
澳 門 理 工 學 院
Instituto Politécnico de Macau
Macao Polytechnic Institute

# COMP412: Computer Security

# Classical Encryptions

**Dr. Kim, Song-Kyoo (Amang)**
**Associate Professor,**

**Faculty of Applied Sciences**
**MACAO POLYTECHNIC INSTITUTE**
**Macau, SAR**

# Agenda

- Symmetric Cipher Model
- Caesar cipher
- Monoalphabetic cipher
- Playfair cipher
- Vigenère cipher

# Symmetric Cipher Model (1/8)

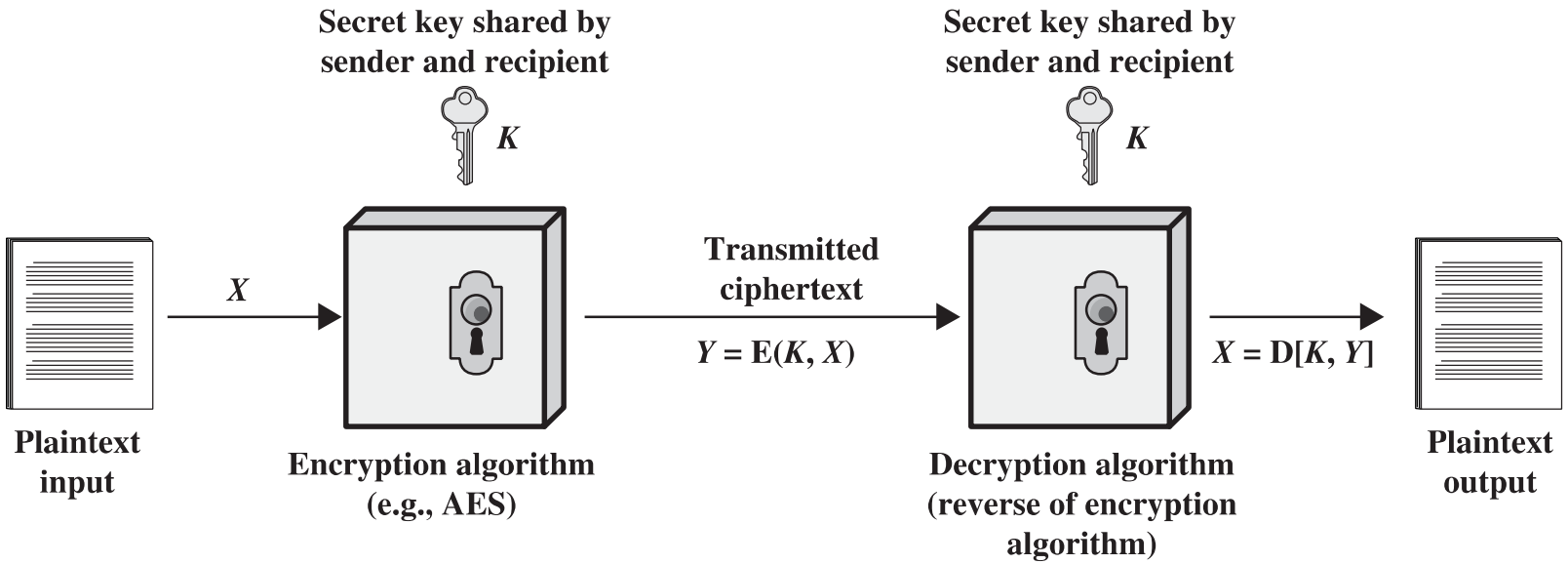
- A symmetric encryption scheme has five ingredients:
  - **Plaintext:** This is the original intelligible message or data that is fed into the algorithm as input.
  - **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.
  - **Secret key:** The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

# Symmetric Cipher Model (2/8)

- Ciphertext:
  - This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.
- Decryption algorithm:
  - This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

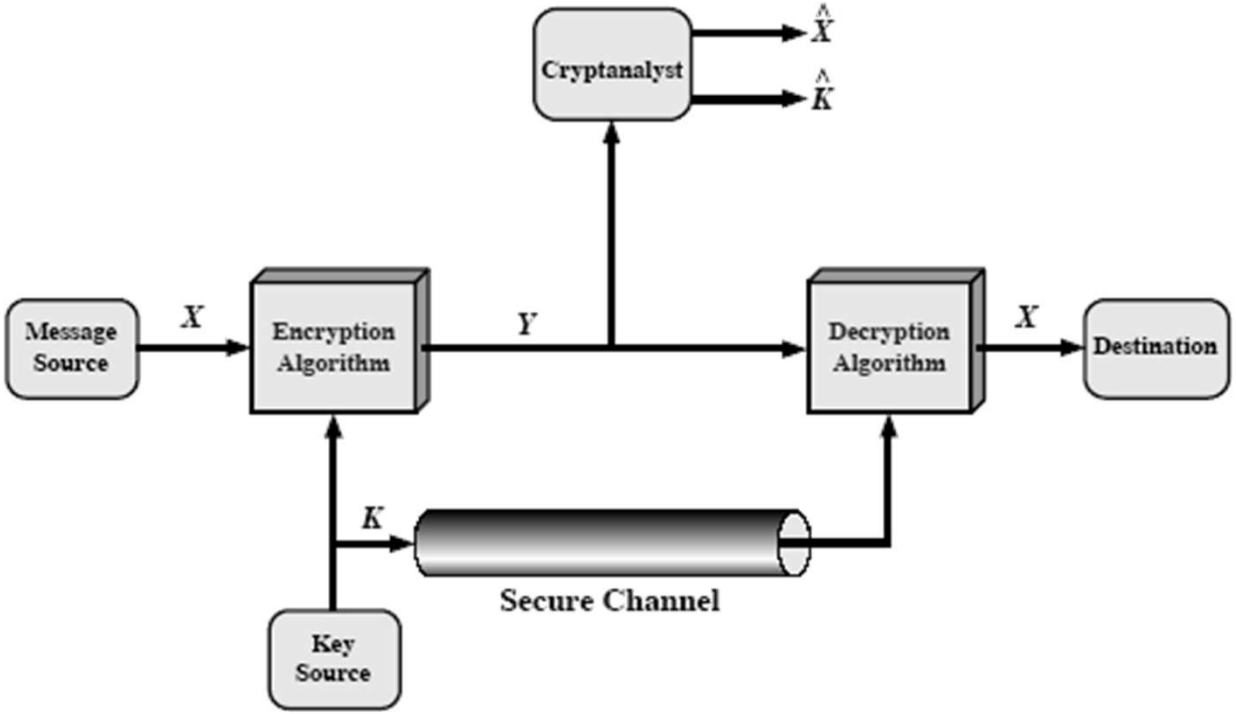
# Symmetric Cipher Model (3/8)

- Simplified Symmetric Encryption



# Symmetric Cipher Model (4/8)

- Conventional Encryption Algorithms
  - A private-key (or secret-key, or single-key) encryption algorithm is one where the sender and the recipient share a common key.
  - Traditional encryption algorithms are **private-key.**



# Symmetric Cipher Model (5/8)

- **Key**
  - The parameter which selects which individual transformation is used, and is selected from a key space K.
  - More formally we can define the cryptographic system as a single parameter family of invertible transformations.

With the message $X$ and the encryption key $K$ as input, the encryption algorithm forms the ciphertext $Y = [Y_1, Y_2, \ldots, Y_N]$. We can write this as

$$Y = \mathrm{E}(K, X)$$

This notation indicates that $Y$ is produced by using encryption algorithm E as a function of the plaintext $X$, with the specific function determined by the value of the key $K$.

The intended receiver, in possession of the key, is able to invert the transformation:

$$X = \mathrm{D}(K, Y)$$

# Symmetric Cipher Model (6/8)

- **Exhaustive Key Search**
  - It is also called **Brute-force attack** that is always theoretically possible to simply try every key .
  - Most basic attack, directly proportional to key size.
  - It is the attack we would assume.
  - Assume either know or can recognize when plaintext is found.
  - Tabulate for reasonable assumptions about number of operations possible.

# Symmetric Cipher Model (7/8)

- **Exhaustive Key Search (cont.)**

| Key Size (bits) | No. of keys | Time (1 encryption/$\mu s$) | Time ($10^6$ encryptions/$\mu s$) |
|---|---|---|---|
| 32 | $2^{32} = 4.3 \times 10^9$ | 35.8 minutes | 2.15 millisec |
| 56 (DES) | $2^{56} = 7.2 \times 10^{16}$ | 1142 years | 10.01 hours |
| 128 (AES) | $2^{128} = 3.4 \times 10^{38}$ | $5.4 \times 10^{24}$ years | $5.4 \times 10^{18}$ years |
| 168 (3DES) | $2^{168} = 3.7 \times 10^{50}$ | $5.9 \times 10^{36}$ years | $5.9 \times 10^{30}$ years |
| 26 characters permutation | $26! = 4 \times 10^{26}$ | $6.4 \times 10^{12}$ years | $6.4 \times 10^{6}$ years |

# Symmetric Cipher Model (8/8)

- **Unconditional secure**
  - 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 secure**
  - Given limited computing resources (e.g. time needed for calculations is greater than age of universe), the cipher cannot be broken
  - Cost of breaking exceeds the value of information
  - Time required exceeds the lifetime of information

# Classical Ciphers (1/12)

- Substitution ciphers by replacing letters
  - Caesar cipher
  - Monoalphabetic cipher
  - Playfair cipher
  - Vigenère cipher
- Transposition ciphers by arranging letters in a different order.
- Several such ciphers may be concatenated together to form a product cipher.

# Classical Ciphers (2/12)

## Caesar Cipher

- Firstly used in military affairs (Gallic wars)

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

- Replace each letter by a shift operation from 1 to 25

| 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 |

- Mathematically expressed as the function:

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

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

# Classical Ciphers (3/12)

- **Cryptanalysis – Brute Force**
  - Each alphabet is mapped to another alphabet by shifting each to the left or right circularly.
  - Could simply try each in turn by an exhaustive key search.
  - Encryption and decryption algorithm are known
  - Too small for brute-force.
  - Language of plaintext is known and easily recognizable.
  - If language of plaintext is unknown, the plaintext output may not be recognizable.

# Classical Ciphers (4/12)

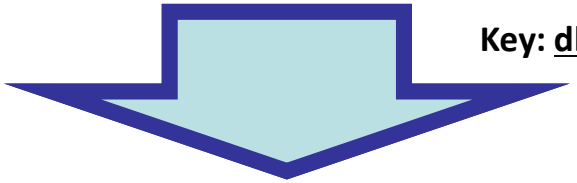
- Cryptanalysis – Brute Force

| KEY | PHHW PH DIWHU WKH WRJD SDUWB |
|---|---|
| 1 | oggv og chvgt vjg vqic rctva |
| 2 | nffu nf bgufs uif uphb qbsuz |
| 3 | meet me after the toga party |
| 4 | ldds ld zesdq sgd snfz ozqsx |
| 5 | kccr kc ydrcp rfc rmey nyprw |
| 6 | jbbq jb xcqbo qeb qldx mxoqv |
| 7 | iaap ia wbpan pda pkcw lwnpu |
| 8 | hzzo hz vaozm ocz ojbv kvmot |
| 9 | gyyn gy uznyl nby niau julns |
| 10 | fxxm fx tymxk max mhzt itkmr |

# Classical Ciphers (5/12)

- Monoalphabetic Cipher
  - Rather than just shifting the alphabet, we could **shuffle the letters arbitrarily** (1-on-1 mapping character).
  - Each plaintext letter maps to a different random ciphertext letter.
  - The key is a sequence of 26 letters (Number of keys: 26!).

**if we wish to replace letters**



**Key: dkvqfibjwpescxhtmyauolrgzn**

**wi rf rwaj uh yftsdvf sfuufya**

# Classical Ciphers (6/12)

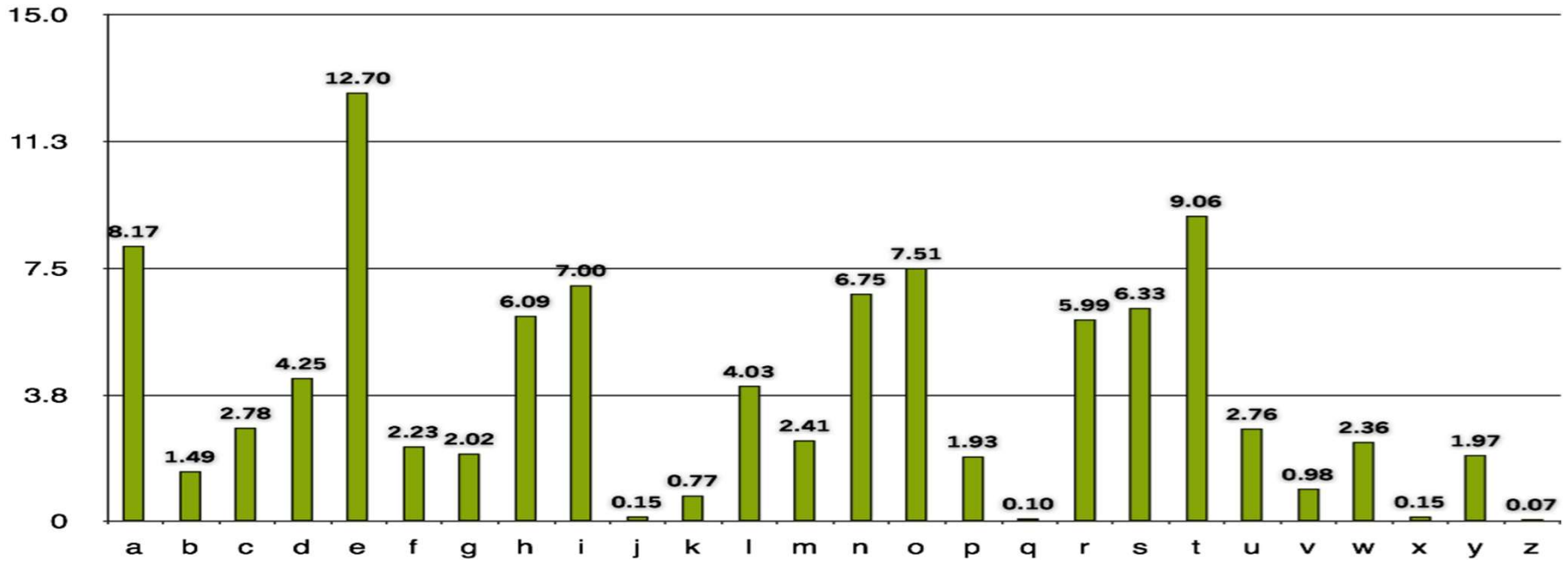
- **Cryptanalysis – Statistical Attack**
  - Monoalphabetic substitution does not change relative letter frequencies.
  - Calculate letter frequencies for ciphertext being analyzed.
  - Compare counts/plots against known values.
  - In particular look for common peaks and troughs.
    - Peaks @ AEI spaced triple, NO pair, RST triple with U shape;
    - Troughs at: JK, XZ

  - **Ciphered texts**

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
```

# Classical Ciphers (7/12)

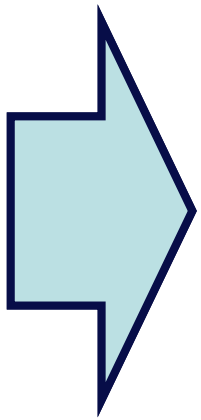
- **Cryptanalysis – Statistical Attack (cont.)**
  - Human languages are redundant (Eg., the, is, etc)
  - Letters are not equally commonly used.
  - e is by far the most common letter then T, R, N, I, O, A, S
  - Other letters are fairly rare (such as z, j, k, q, x)



# Classical Ciphers (8/12)

- Cryptanalysis – Statistical Attack (cont.)
  - Ranking of frequented letters

| Letter | (%) |
|---|---|
| P | 13.3 |
| Z | 11.7 |
| S | 8.3 |
| U | 8.3 |
| O | 7.5 |
| M | 6.7 |



| Letter | (%) |
|---|---|
| e | 12.7 |
| t | 9.1 |
| a | 8.2 |
| o | 7.5 |
| i | 7.0 |
| s | 6.3 |

  - Ciphered Text

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
 t a        e  e te  a that e e a       a
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
   e t   ta t ha e ee  a e  th    t  a
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
 e  e e tat  e   the   t
```

# Classical Ciphers (9/12)

- **Playfair Cipher**
  - The best-known multiple-letter encryption cipher is the Playfair, which treats diagram in the plaintext as single units and translates these units into ciphertext diagrams.
  - The Playfair algorithm is based on the use of a 5 x 5 matrix of letters constructed using a keyword (Key: **Monarchy**).

| | | | | |
|---|---|---|---|---|
| M | O | N | A | R |
| C | H | Y | B | D |
| E | F | G | I/J | K |
| L | P | Q | S | T |
| U | V | W | X | Z |

# Classical Ciphers (10/12)

- Playfair Cipher (cont.)
  - Plaintext is encrypted two letters at a time, according to the following rules:
    - Repeating plaintext letters that are in the same pair are separated with a filler letter (X).
    - Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last.
    - Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last.
    - Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.

# Classical Ciphers (11/12)

- Playfair Cipher (cont.)
  - Plain text: “Nice to meet you” →NI CE TO ME ET YO UX
  - Key: Monarchy
  - Ciphered text: _____

| | | | | |
|---|---|---|---|---|
| M | O | N | A | R |
| C | H | Y | B | D |
| E | F | G | I/J | K |
| L | P | Q | S | T |
| U | V | W | X | Z |

# Classical Ciphers (12/12)

- Vigenère Cipher
  - Vigenère cipher is a multiple Caesar cipher

$$\|K = \{K_1, K_2, \ldots, K_m\}$$

  - Use each alphabet in turn
  - Repeat from start after n letters in message

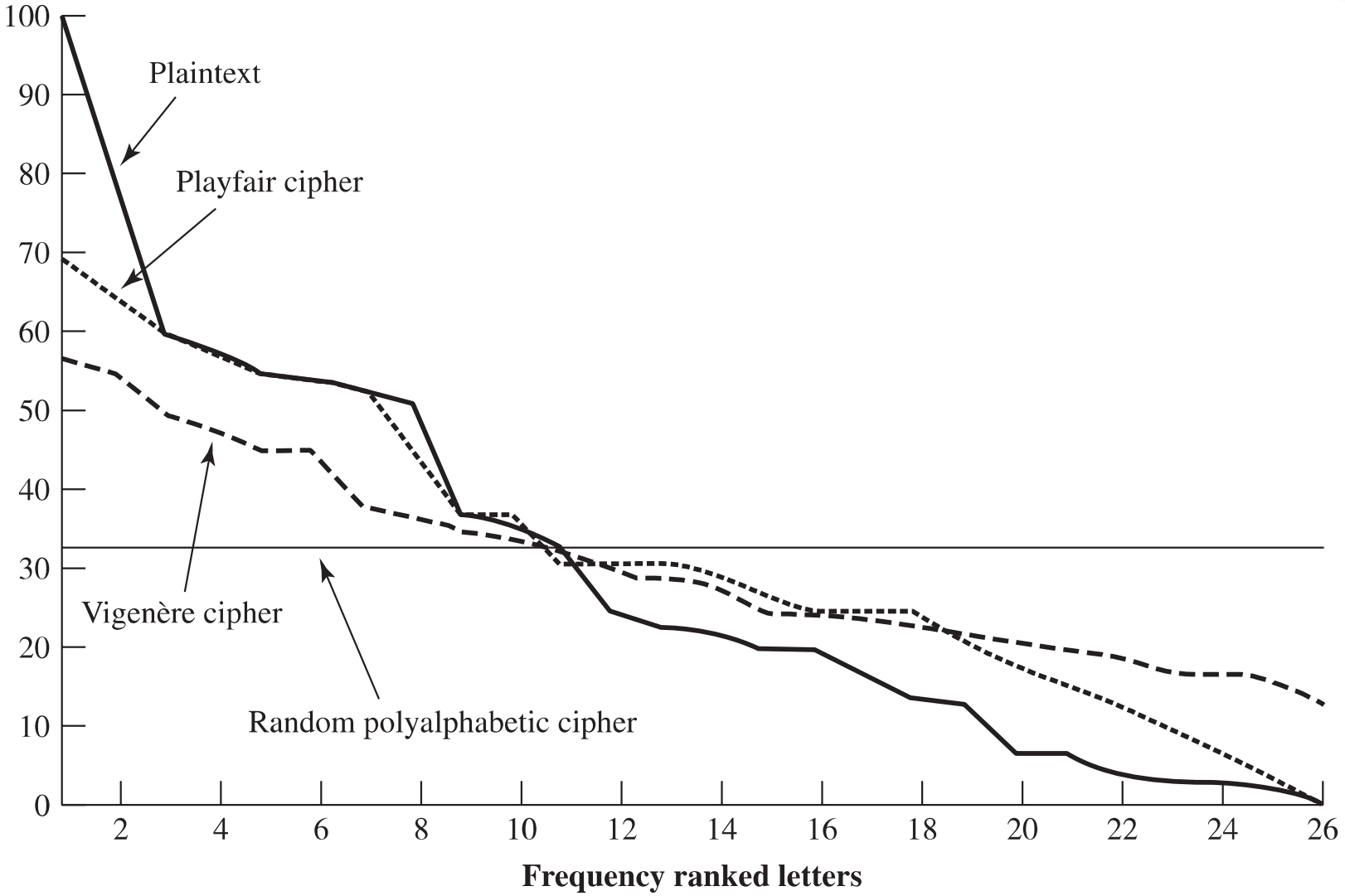
$$\|P = \{P_1 P_2 P_3 \cdots P_n\}$$

  - Mathematically:

$$C = E(\|K, \|P) = (\|P + \|K) \bmod 26$$

$$\|P = C(\|K, \|P) = (\|P - \|K) \bmod 26$$

# Relative Frequency of Occurrence of Letters



# Exercises (1/3)

- Which security service(s) would be required in each of these applications, why (in two sentences) and when:
  - Sending a purchase order to an online merchant.
  - Sending an email with confidential details to your friend.
  - Sending the current status of a door alarm sensor back to the central control panel.
  - Providing a system to control a chemical processing plant.
  - Providing a system to manage sensitive organizational personal records.
- For each of the above, identify which security model is most applicable, identify the parties involved, and discuss your choices.

# Exercises (2/3)

- What type of cryptanalytic attack is used in each of the following scenarios, why and when an attacker analyses:
  - A network dump of a secure web credit card order
  - A photocopy of a scrambled message
  - The interaction with a smart card in his custom reader
- What are the Security services defined in X.800?
- What are the four basic tasks in designing a particular security service?
- What are the categories of active and passive attacks?
- What are plaintext, ciphertext and key?
- In computer security, what is the key space?

# Exercises (3/3)

- Encrypt and then decrypt by hand, the text below using a **Vigenère cipher** with a key of “HAPPY":
  - Plain texts: She felt that it ought to be treated with respect

- Encrypt and decrypt by hand, the text below using the **Playfair cipher** with a key of “AMANGKIM”
  - Pain texts: the common herd is not the acme of excellence


澳門理工學院
INSTITUTO POLITÉCNICO DE MACAU
MACAO POLYTECHNIC INSTITUTE