

Computer Systems Security

Dr. Ayman Abdel-Hamid

College of Computing and Information Technology

Arab Academy for Science & Technology and
Maritime Transport

Chapter 2

Classical Encryption Techniques

Outline

- Classical Encryption Techniques

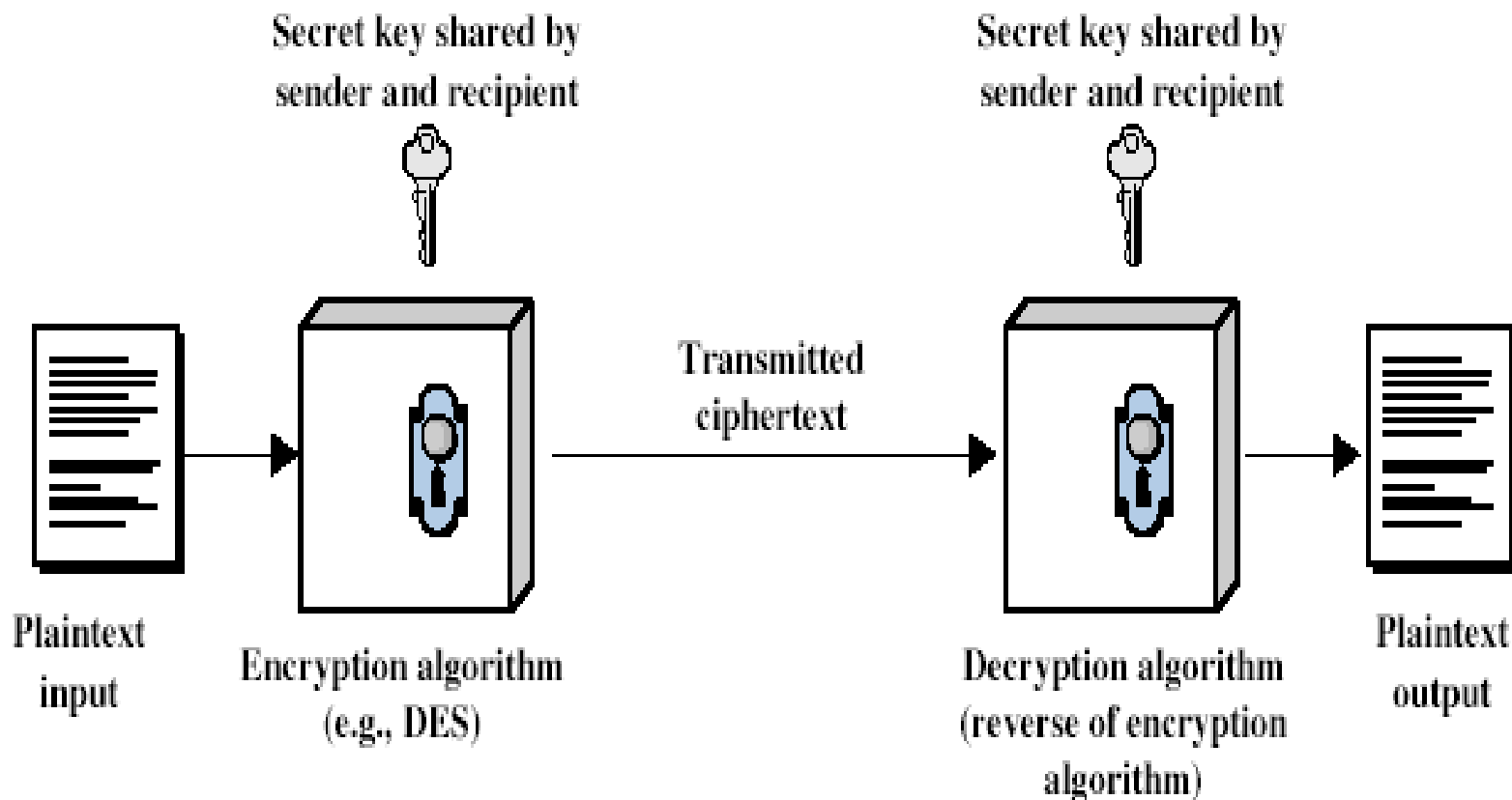
Symmetric Encryption

- 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

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
- **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 ^{1/2}

- two requirements for secure use of symmetric encryption:
 - a strong encryption algorithm (if you know the algorithm, and have access to one or more ciphertexts, you are unable to decipher or figure out key, **stronger?**)
 - 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

Requirements ^{2/2}

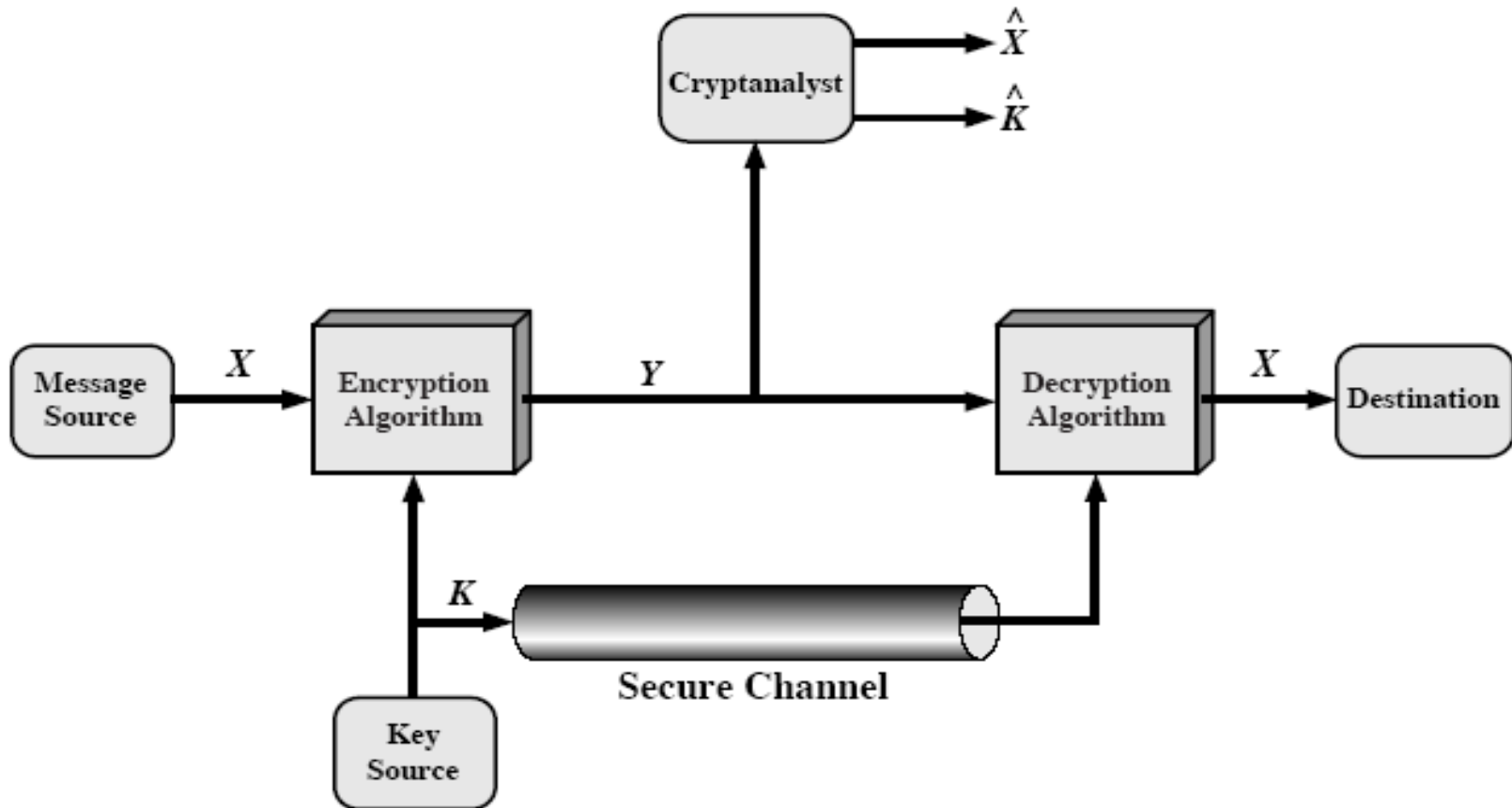


Figure 2.2 Model of Symmetric Cryptosystem

Cryptography

- can characterize by:
 - type of encryption operations used
 - substitution / transposition / product (multiple stages)
 - number of keys used
 - single-key or private or secret-key (symmetric)
 - two-key or public (asymmetric)
 - way in which plaintext is processed
 - block (1 output block for each input block)
 - Stream (one element at time)

How to attack secret-key Encryption?

- **Cryptanalysis**
 - Relies on nature of algorithm and may be knowledge of properties of plain text or even knowledge of sample plaintext-ciphertext pairs
- **Brute-force Attack**
 - Attempt every possible key on a ciphertext until an intelligible translation into plaintext is obtained

Types of Cryptanalytic Attacks

- **ciphertext only**
 - only know algorithm / ciphertext, *statistical (general idea about type of plaintext)*, 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

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 (no matter how much ciphertext is available)
- **computational security**
 - Cost of breaking the cipher exceeds the value of encrypted information
 - Time required to break the cipher exceeds the useful lifetime of the information

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/ μ s	Time required at 10^6 encryptions/ μ s
32		$2^{32} = 4.3 \times 10^9$	$2^{31} \mu\text{s} = 35.8$ minutes	2.15 milliseconds
56	DES	$2^{56} = 7.2 \times 10^{16}$	$2^{55} \mu\text{s} = 1142$ years	10.01 hours
128	AES	$2^{128} = 3.4 \times 10^{38}$	$2^{127} \mu\text{s} = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	3 DES	$2^{168} = 3.7 \times 10^{50}$	$2^{167} \mu\text{s} = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)		$26! = 4 \times 10^{26}$	$2 \times 10^{26} \mu\text{s} = 6.4 \times 10^{12}$ years	6.4×10^6 years

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 ^{1/2}

- 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

Caesar Cipher ^{2/2}

- 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 as:

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

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

Cryptanalysis of Caesar Cipher

- only have 26 possible ciphers
 - A maps to A,B,..Z (A to A is not really secure)
- could simply try each in turn
- a **brute force search** (encryption/decryption algorithms known, only 25 keys to try, and language of plaintext is known and recognized)
- given ciphertext, just try all shifts of letters
- do need to recognize when have plaintext
- e.g., break ciphertext "GCUA VQ DTGCM"

Monoalphabetic Cipher

- rather than just shifting the alphabet
- could shuffle (jumble) the letters arbitrarily
- *Monoalphabetic substitution cipher* (a single cipher alphabet is used per message)
- hence key is 26 letters long

Plain: abcdefghijklmnopqrstuvwxyz

Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext: ifwewishtoreplaceletters

Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA

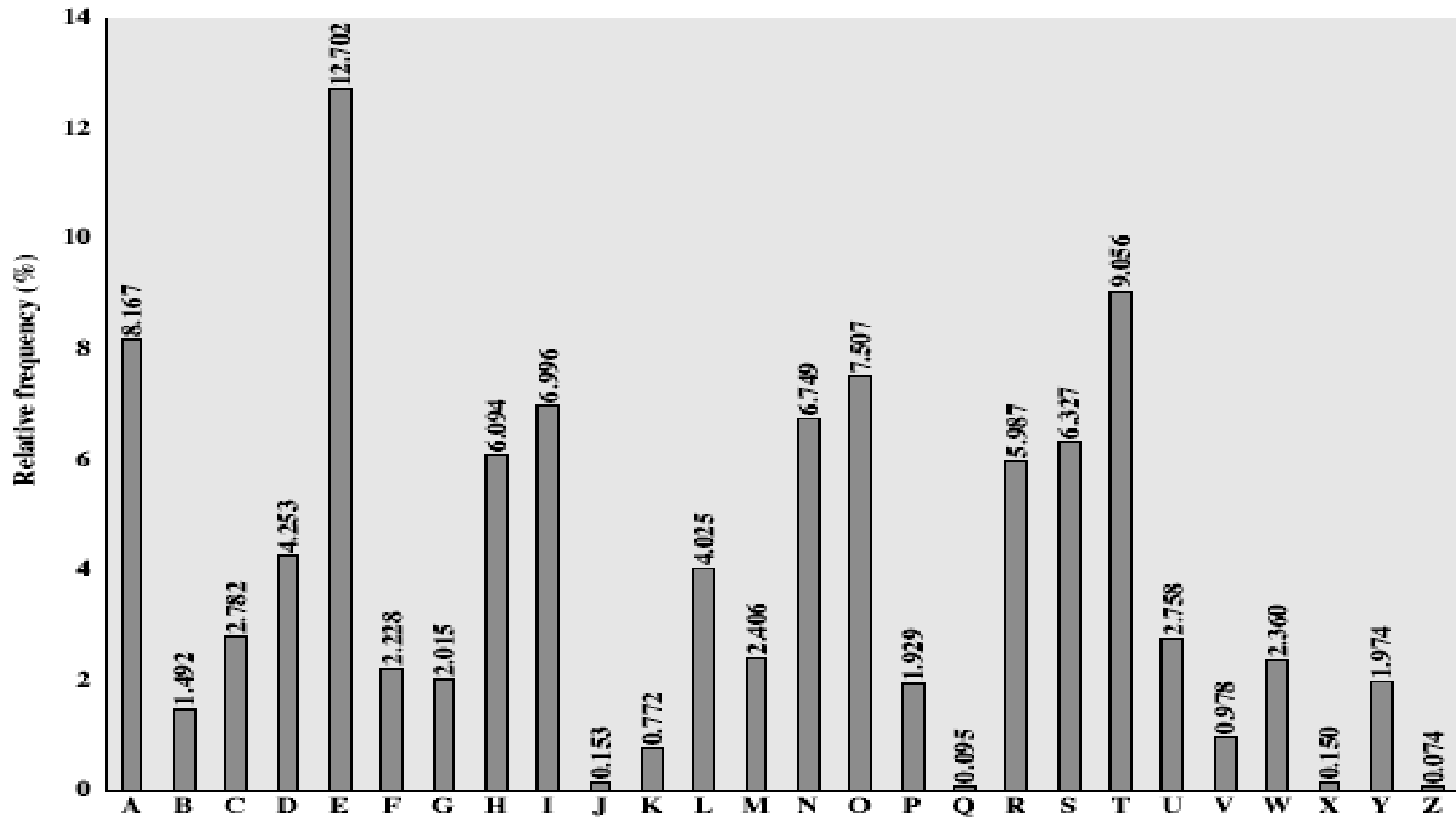
Monoalphabetic Cipher Security

- now have a total of $26! = 4 \times 10^{26}$ keys
- with so many keys, might think is secure
- but would be **!!!WRONG!!!**
- problem is language characteristics

Language Redundancy and Cryptanalysis

- human languages are **redundant**
- eg "th lrd s m shphrd shll nt wnt"
- letters are not equally commonly used
- in English **e** is by far the most common letter
- then T,R,N,I,O,A,S
- other letters are fairly rare
- cf. Z,J,K,Q,X
- have tables of single, double & triple letter frequencies

English Letter Frequencies



Use in Cryptanalysis

- key concept - monoalphabetic substitution ciphers do not change relative letter frequencies
- discovered by Arabian scientists in 9th century
- calculate letter frequencies for ciphertext
- compare counts/plots against known values

Example Cryptanalysis

- given ciphertext:

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ  
VUEPHZHMDZSHZOWSFPAPDTSVPQUZWYMXUZUHSX  
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
```

- count relative letter frequencies (see text)
- guess P & Z are e and t
- guess ZW is th and hence ZWP is the
- proceeding with trial and error finally get:
it was disclosed yesterday that several informal but
direct contacts have been made with political
representatives of the viet cong in moscow

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
- e.g., 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
```

Row Transposition Ciphers

- a more complex scheme
- write letters of message out in rows over a specified number of columns
- then reorder the columns according to some key before reading off the rows

Key: 4 3 1 2 5 6 7

Plaintext: a t t a c k p

o s t p o n e

d u n t i l t

w o a m x y z

Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

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 a 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