



زانكۆی سه‌لاحه‌دین - هه‌ولێر
Salahaddin University-Erbil

Information Security

Lecture Five

Classical Cryptography- Part 1

Instructor: Newroz N. Abdulrazaq

Science College- Department of Computer Science & I.T.

`newroz.abudlrzaq@su.edu.krd`

Text Book: Mark Stamp, Information Security: Principles and Practice.+ Educational Websites..

Overview:

- ✔ Introduction.
- ✔ Basic Components Classical Cryptography.
 - » Substitution Cipher.
 - » Transposition Cipher.
- ✔ Monoalphabetic and Polyalphabetic Cipher.
- ✔ Caesar Cipher.
- ✔ Breaking a Caesar Cipher (Cryptanalysis)

Introduction

- Methods of making messages unreadable to adversaries have been important throughout history.
- In this chapter we shall cover some of the older techniques that were primarily used before the era of the computer.
- These techniques are too weak to be of much use today, especially with computers at our disposal, but they give good illustrations of several of the important ideas of cryptology.

Terminologies

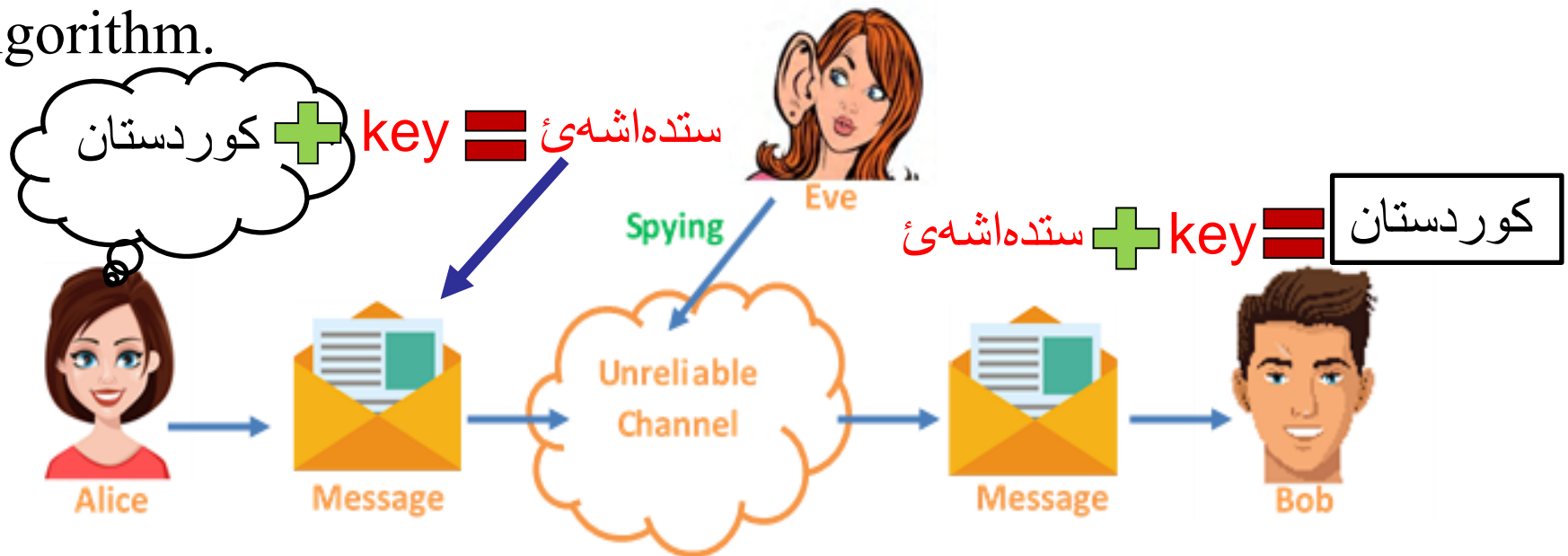
- The art and science of making and breaking "secret codes." is known as **Cryptology**.
- The making of "secret codes." i.e. convert readable data to unreadable data and vice versa using parameters (keys) is known as **Cryptography**.
- The breaking of "secret codes." without knowing the key(s) is known as **Cryptanalysis**.

Terminologies

- A **key** is a piece of information, usually a string of numbers or letters, which, when processed through a cryptographic algorithm, can encode or decode cryptographic data.
- **Encryption** process use a key(s) to alter readable data so that it's scrambled (unreadable).
- The conversion of encrypted data into its original form (readable) is called **Decryption**.

Terminologies

- In cryptography, **plaintext** is usually ordinary readable text before it is encrypted into ciphertext, or readable text after it is decrypted.
- **Cipher text** is the unreadable output of an encryption algorithm.



Basic Components of Classical Cipher

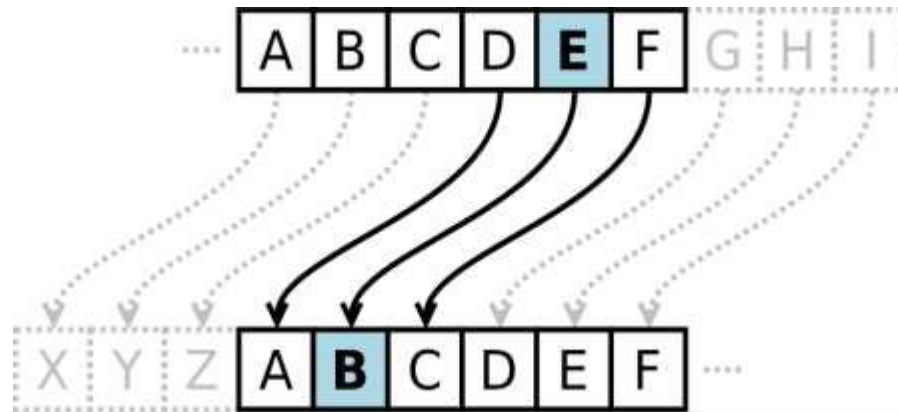
- 1 Substitution Cipher:** is a classical encryption technique where the characters present in the original message are replaced by the other characters or numbers or by symbols.
- 2 Transposition Cipher:** Transposition Cipher is a cryptographic algorithm where the order of alphabets in the plaintext is rearranged to form a cipher text. In this process, the actual plain text alphabets are not included.

Substitution Cipher

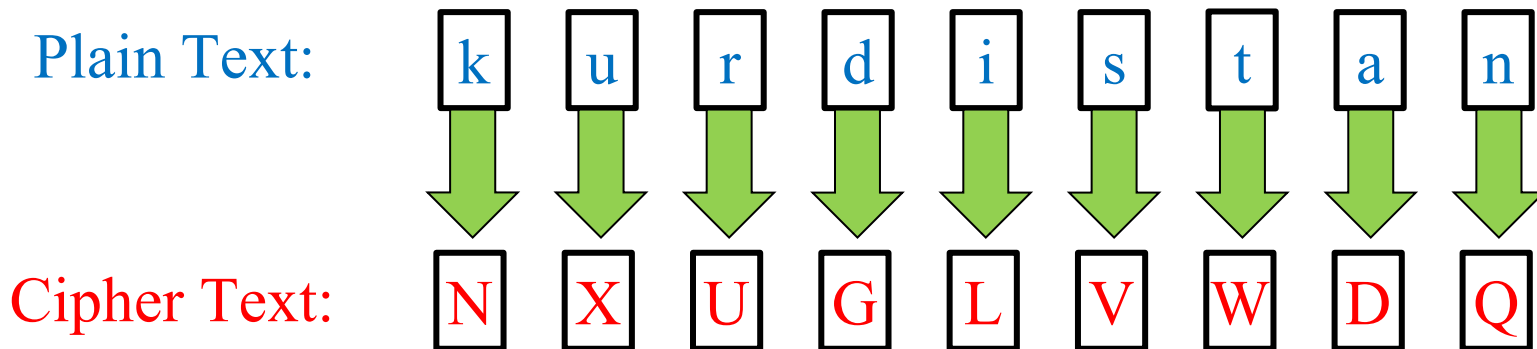
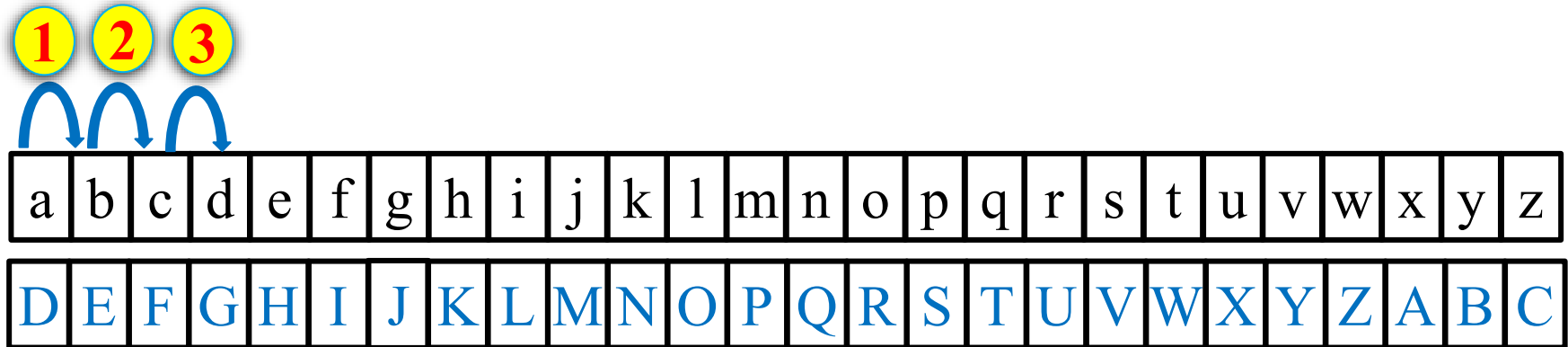
- 1 Monoalphabetic Cipher:** is a substitution cipher, where the cipher alphabet for each plain text alphabet is fixed, for the entire encryption.
- 2 Polyalphabetic Cipher:** Each alphabetic character of plain text can be mapped onto different alphabetic characters of a cipher text.

Caesar Cipher

- ✓ One of the earliest cryptosystems is often attributed to Julius Caesar.
- ✓ It is a type of Monoalphabetic substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet (as shown in picture)

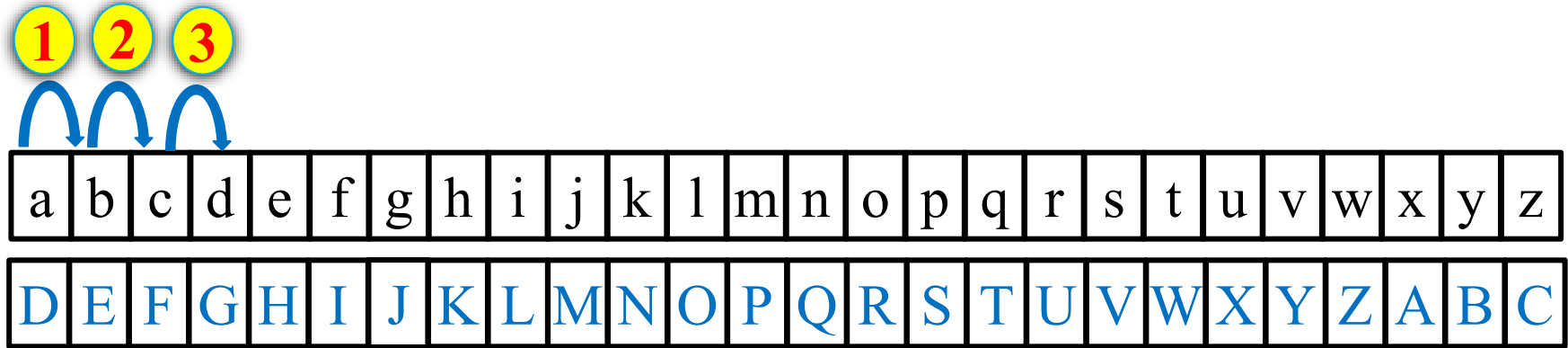


Example: Encrypt (Kurdistan) using Caesar cipher with key= 3?



∴ Cipher Text = NXUGLVWDQ

Example: Decrypt (NXUGLVWDQ) using Caesar cipher with key= 3?



Cipher Text: N X U G L V W D Q

Plain Text: k u r d i s t a n

∴ Plain Text = kurdistan

Mathematical Representation

- 1 Write down the letters from a to z.
- 2 Index the letters from 0 to 25.
- 3 Choose the index for the specified letter that you want to encrypt or decrypt it.
- 4 Use $c = (\text{index} + \text{key}) \bmod 26$ **for encryption**.
Or use $p = (\text{index} - \text{key}) \bmod 26$ **for decryption**.

Example: Encrypt (Dhuk) using Caesar cipher with key= 21?

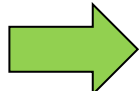
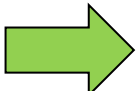
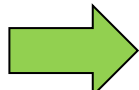
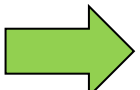
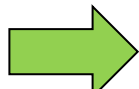
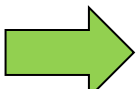
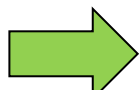
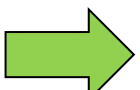
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

For encryption we should use:

$$c = (\text{index} + \text{Key}) \bmod 26 = (\text{index} + 21) \bmod 26$$

Plain Text:

Cipher Text:

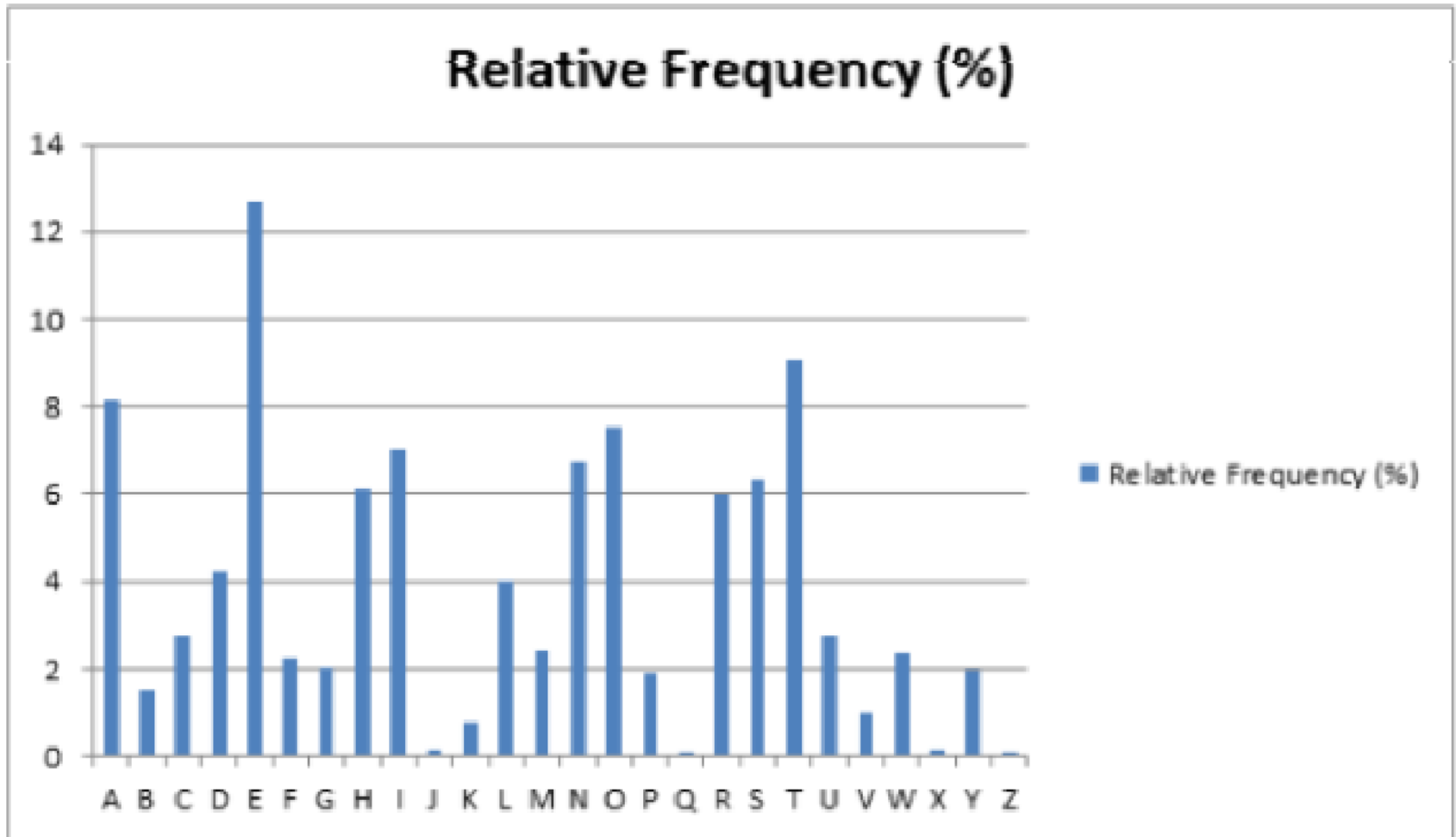
d \equiv 3		$c = 3 + 21 = 24 \bmod 26 = 24$		Y
h \equiv 7		$c = 7 + 21 = 28 \bmod 26 = 2$		C
u \equiv 20		$c = 20 + 21 = 41 \bmod 26 = 15$		P
K \equiv 10		$c = 10 + 21 = 31 \bmod 26 = 5$		F

\therefore Cipher Text = YCPF

Breaking a Caesar Cipher (Cryptanalysis)

- The key space is very small. Using a brute force method, one could easily try all (25) possible combinations in order to decrypt the message without initially knowing the key.
- The structure of the original plaintext remains intact. This makes the encryption method vulnerable to frequency analysis by looking at how often certain characters or sequences of characters appear, one can discover patterns and potentially discover the key without having to perform a full brute force search.

Frequency Analysis



Example: Cryptanalytic (OHZOMDON), if you know that the sender use Caesar cipher to encrypt the message.

According to relative frequency of letters, the most letter used in English language is e, t, a, o and i.

According to the message, the most letter used O.

Hence, let $O \equiv e$

Since , index of $O \equiv 14$ and index of $e \equiv 4$.

$$\therefore \text{key} = 14 - 4 = 10$$

Cipher text: OHZOMDON

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
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

For decryption we should use $p = (\text{index} - \text{Key}) \bmod 26 = (\text{index} - 10) \bmod 26$

Cipher Text:

Plain Text:

O \equiv 14 \longrightarrow $p = 14 - 10 = 4 \bmod 26 = 4$ \longrightarrow e

H \equiv 7 \longrightarrow $p = 7 - 10 = -3 \bmod 26 = 23$ \longrightarrow x

Z \equiv 25 \longrightarrow $p = 25 - 10 = 15 \bmod 26 = 15$ \longrightarrow p

O \equiv 14 \longrightarrow $p = 14 - 10 = 4 \bmod 26 = 4$ \longrightarrow e

M \equiv 12 \longrightarrow $p = 12 - 10 = 2 \bmod 26 = 2$ \longrightarrow c

D \equiv 3 \longrightarrow $p = 3 - 10 = -7 \bmod 26 = 19$ \longrightarrow t

O \equiv 14 \longrightarrow $p = 14 - 10 = 4 \bmod 26 = 4$ \longrightarrow e

N \equiv 13 \longrightarrow $p = 13 - 10 = 3 \bmod 26 = 3$ \longrightarrow d

\therefore Plain Text = expected

Homework5:

Q1: Use Caesar cipher to encrypt the message (Computer Science) with key =15?

Q2: Use Caesar cipher to decrypt the message (UNJYRG) with key =13?

Q3: Use Caesar cipher to Cryptanalytic the message (ACGHQCAACB) ? (Hint: use the 4th most repeated letter in relative frequency

