

Cryptography and network security

BY: DR. UPMA JAIN

Categories of traditional ciphers

- ▶ Substitution Ciphers: Replaces only one symbol with another.
- ▶ Transposition Ciphers: Does not substitute one symbol for another, instead changes the location of the symbols.

Substitution ciphers

- ▶ Categorized as
 - ▶ Monoalphabetic cipher:
 - ▶ A character in plaintext **always changes to the same character** in the ciphertext regardless of its position.
 - ▶ Relationship between a symbol in plaintext and ciphertext will be **one to one**
 - ▶ **Eg. Plaintext: hello Ciphertext: KHOOR**
 - ▶ Polyalphabetic cipher:
 - ▶ Each occurrence of the symbol may have a different substitute.
 - ▶ Relationship between a symbol in plaintext and ciphertext will be **one to many**.
 - ▶ **Eg. Plaintext: hello Ciphertext: ABNZF**

Caesar Cipher

- ▶ A simple example of a substitution cipher is called the **Caesar cipher**, sometimes called a shift cipher. In this approach, each letter is replaced with a letter some fixed number of positions later in the alphabet. For example, if we use a shift of 3, then the letter A would be replaced with D, the letter 3 positions later in the alphabet. The entire mapping would look like:

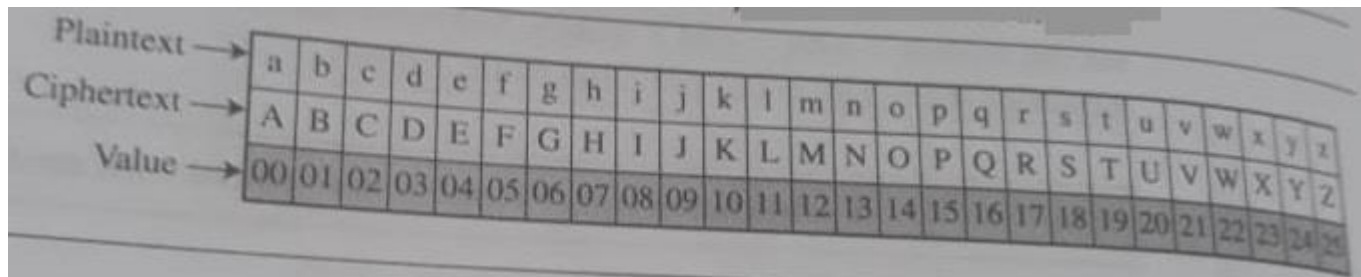
Original: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Maps to: DEFGHIJKLMNOPQRSTUVWXYZABC

- The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,..., Z = 25. Encryption of a letter by a shift n can be described mathematically as.

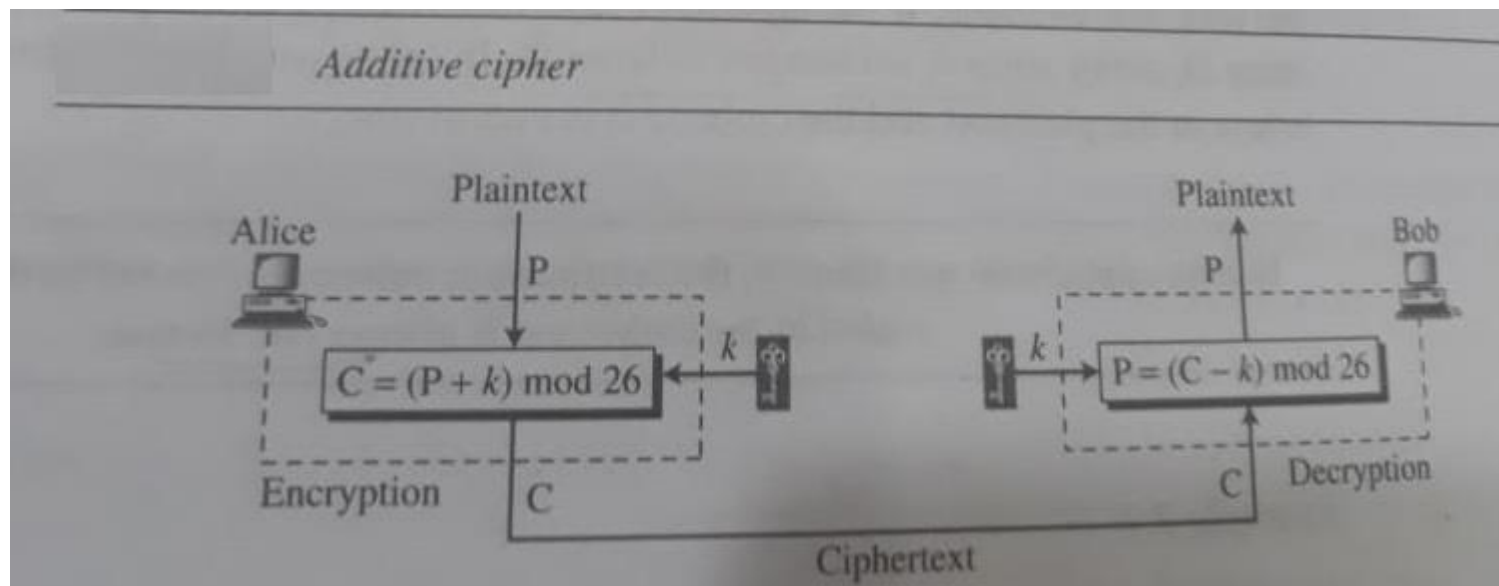
$$E = (P+k) \bmod n$$

$$D = (C-k) \bmod n$$



Plaintext →	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
Ciphertext →	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
Value →	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

Representation of plaintext and ciphertext characters



Additive cipher working

Additive cipher

- ▶ Eg. Use the additive cipher with key=15 to encrypt the message "hello"

Solution

► Solution:

$P = h = 07$	$\text{Enc}(7+15) \bmod 26$	$C = 22 = W$
$P = e = 04$	$\text{Enc}(4+15) \bmod 26$	$C = 19 = T$
$P = l = 11$	$\text{Enc}(11+15) \bmod 26$	$C = 22 = A$
$P = l = 11$	$\text{Enc}(11+15) \bmod 26$	$C = 22 = A$
$P = o = 14$	$\text{Enc}(14+15) \bmod 26$	$C = 22 = D$

Additive cipher

- ▶ Use the additive cipher with key = 15 to decrypt the message “WTAAD”.

► Solution:

$C = W = 22$ $\text{Dcn}(22-15) \bmod 26 \quad P = 07 = h$

$C = T = 19$ $\text{Dcn}(19-15) \bmod 26 \quad P = 04 = e$

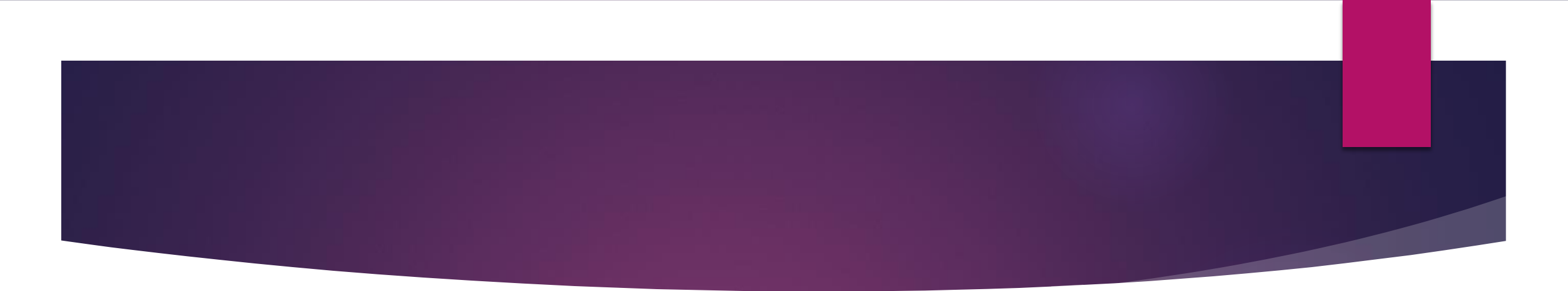
$C = A = 00$ $\text{Dcn}(00-15) \bmod 26 \quad P = 11 = l$

$C = A = 00$ $\text{Dcn}(00-15) \bmod 26 \quad P = 11 = l$

$C = D = 03$ $\text{Dcn}(03-15) \bmod 26 \quad P = 14 = o$

Problems with monoalphabetic ciphers

- ▶ Easy to break because they reflect the frequency data of original alphabet.
- ▶ Possible solution is to use multiple substitutes known as homophones for a single letter.
- ▶ Like for e we can assign different cipher symbols such as 16, 74, 35, 21 with each homophone each rotational or randomly.

- 
- ▶ Two principle methods used in substitution cipher to lessen the extent to which the structure of the plaintext survives in the ciphertext.
 - ▶ Encrypt multiple letters of plaintext
 - ▶ Playfair cipher
 - ▶ Use multiple cipher alphabets

Playfair Cipher

- ▶ The **Playfair cipher** was the first practical digraph substitution cipher.
- ▶ The scheme was invented in **1854** by **Charles Wheatstone** but was named after Lord Playfair who promoted the use of the cipher.
- ▶ In playfair cipher unlike traditional cipher we encrypt a pair of alphabets(digraphs) instead of a single alphabet.

PLAYFAIR CIPHER

The playfair algorithm is based on the use of a 5 X 5 matrix of letters constructed using a keyword is **monarchy**. The matrix is constructed by filling in the letter of the keyword from left to right and from top to bottom , and then filling in the remainder of the matrix with the remaining letters in alphabetic order. The letters I and J count as one letter.

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

Plaintext is encrypted two letters at a time , according to the following rules:

1. Repeating plaintext letters that are in the same pair are separated with a filler letter , such as x , so that balloon would be treated as ba lx lo on.
2. 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. For example , ar is encrypted as RM.

3. 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. For example , mu is encrypted as CM.
4. 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. Thus hs becomes BP and ea becomes IM(or JM , as the encipher wishes).

Algorithm to encrypt the plain text:

- The plaintext is split into pairs of two letters (digraphs).
- If there is an odd number of letters, a Z is added to the last letter.

For example:

PlainText: "instruments"

After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz'

- Pair cannot be made with same letter. Break the letter in single and add a bogus letter to the previous letter.

For Example:

Plain Text: "hello"

After Split: 'he' 'lx' 'lo'

Here 'x' is the bogus letter.

HILL CIPHER

The encryption algorithm takes m successive plaintext letters and substitutes for them m cipher text letters. The substitution is determined by m linear equations in which each character is assigned a numerical value

($a=0$, $b=1$, $z=25$). For $m=3$, the system can be described as follows:

$$c_1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \bmod 26$$

$$c_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \bmod 26$$

$$c_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \bmod 26$$



Thank you