maps to A,B,..Z
- could simply try each in turn
- a **brute force search**
- given ciphertext, just try all shifts of letters
- e.g., break ciphertext "GCUA VQ DTGCM"

# Polyalphabetic Ciphers

- another approach to improving security is to use multiple cipher alphabets
- called **polyalphabetic substitution ciphers**
- makes cryptanalysis harder with more alphabets to guess and flatter frequency distribution
- use a key to select which alphabet is used for each letter of the message
- use each alphabet in turn
- repeat from start after end of key is reached

# Vigenère Cipher

- simplest polyalphabetic substitution cipher is the **Vigenère Cipher**
- effectively multiple caesar ciphers
- key is multiple letters long K = k1 k2 ... kd
- $i^{th}$ letter specifies $i^{th}$ alphabet to use
- use each alphabet in turn
- repeat from start after d letters in message
- decryption simply works in reverse

# Example

- write the plaintext out
- write the keyword repeated above it
- use each key letter as a caesar cipher key
- encrypt the corresponding plaintext letter
- eg using keyword *deceptive*

```
key:        deceptivedeceptivedeceptive
plaintext:  wearediscoveredsaveyourself
ciphertext:ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

# One-Time Pad

- if a truly random key as long as the message is used, the cipher will be secure
- called a One-Time Pad
- is unbreakable since ciphertext bears no statistical relationship to the plaintext
- since for **any plaintext** & **any ciphertext** there exists a key mapping one to other
- can only use the key **once** though
- have problem of safe distribution of key

# Transposition Ciphers

- now consider classical **transposition** or **permutation** ciphers
- these hide the message by rearranging the letter order
- without altering the actual letters used
- can recognise these since have the same frequency distribution as the original text

# Rail Fence cipher

- write message letters out diagonally over a number of rows
- then read off cipher row by row
- eg. write message out as:

```
m e m a t r h t g p r y
 e t e f e t e o a a t
```

- giving ciphertext

```
MEMATRHTGPRYETEFETEOAAT
```

# Product Ciphers

- ciphers using substitutions or transpositions are not secure because of language characteristics
- hence consider using several ciphers in succession to make harder, but:
  - two substitutions make a more complex substitution
  - two transpositions make more complex transposition
  - but a substitution followed by a transposition makes a new much harder cipher
- this is bridge from classical to modern ciphers

# Steganography

- an alternative to encryption
- hides existence of message
  - using only a subset of letters/words in a longer message marked in some way
  - using invisible ink
  - hiding in LSB in graphic image or sound file
- has drawbacks
  - high overhead to hide relatively few info bits

# steganography : 메시지가 전송되고 있다는 사실을 숨기는 기술 (정보은닉)

# Summary

- have considered:
  - classical cipher techniques and terminology
  - cryptanalysis using letter frequencies
  - polyalphabetic ciphers
  - transposition ciphers
  - product ciphers and rotor machines
  - stenography