Chapter Two

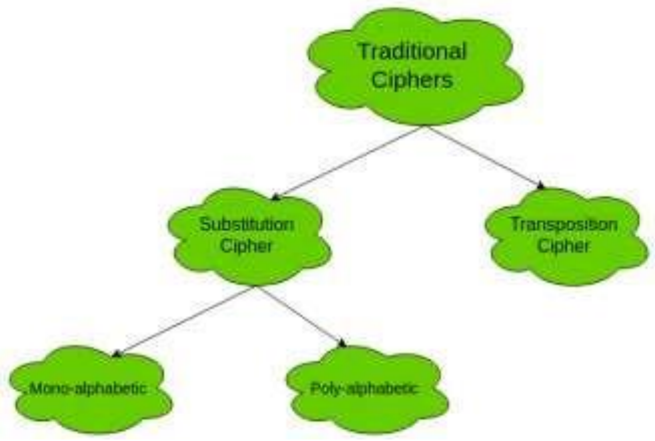
CLASSICAL ENCRYPTION TECHNIQUES

Cryptography Classification

The old Encryption and Decryption techniques before the implementation of computer systems are called Classical techniques, while those invented and implemented for the computer systems are called modern techniques. However, cryptography system (whether Classical or Modern) are generally classified along three independent dimensions:

1- The **type of operations** used for transforming plaintext to cipher text. All encryption algorithm are based on general principle:

- Substitution
- Transposition



2- The **number of keys** used.

(a) **Symmetric:** If the same key is used by both, the sender and the receiver for encryption and decryption. It might be also called **Single key, Secret key, or Conventional encryption.**

(b) **Asymmetric:** If the sender and receiver, each were using different keys, usually two sets of keys, one for encryption and the other for decryption.

3- The **way,** in which the plaintext is processed.

- **Block cipher**: The input message is divided in blocks of elements and each block is processes at a time, producing an output block for each input block.
- **Stream cipher**: The input elements are processed individually, producing an output as one element at a time, too.

Symmetric Cipher Model:

All traditional schemes are symmetric / single key / private-key encryption algorithms, with a single key, used for both encryption and decryption, since both sender and receiver are equivalent, either can encrypt or decrypt messages using that common key.

However, there are hundreds of traditional methods for information security which all employ (1) **Substitution** or (2) **Transposition** techniques (or both), however, they can be categorized into only two techniques, symmetric and asymmetric systems, which are well suited and implemented for computer system applications, which will be studied during the course.

The basic terminology used:

- **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
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (code breaking)** - the study of principles/ methods of deciphering ciphertext *without* knowing key

- **cryptology** - the field of both cryptography and cryptanalysis

A simplified model of conventional encryption/decryption system is shown in figure 2-2.

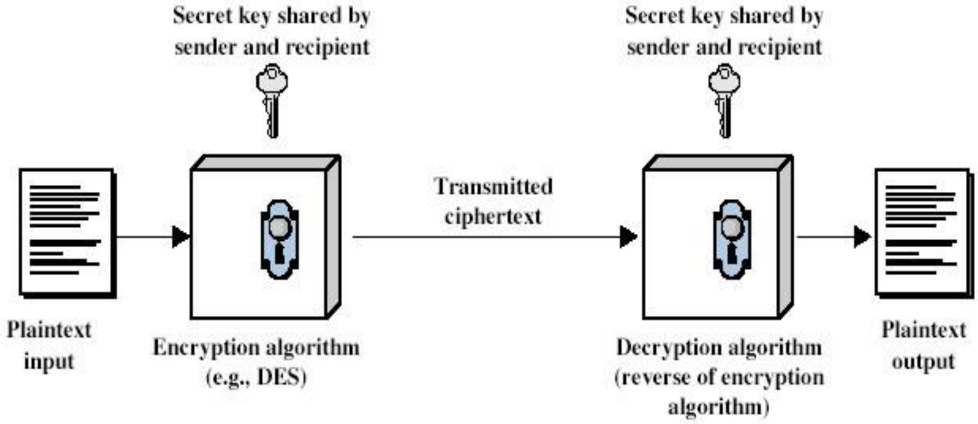

Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Fig. 2-2 simplified cipher model

Requirements:

Two requirements for secure use of symmetric encryption:

1. a strong encryption **algorithm**
2. a secret **key** known only to sender / receiver

Generally one assumes that the algorithm is known. This allows easy distribution of s/w and h/w implementations and hence assume just keeping **key secret** is sufficient to secure encrypted messages.

Having plaintext X, ciphertext Y, secret key k, encryption algorithm E_k and decryption algorithm D_k , the calculation involve

$C = E_k(Y)$ and $X = D_K(Y)$

This implies the need for secure channel to distribute key.

Substitution Techniques:

A substitution technique is one in which the letters of plaintext are replaced by other letters or numbers or symbols. But, if plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.

Few security techniques will be considered here as examples for substitution cipher.

1. Caesar Cipher:

Substitution ciphers form the first of the fundamental building blocks. The core idea is to replace one basic unit (letter/byte) with another. Whilst the early Greeks described several substitution ciphers, the first attested use in military affairs of one was by Julius Caesar, described by him in *Gallic Wars* (cf. Kahn pp83-84). Still any cipher using a simple letter shift is called **Caesar cipher**, not just those with shift **3**.

Caesar cipher involves replacing each letter of the alphabet with a letter standing 3 places further down the alphabet. Therefore the alphabet transformation sets for plain and cipher are:

PLAIN:

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

Cipher:

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

***Example 1*.**

Encipher the message: Plaintext = "**COME HERE**" by Caesar cipher. Solution: Ciphertext = "**FRPH KHUH**"

Example 2..

Plaintext = "**MEET ME AFTER THE TOGA PARTY**"
Ciphertext = "**PHHW PH DIWHU WKH WRJD SDUWB**"

This mathematical description uses **modulo arithmetic** (i.e. clock arithmetic). Here, when you reach **Z** you go back to **A** and start again. Mod **26** implies that when you reach **26**, you use **0** instead (i.e. the letter after **Z**, or **25 + 1** goes to A or 0).

Mathematically, if we assign a numerical equivalent to each letter (a=1, b=2, etc.), i.e.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Then the algorithm can be expressed as follow: For each plaintext letter p, substitute the cipher text letter C:

$$C = E(p) = (p + 3) \bmod (26)$$

A shift may be of any value **k**, so that the general Caesar algorithm is

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

Where **k** takes on a value in the range 1 to 25.

The Decryption algorithm is simply $p = D(C) = (C - \mathbf{k}) \bmod (26)$