

# Cybersecurity Concepts

Prepared by Dr. Diaa Salama

FNT625  
Classical Encryption Techniques

## Lecture 5





مجموعة جامعة  
الجميع الذكية  
للتعليم القابضة

MIDOCEAN  
UNIVERSITY

# Cybersecurity Concepts

## Lecture 5

FNT625  
Classical Encryption Techniques

Prepared by  
**Dr. Diao Salama**

[www.midocean.ae](http://www.midocean.ae)

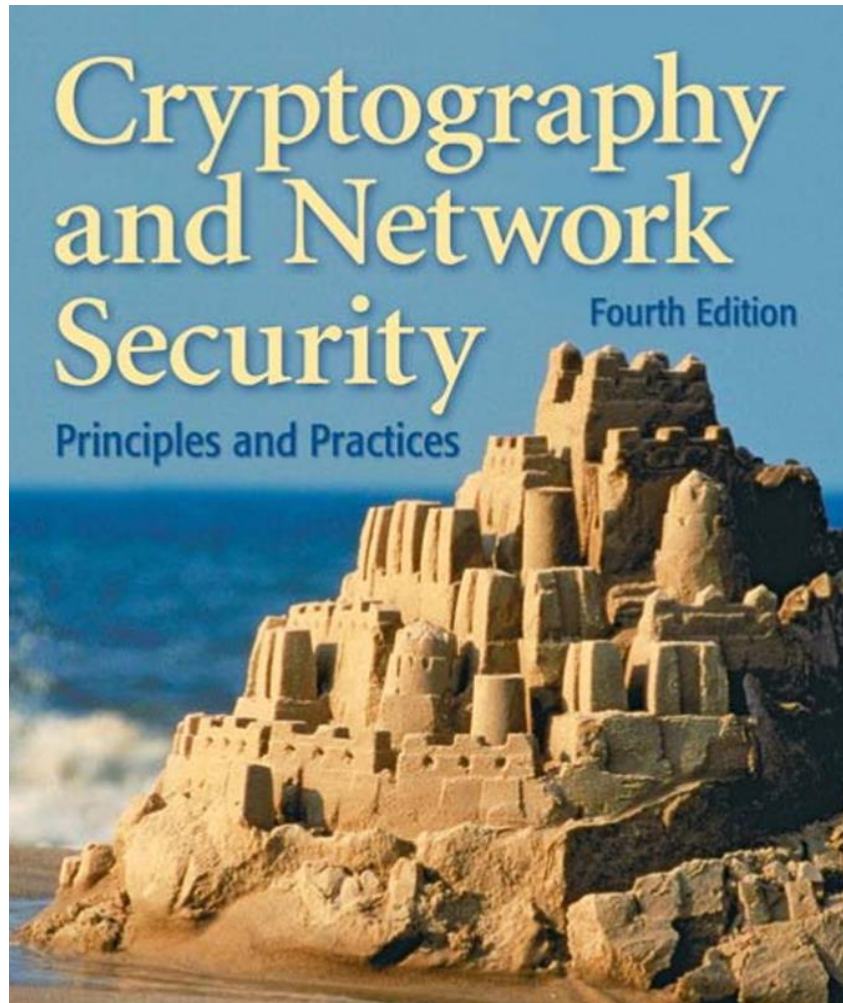
---

**PLEASE**  
BE QUIET



10





**Book Title:**

Cryptography and Network Security

**Authors:**

William Stallings

**Publisher:**

Pearson Education, Inc.

**Edition:**

Seven edition

Lecture

05

Lets Start the Fifth Lecture

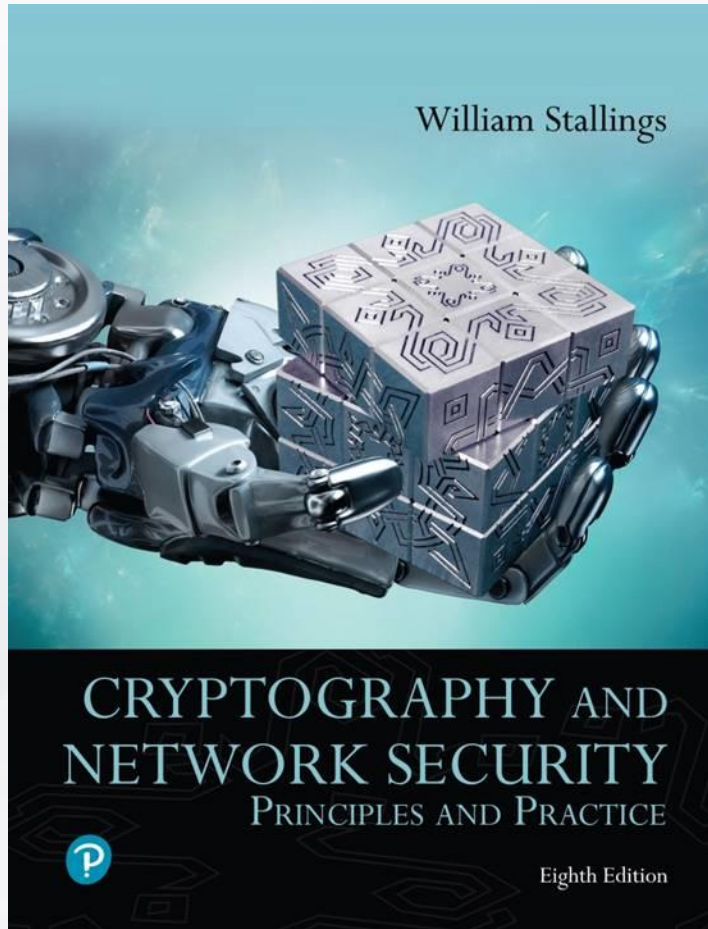


# Classical Encryption Techniques



# Cryptography and Network Security: Principles and Practice

Eighth Edition



## Chapter 3

### Classical Encryption Techniques

**Symmetric Encryption**

**Substitution Techniques**

**Caesar Cipher**

**Monoalphabetic Cipher**

**Playfair Cipher**

Hill Cipher

**Symmetric Encryption**

**Substitution Techniques**

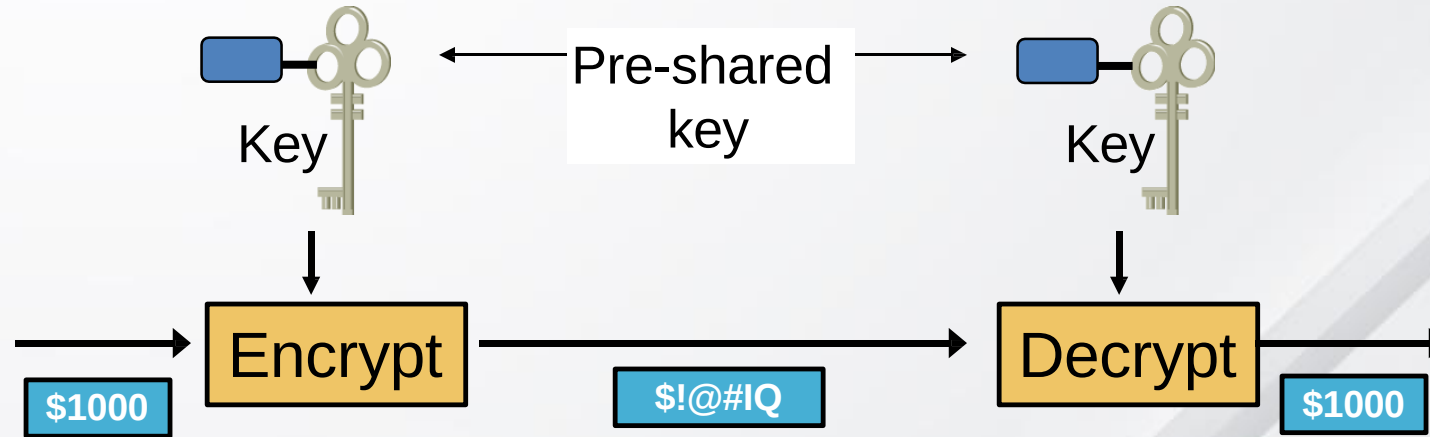
**Caesar Cipher**

**Monoalphabetic Cipher**

**Playfair Cipher**

Hill Cipher

# Symmetric Encryption



- ❑ Best known as shared-secret key algorithms
- ❑ The usual key length is 80 - 256 bits
- ❑ A sender and receiver must share a secret key
- ❑ Faster processing because they use simple mathematical operations.
- ❑ Examples include DES, 3DES, AES, IDEA, RC2/4/5/6, and Blowfish.

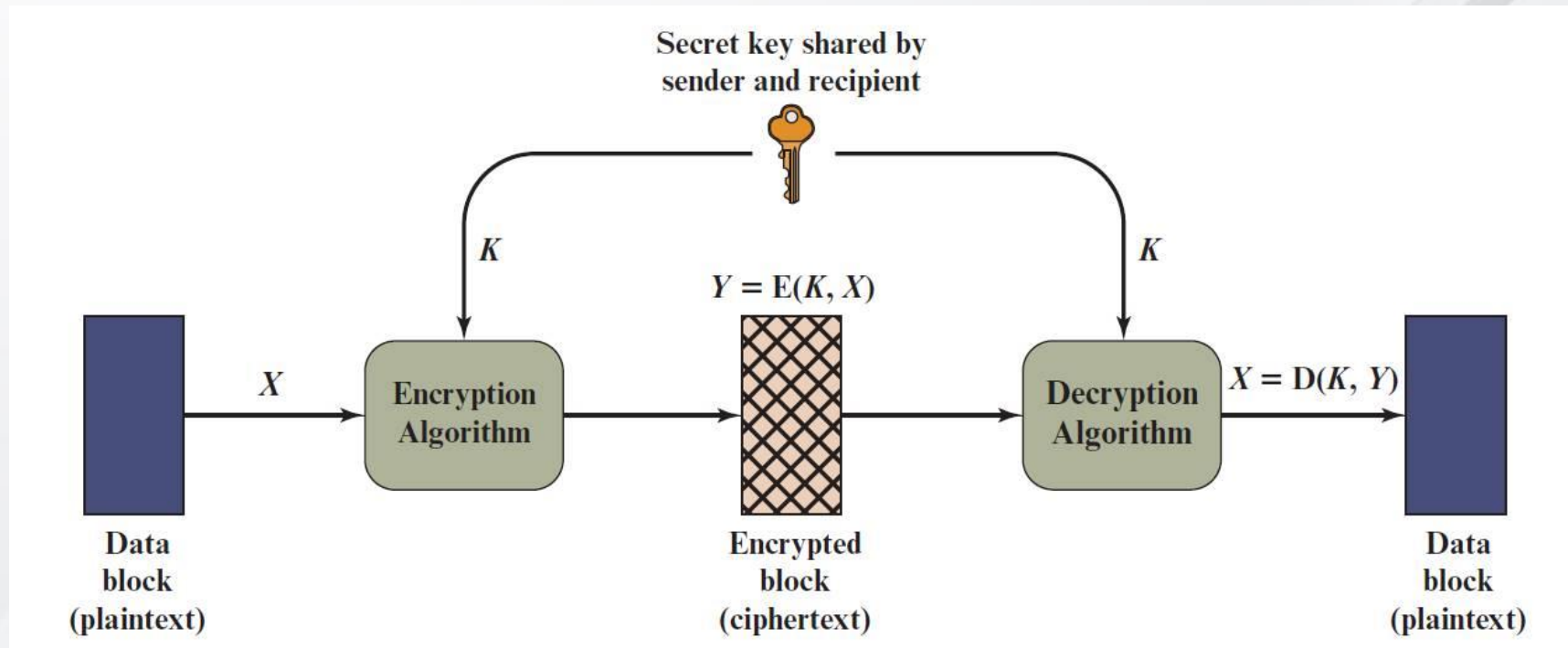
# Definitions (1 of 2)

- Plaintext
  - An original message
- Ciphertext
  - The coded message
- Enciphering/encryption
  - The process of converting from plaintext to ciphertext
- Deciphering/decryption
  - Restoring the plaintext from the ciphertext

## Definitions (2 of 2)

- Cryptography
  - The area of study of the many schemes used for encryption
- Cryptographic system/cipher
  - A scheme
- Cryptanalysis
  - Techniques used for deciphering a message without any knowledge of the enciphering details
- Cryptology
  - The areas of cryptography and cryptanalysis

## Figure 3.1 Simplified Model of Symmetric Encryption

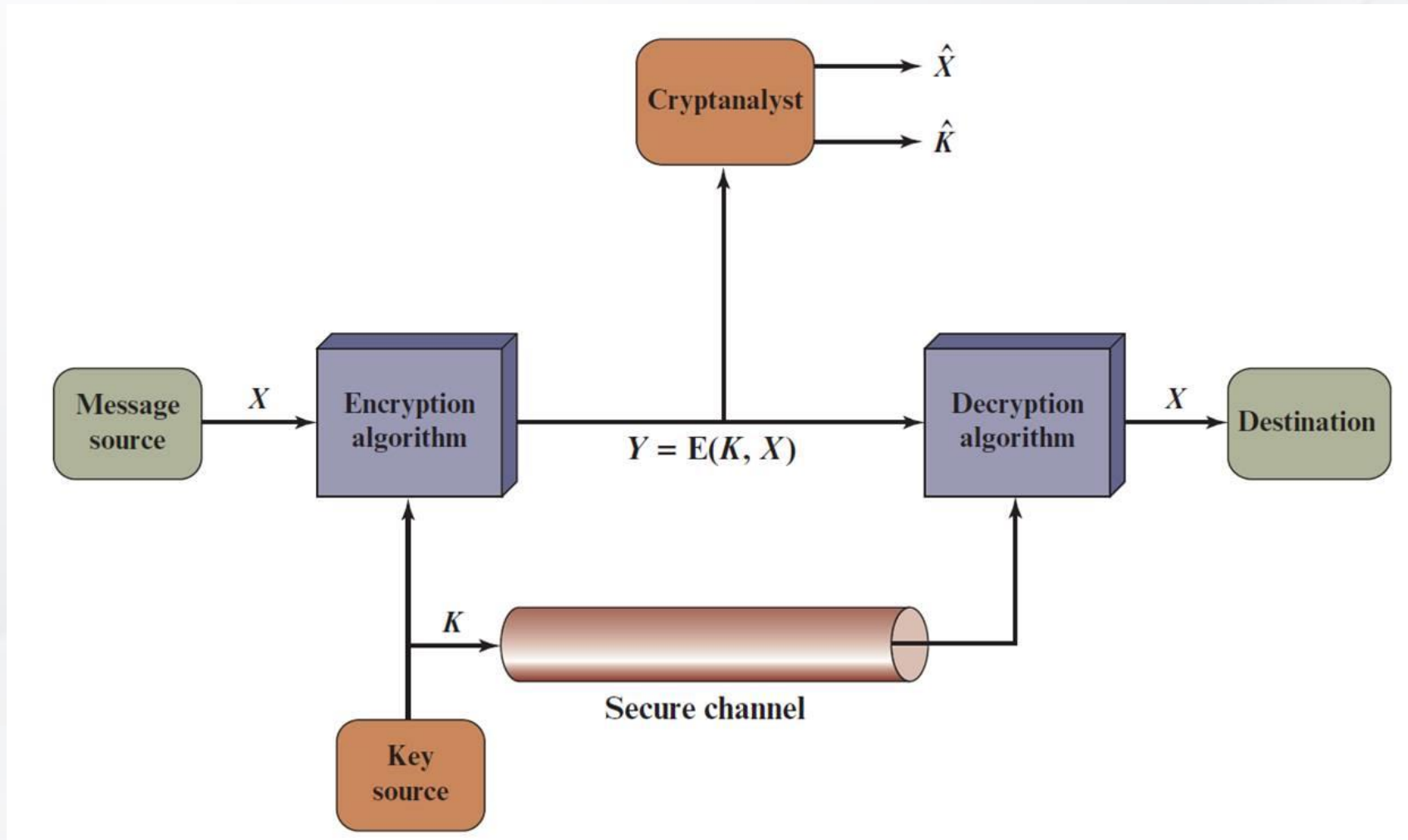


# Symmetric Cipher Model

- There are two requirements for secure use of conventional encryption:
  - A strong encryption algorithm
  - Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure



# Figure 3.2 Model of Symmetric Cryptosystem



# Cryptographic Systems

- Characterized along **three** independent dimensions:
  - **The type of operations used for transforming plaintext to ciphertext**
    - Substitution
    - Transposition
  - **The number of keys used**
    - Symmetric, single-key, secret-key, conventional encryption
    - Asymmetric, two-key, or public-key encryption
  - **The way in which the plaintext is processed**
    - Block cipher
    - Stream cipher

# Cryptanalysis and Brute-Force Attack

- **Cryptanalysis**
  - Attack relies on the nature of the algorithm plus some knowledge of the general characteristics of the plaintext
  - Attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used
- **Brute-force attack**
  - Attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained
  - On average, half of all possible keys must be tried to achieve success

# Brute-Force Attack

- Involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained
- On average, half of all possible keys must be tried to achieve success
- To supplement the brute-force approach, some degree of knowledge about the expected plaintext is needed, and some means of automatically distinguishing plaintext from garble is also needed

## Table 3.1 Types of Attacks on Encrypted Messages

| Type of Attack    | Known to Cryptanalyst                                                                                                                                                                                                                                                                                                                                   |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ciphertext Only   | <ul style="list-style-type: none"><li>• Encryption algorithm</li><li>• Ciphertext</li></ul>                                                                                                                                                                                                                                                             |
| Known Plaintext   | <ul style="list-style-type: none"><li>• Encryption algorithm</li><li>• Ciphertext</li><li>• One or more plaintext–ciphertext pairs formed with the secret key</li></ul>                                                                                                                                                                                 |
| Chosen Plaintext  | <ul style="list-style-type: none"><li>• Encryption algorithm</li><li>• Ciphertext</li><li>• Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key</li></ul>                                                                                                                                |
| Chosen Ciphertext | <ul style="list-style-type: none"><li>• Encryption algorithm</li><li>• Ciphertext</li><li>• Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key</li></ul>                                                                                                                              |
| Chosen Text       | <ul style="list-style-type: none"><li>• Encryption algorithm</li><li>• Ciphertext</li><li>• Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key</li><li>• Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key</li></ul> |

# Encryption Scheme Security

- Unconditionally secure
  - No matter how much time an opponent has, it is impossible for him or her to decrypt the ciphertext simply because the required information is not there
- 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



# Strong Encryption

- The term *strong encryption* refers to encryption schemes that make it impractically difficult for unauthorized persons or systems to gain access to plaintext that has been encrypted
- Properties that make an encryption algorithm strong are:
  - Appropriate choice of cryptographic algorithm
  - Use of sufficiently long key lengths
  - Appropriate choice of protocols
  - A well-engineered implementation
  - Absence of deliberately introduced hidden flaws

**Symmetric Encryption**

**Substitution Techniques**

**Caesar Cipher**

**Monoalphabetic Cipher**

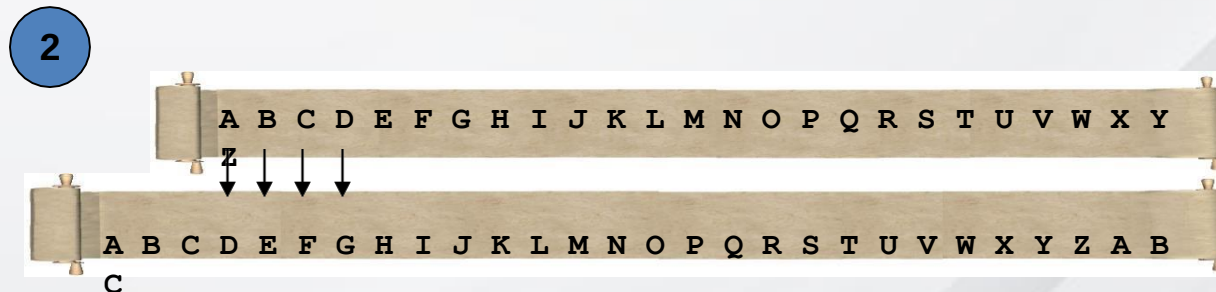
**Playfair Cipher**

**Hill Cipher**

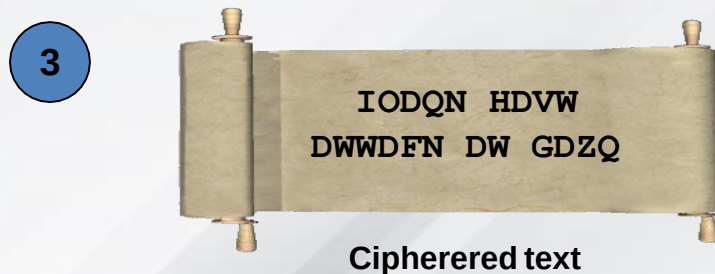
# Substitution Techniques



The clear text message would be encoded using a key of 3.



Shift the top scroll over by three characters (key of 3), an A becomes D, B becomes E, and so on.



The clear text message would be encrypted as follows using a key of 3.

# Substitution Techniques

- ☐ Caesar Cipher
- ☐ Monoalphabetic Ciphers
- ☐ Playfair Cipher
- ☐ Hill Cipher
- ☐ Polyalphabetic Ciphers
- ☐ Vigenère Cipher
- ☐ Autokey Cipher
- ☐ Vernam Cipher

**Symmetric Encryption**

**Substitution Techniques**

**Caesar Cipher**

**Monoalphabetic Cipher**

**Playfair Cipher**

Hill Cipher

# Caesar Cipher

- Simplest and earliest known use of a substitution cipher
- Used by Julius Caesar
- Involves replacing each letter of the alphabet with the letter standing three places further down the alphabet
- Alphabet is wrapped around so that the letter following Z is A

plain: meet me after the toga party

cipher: PHHW PH DIWHU WKH WRJD SDUWB

# Caesar Cipher Algorithm

- 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 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

- Algorithm can be expressed as:

$$c = E(3, p) = (p + 3) \bmod (26)$$

- A shift may be of any amount, so that the general Caesar algorithm is:

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

- Where k takes on a value in the range 1 to 25; the decryption algorithm is simply:

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

# Caesar Cipher Algorithm

- 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

- <https://www.101computing.net/caesar-shift-substitution-cipher/>

| Key                   | +5                |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |  |  |  |  |
|-----------------------|-------------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|--|--|--|--|
| Plain text alphabet:  | A                 | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |  |  |  |  |
|                       | Shift by 5 places |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |  |  |  |  |
| Cipher text alphabet: | F                 | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |  |  |  |  |

# Caesar Cipher Algorithm

- **Example: 1** Use the Caesar cipher to encrypt and decrypt the message "JAVATPOINT," and the key (shift) value of this message is 3.
- **Encryption**
- We apply encryption formulas by character, based on alphabetical order.
- The formula of encryption is:
- $En(x) = (x + n) \bmod 26$

|    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 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  |
| 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

# Caesar Cipher Algorithm

- Solution :**

|    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 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  |
| 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

|                   |                          |                    |
|-------------------|--------------------------|--------------------|
| Plaintext: J → 09 | $E_n: (09 + 3) \bmod 26$ | Ciphertext: 12 → M |
| Plaintext: A → 00 | $E_n: (00 + 3) \bmod 26$ | Ciphertext: 3 → D  |
| Plaintext: V → 21 | $E_n: (21 + 3) \bmod 26$ | Ciphertext: 24 → Y |
| Plaintext: A → 00 | $E_n: (00 + 3) \bmod 26$ | Ciphertext: 3 → D  |
| Plaintext: T → 19 | $E_n: (19 + 3) \bmod 26$ | Ciphertext: 22 → W |
| Plaintext: P → 15 | $E_n: (15 + 3) \bmod 26$ | Ciphertext: 18 → S |
| Plaintext: O → 14 | $E_n: (14 + 3) \bmod 26$ | Ciphertext: 17 → R |
| Plaintext: I → 08 | $E_n: (08 + 3) \bmod 26$ | Ciphertext: 11 → L |
| Plaintext: N → 13 | $E_n: (13 + 3) \bmod 26$ | Ciphertext: 16 → Q |
| Plaintext: T → 19 | $E_n: (19 + 3) \bmod 26$ | Ciphertext: 22 → W |

The encrypted message is "MDYDWSRLQW". Note that the Caesar cipher is monoalphabetic, so the same plaintext letters are encrypted as the same letters. For example, "JAVATPOINT" has "A", encrypted by "D".

# Caesar Cipher Algorithm

- Solution :**

|    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 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  |
| 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

|                   |                          |                    |
|-------------------|--------------------------|--------------------|
| Plaintext: J → 09 | $E_n: (09 + 3) \bmod 26$ | Ciphertext: 12 → M |
| Plaintext: A → 00 | $E_n: (00 + 3) \bmod 26$ | Ciphertext: 3 → D  |
| Plaintext: V → 21 | $E_n: (21 + 3) \bmod 26$ | Ciphertext: 24 → Y |
| Plaintext: A → 00 | $E_n: (00 + 3) \bmod 26$ | Ciphertext: 3 → D  |
| Plaintext: T → 19 | $E_n: (19 + 3) \bmod 26$ | Ciphertext: 22 → W |
| Plaintext: P → 15 | $E_n: (15 + 3) \bmod 26$ | Ciphertext: 18 → S |
| Plaintext: O → 14 | $E_n: (14 + 3) \bmod 26$ | Ciphertext: 17 → R |
| Plaintext: I → 08 | $E_n: (08 + 3) \bmod 26$ | Ciphertext: 11 → L |
| Plaintext: N → 13 | $E_n: (13 + 3) \bmod 26$ | Ciphertext: 16 → Q |
| Plaintext: T → 19 | $E_n: (19 + 3) \bmod 26$ | Ciphertext: 22 → W |

The encrypted message is "MDYDWSRLQW". Note that the Caesar cipher is monoalphabetic, so the same plaintext letters are encrypted as the same letters. For example, "JAVATPOINT" has "A", encrypted by "D".

# Caesar Cipher Algorithm

- Decryption (**MDYDWSRLQW**)
- We apply decryption formulas by character, based on alphabetical order.
- The formula of decryption is:
- $D_n(x) = (x_i - n) \bmod 26$
- If any case ( $D_n$ ) value becomes negative (-ve), in this case, we will add 26 in the negative value.

|    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 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  |
| 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

# Caesar Cipher Algorithm

- Solution :**      *Decryption (MDYDWSRLQW)*

|    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 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  |
| 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

|                    |                          |                    |
|--------------------|--------------------------|--------------------|
| Ciphertext: M → 12 | $D_n: (12 - 3) \bmod 26$ | Plaintext: 09 → J  |
| Ciphertext: D → 03 | $D_n: (03 - 3) \bmod 26$ | Plaintext: 0 → A   |
| Ciphertext: Y → 24 | $D_n: (24 - 3) \bmod 26$ | Plaintext: 21 → V  |
| Plaintext: A → 00  | $E_n: (00 + 3) \bmod 26$ | Ciphertext: 3 → D  |
| Plaintext: T → 19  | $E_n: (19 + 3) \bmod 26$ | Ciphertext: 22 → W |
| Plaintext: P → 15  | $E_n: (15 + 3) \bmod 26$ | Ciphertext: 18 → S |
| Plaintext: O → 14  | $E_n: (14 + 3) \bmod 26$ | Ciphertext: 17 → R |
| Plaintext: I → 08  | $E_n: (08 + 3) \bmod 26$ | Ciphertext: 11 → L |
| Plaintext: N → 13  | $E_n: (13 + 3) \bmod 26$ | Ciphertext: 16 → Q |
| Plaintext: T → 19  | $E_n: (19 + 3) \bmod 26$ | Ciphertext: 22 → W |

The decrypted message is "JAVATPOINT".

# Caesar Cipher Algorithm

- Example: 1 Plaintext: **THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG**
- Use the Caesar cipher to encrypt and decrypt the message "JAVATPOINT," and the key (shift) value of this message is 23.
- Encryption
- Ciphertext: **QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD**
- <https://www.101computing.net/caesar-cipher/>

|    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 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  |
| 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

## Lecture

## 05

## Caesar Cipher Algorithm Example

- ❑ PlainText = dcodex
- ❑  $K=3$
- ❑  $P=d$
- ❑ 2)  $P=3$
- ❑ 3)  $C=P+K \bmod 26=3+3 \bmod 26=6 \bmod 26 =6$
- ❑ 4)  $C=g$

## Caesar Cipher Algorithm Example

- ❑ PlainText = dcodex
- ❑  $K=3$
- ❑  $P=x$  2)  $P=23$
- ❑ 3)  $C=P+K \bmod 26=23+3 \bmod 26=26 \bmod 26= 0$
- ❑ 4)  $C=a$

Lecture

05

## Caesar Cipher Algorithm Example

- ❑  $P = \text{dcdex}$
- ❑  $C = \text{gfrgha}$
- ❑  $K = 3$

## Caesar Cipher Decryption Example

- ❑ CipherText = gfrgha
- ❑  $K=3$
- ❑  $C=g$
- ❑ 2)  $C=6$
- ❑ 3)  $P=C-K \bmod 26=6-3 \bmod 26=3$
- ❑ 4)  $P=d$

## Caesar Cipher Decryption Example

- ❑ CipherText = gfrgha
- ❑  $K=3$
- ❑  $C=a$
- ❑ 2)  $C=0$
- ❑ 3)  $P=C-K \bmod 26=0-3 \bmod 26=-3 \bmod 26=23$
- ❑ 4)  $P=x$

## Brute-Force Cryptanalysis

- ❑ Ensuring Three important characteristics of this problem enabled us to use a bruteforce cryptanalysis:
  - ❑ The encryption and decryption algorithms are known.
  - ❑ There are only 25 keys to try.
  - ❑ The language of the plaintext is known and easily recognizable.

## Figure 3.3 Brute-Force Cryptanalysis of Caesar Cipher

| KEY | PHHW | PH | DIWHU | WKH | WRJD | SDUWB  |
|-----|------|----|-------|-----|------|--------|
| 1   | oggv | og | chvgt | vjg | vqic | rectva |
| 2   | nffu | nf | bgufs | uif | uphb | qbsuz  |
| 3   | meet | me | after | the | toga | party  |
| 4   | ldds | ld | zesdq | sgd | snfz | ozqsx  |
| 5   | kccr | kc | ydrp  | rfe | rmey | nyprw  |
| 6   | jbbq | jb | xcqbo | qeb | qldx | mxoqv  |
| 7   | iaap | ia | wbpan | pda | pkcw | lwnpu  |
| 8   | hzzo | hz | vaozm | ocz | objv | kvmot  |
| 9   | gyyn | gy | uznyl | nby | niau | julns  |
| 10  | fxxm | fx | tymxk | max | mhzt | itkmr  |
| 11  | ewwl | ew | sxlwj | lzw | lgys | hsjlg  |
| 12  | dvvk | dv | rwkvi | kyv | kfxr | grikp  |
| 13  | cuuj | cu | qvjuh | jxu | jewq | fqhjo  |
| 14  | btti | bt | puigt | iwt | idvp | epgin  |
| 15  | assh | as | othsf | hvs | hcuo | dofhm  |
| 16  | zrrg | zr | nsgre | gur | gbtn | cnegl  |
| 17  | yqqf | yq | mrfqd | ftq | fasm | bmdfk  |
| 18  | xppe | xp | lqepc | esp | ezrl | alcej  |
| 19  | wood | wo | kpdob | dro | dyqk | zkbdi  |
| 20  | vnnv | vn | jocna | cqn | cxpj | yjach  |
| 21  | ummb | um | inbmz | bpm | bwoi | xizbg  |
| 22  | tlla | tl | hmaly | aol | avnh | whyaf  |
| 23  | skkz | sk | glzcx | znk | zumg | vgxze  |
| 24  | rjjy | rj | fkyjw | ymj | ytlf | ufwyd  |
| 25  | qiix | qi | ejxiv | xli | xske | tevxv  |

- ❑ **How to implement Caesar Cipher technique on Arabic letters?**

**Symmetric Encryption**

**Substitution Techniques**

**Caesar Cipher**

**Monoalphabetic Cipher**

**Playfair Cipher**

Hill Cipher

## monoalphabetic cipher

- ❑ A monoalphabetic cipher uses fixed substitution over the entire message
- ❑ Random Key

# monoalphabetic cipher

- Permutation
  - Of a finite set of elements  $S$  is an ordered sequence of all the elements of  $S$ , with each element appearing exactly once
- If the “cipher” line can be any permutation of the 26 alphabetic characters, then there are  $26!$  or greater than  $4 \times 10^{26}$  possible keys
  - This is 10 orders of magnitude greater than the key space for DES
  - Approach is referred to as a *monoalphabetic substitution* cipher because a single cipher alphabet is used per message

Lecture

05

# monoalphabetic cipher

- ❑ Example:
- ❑ Plaintext alphabets:    ABCDEFGHIJKLMNOPQRSTUVWXYZ
- ❑ Ciphertext alphabet: ZEBRASCDFGHIJKLMNOPQTUVWXY
  - ❑ P= ITEMS
- ❑ Encoding
  - ❑ C= FQAIP
- ❑ Decoding
  - ❑ P= ITEMS

# monoalphabetic cipher

- **A mono-alphabetic cipher** (aka simple substitution cipher) is a substitution cipher where each letter of the plain text is replaced with another letter of the alphabet.
- It uses a fixed key which consist of the 26 letters of a “shuffled alphabet”.
- **Plaintext : How Are you                      cipher text : ?????**
- <https://www.101computing.net/mono-alphabetic-substitution-cipher/>

|                                      |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|--------------------------------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Plain text<br>alphabet:              | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| Cipher<br>text<br>alphabet<br>(key): | M | U | A | L | V | O | Z | K | R | N | J | X | Q | D | F | S | H | P | E | B | C | T |   |

# monoalphabetic cipher

## ❑ Example:

❖ Plaintext alphabets: ABCDEFGHIJKLMNOPQRSTUVWXYZ

❖ Ciphertext alphabet: ZEBRASCDFGHIJKLMNOPQTUVWXY

- P= ITEMS

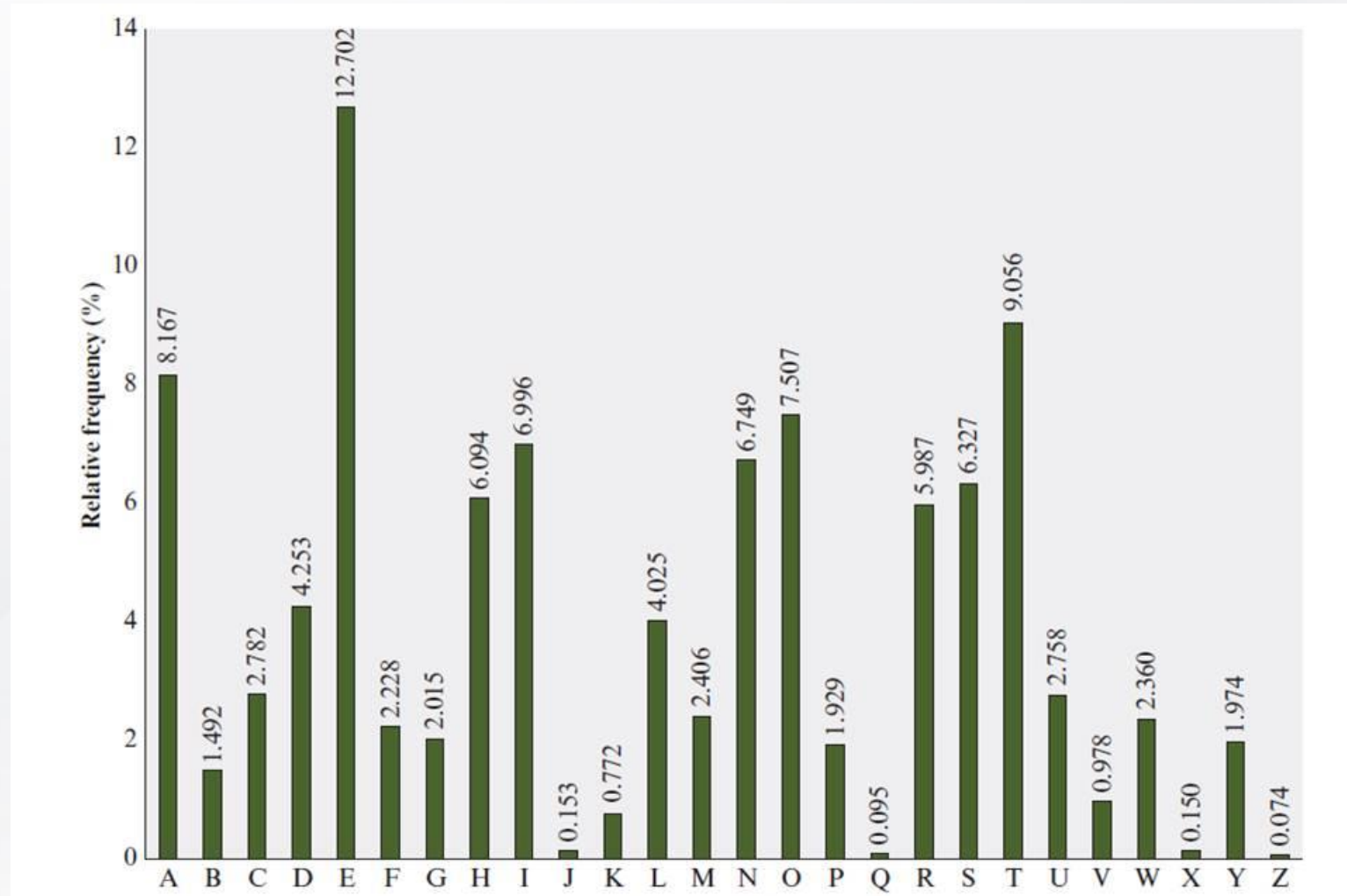
## ❑ Encoding

- C= FQAIP

## ❑ Decoding

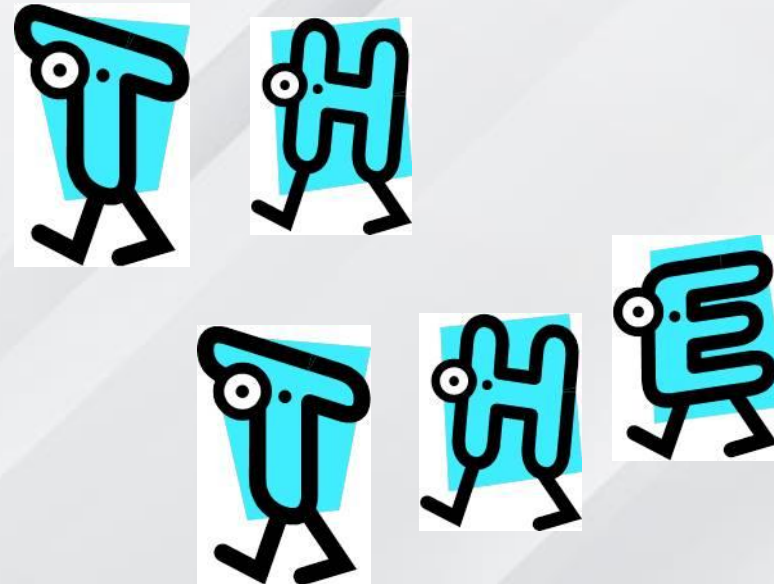
- P= ITEMS

Figure 3.5 Relative Frequency of Letters in English Text



# monoalphabetic cipher

- Easy to break because they reflect the frequency data of the original alphabet
- Countermeasure is to provide multiple substitutes (homophones) for a single letter
- **Digram**
  - **Two-letter combination**
  - **Most common is *th***
- **Trigram**
  - **Three-letter combination**
  - **Most frequent is *the***



# Example Cryptanalysis

- Given ciphertext

uzqsovuohxmopvgpozpevsgzwszopfpesxudbmetsxaizvuephzhzshzowsfpappdtsvpquzwymxuzuh  
 sxepyepopdzszufpombzwpfupzhmdjudtmohmq

- Frequency Analysis

|         |        |        |        |        |
|---------|--------|--------|--------|--------|
| P 13.33 | H 5.83 | F 3.33 | B 1.67 | C 0.00 |
| Z 11.67 | D 5.00 | W 3.33 | G 1.67 | K 0.00 |
| S 8.33  | E 5.00 | Q 2.50 | Y 1.67 | L 0.00 |
| U 8.33  | V 4.17 | T 2.50 | I 0.83 | N 0.00 |
| O 7.50  | X 4.17 | A 1.67 | J 0.83 | R 0.00 |
| M 6.67  |        |        |        |        |

## Example Cryptanalysis

- Guess P & Z are E and T, respectively
- utqsovuohxmo**e**vg**e**o**t**eevsg**t**ws**t**o**e**f**e**esxudbmetsxai**t**vu  
eeh**t**h**t**sh**t**owsf**e**a**ee**edtsvequ**t**wymxu**t**uhsx**e**ey**ee**o**e**dt**t**st**u**  
f**e**omb**t**w**e**fu**e**thmdjudtmohmq

## Example Cryptanalysis

- Among digrams starting with Z, ZW has the highest occurrence (3 times)
- Guess ZW is TH
- U**t**qsovuohxmo**e**vg**e**o**t**eevsg**th**s**t**o**e**f**e**esxudbmetsxai**t**vue**e**h  
**th****t**sh**t**owsf**e**a**e**edtsv**e**qu**th**ymxu**t**uhsx**e**ye**e**o**e**dt**t**stuf**e**omb**t**  
**he**fu**e**thmdjudtmohmq
- Hence ZWP is THE

## Example Cryptanalysis

- Ut**t**qsovuohxmo**e**vg**e**o**t**eevsg**thst**o**e**f**e**esxudbmet**s**xai**t**vue**e**h  
**t**h**t**sh**t**owsf**e**a**e**edt**s**v**e**qu**t**hymxu**t**uhsx**e**eye**e**oedt**s**tuf**e**omb**t**  
**h**efu**e**thmdjudtmohmq
- Guess S is A
- Ut**t**q**a**ovuohxmo**e**vg**e**o**t**eev**a**g**th**at**o**e**f**e**e**a**x**udbmet**a**xai**t**vue**e**h  
**t**h**t**a**h**tow**a**f**e**a**e**edt**a**v**e**qu**t**hymxu**t**uh**a**x**e**eye**e**oedt**a**tuf**e**omb**t**  
**h**efu**e**thmdjudtmohmq

## Example Cryptanalysis

- U, V and M may correspond to O, I and N
- Continuing with trial and error, we finally get the following plaintext

It was disclosed yesterday that several informal but direct contacts have been made with political representatives of the Viet Cong in Moscow

- ❑ How to implement Monoalphabetic Cipher technique on Arabic letters?



مجموعة جامعة  
الجميع الذكية  
للتعليم القابضة

MIDOCEAN  
UNIVERSITY



# Thank You

