Chapter 2 Classical Encryption Techniques

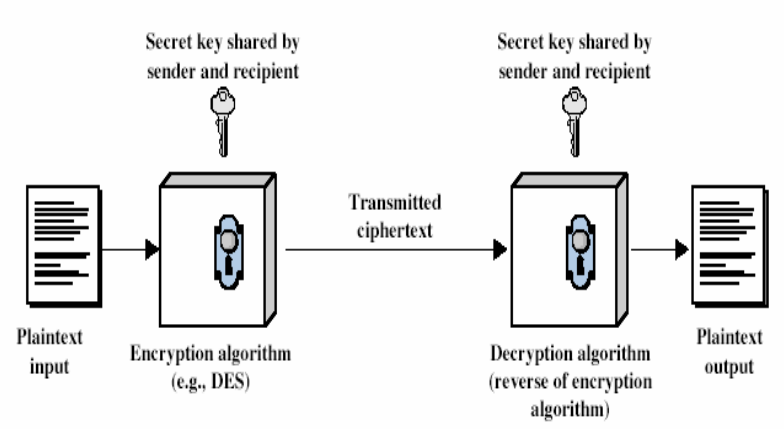
Cryptography and Network Security:
Principles and Practices (3rd Ed)

2.1 Symmetric Cipher Model

- Symmetric Encryption
  - or conventional/ private-key/ single-key
  - sender and recipient share a common key
  - all classical encryption algorithms are private-key
  - was only type prior to invention of public-key in 1970's.
  - Examples
    - DES
    - AES (Rijandel)

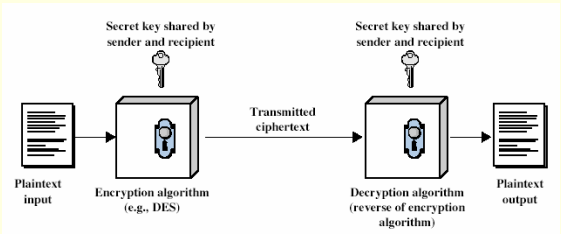
2.1 Symmetric Cipher Model

- Symmetric Cipher Model [Fig. 2.1]



2.1 Symmetric Cipher Model

- Basic Terminology
  - **plaintext** - the original message.
  - **ciphertext** - the coded message.
  - **cipher** - algorithm for transforming plaintext to ciphertext.
  - **key** - info used in cipher known only to sender/receiver.
  - **encipher (encrypt)** - converting plaintext to ciphertext.
  - **decipher (decrypt)** - recovering ciphertext from plaintext.



2.1 Symmetric Cipher Model

- **cryptography** - the 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.

2.1 Symmetric Cipher Model

- 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.
  - *Kerckhoffs' Assumption [1883]: Encryption transformations being used be publicly known* and that *the security of the system should reside only in the key chosen.*
- Implies a secure channel to distribute key.

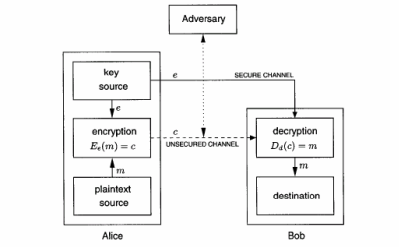


Figure 1.7: *Two-party communication using encryption, with a secure channel for key exchange. The decryption key d can be efficiently computed from the encryption key e.*

2.1 Symmetric Cipher Model

- Cryptographic Systems are characterized alone three independent dimensions
  - type of encryption operations used
    - Substitution
    - Transposition
    - Product
  - Number of keys used
    - Single-key or private
    - Two-key or public
  - Way in which plaintext is processed
    - Block
    - Stream

2.1 Symmetric Cipher Model

- Types of Cryptanalytic Attacks
  - **ciphertext only**
    - only know algorithm / ciphertext, statistical, can identify plaintext
  - **known plaintext**
    - know/suspect plaintext & ciphertext to attack cipher
  - **chosen plaintext**
    - select plaintext and obtain ciphertext to attack cipher
  - **chosen ciphertext**
    - select ciphertext and obtain plaintext to attack cipher
  - **chosen text**
    - select either plaintext or ciphertext to en/decrypt to attack cipher

2.1 Symmetric Cipher Model

- Table 2.1 **Types of Attacks on Encrypted Messages**

Type of Attack	Known to Cryptanalyst
Ciphertext only	•Encryption algorithm •Ciphertext to be decoded
Known plaintext	•Encryption algorithm •Ciphertext to be decoded •One or more plaintext-ciphertext pairs formed with the secret key
Chosen plaintext	•Encryption algorithm •Ciphertext to be decoded •Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen ciphertext	•Encryption algorithm •Ciphertext to be decoded •Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen text	•Encryption algorithm •Ciphertext to be decoded •Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key •Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

2.1 Symmetric Cipher Model

- Brute Force Search
  - always possible to simply try every key
  - most basic attack, proportional to key size
  - assume either know / recognise plaintext

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

2.1 Symmetric Cipher Model

- Kinds of Security
  - **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 (*eg time needed for calculations is greater than age of universe*), the cipher cannot be broken.

2.2 Substitution Techniques

- Caesar Cipher (凱撒加密法)
  - 已知最早的加密法，傳為凱撒大帝所提的。
  - 問題: 如何把英文字母變成數字?
  - 加密規則: replaces each letter by 3rd letter on
  - 解密規則?
  - Example:

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

2.2 Substitution Techniques

- 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
- Define Caesar cipher as:
  - $C = \mathrm{E}(p) = (p + k) \bmod (26)$
  - $p = \mathrm{D}(\mathrm{C}) = (\mathrm{C} - k) \bmod (26)$

2.2 Substitution Techniques

- 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
    - do need to recognize when have plaintext
    - eg. break ciphertext "GCUA VQ DTGCM"

2.2 Substitution Techniques

- 重要觀念
  - Large key space: 所有可能秘密金匙的個數要夠多，至少不能被用電腦以暴力攻擊法所猜到。
  - Example: SSL採用128位元的秘密金匙。
  - Problem:採用128位元的SSL，其秘密金匙的個數多少個?

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