

Substitution cipher

Monoalphabetic Ciphers.

- It is simple substitution
- involves replacing each letter in the message with another letter of the alphabet.

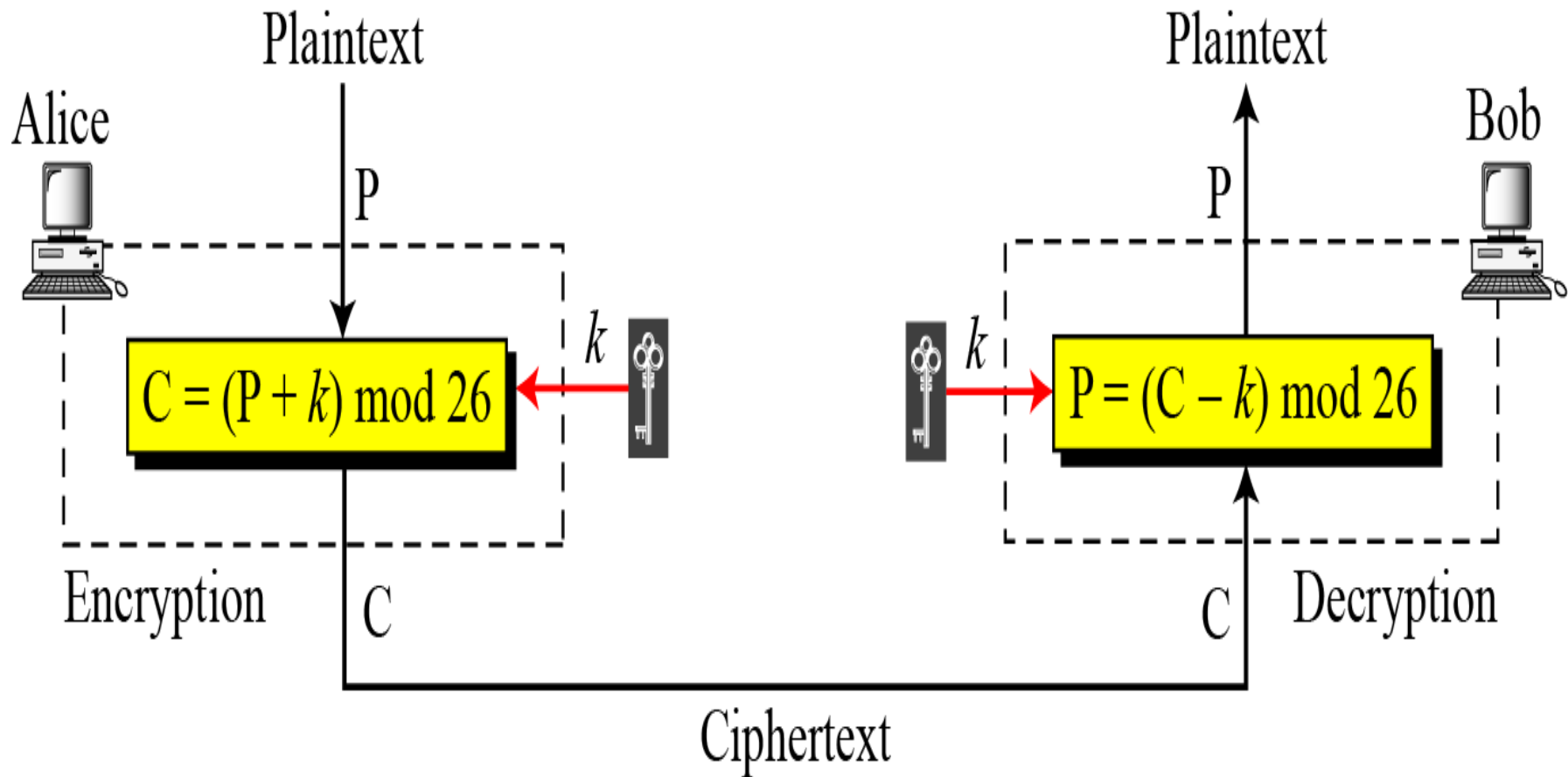
In monoalphabetic substitution, the relationship between a symbol in the plaintext to a symbol in the ciphertext is always one-to-one.

Additive Cipher:- is the simplest monoalphabetic cipher. It is sometimes called a shift cipher and sometimes a **Caesar cipher**, but the term additive cipher better reveals its mathematical nature. When the cipher is additive, the plaintext, ciphertext, and key are integers in Z_{26} .

Plaintext and ciphertext

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

Additive Cipher



Use the additive cipher with key = 15 to encrypt the plain text (hello). •

We apply the encryption algorithm to the plaintext, character by character: •

Plaintext	h	e	l	l	o
	7	4	11	11	14

Encryption

$(7+15) \bmod 26=22 \rightarrow W$, $(4+15) \bmod 26=19 \rightarrow T$, $(11+15) \bmod 26=0 \rightarrow A$, $(11+15) \bmod 26=0 \rightarrow A$, $(14+15) \bmod 26=3 \rightarrow D$

Ciphertext WTAAD

We apply the decryption algorithm to the ciphertext character by character •

Ciphertext	W	T	A	A	D
------------	---	---	---	---	---

	22	19	0	0	3
--	----	----	---	---	---

Decryption

$(22-15) \bmod 26=7 \rightarrow h$, $(19-15) \bmod 26=4 \rightarrow e$, $(0-15) \bmod 26=11 \rightarrow l$, $(0-15) \bmod 26=11 \rightarrow l$, $(3-15) \bmod 26=14 \rightarrow o$

Ciphertext h e l l o

Caesar Cipher: - Named for Julious Caesar. Caesar used a⁴key of 3 for his communications.

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 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

Cryptanalysis of the Caesar cipher: - •

Example : - decrypt the following ciphertext:- •

wklv phvvdjh lv qrw wr kdug wr euhdn

By using the above table, replace the characters as show •

ciphertext = wklv phvvdjh lv qrw wr kdug wr euhdn

**plaintext = THIS MESSAGE IS NOT TOO HARD TO
BREAK**

Example: Eve has intercepted the ciphertext (UVACLYFZLJBYL). Show how she can use a brute-force attack to break the cipher.

Eve tries keys from 1 to 7. With a key of 7, the plaintext is (not very secure),

Ciphertext: UVACLYFZLJBYL

K = 1	→	Plaintext: tuzbkxeykiaxk
K = 2	→	Plaintext: styajwdxjhzwj
K = 3	→	Plaintext: rsxzivcwigyvi
K = 4	→	Plaintext: qrwyhubvhfxuh
K = 5	→	Plaintext: pqvxgtaugewtg
K = 6	→	Plaintext: opuwfsztfdvsv
K = 7	→	Plaintext: notverysecure

TABLE 1

<i>Letter</i>	<i>Frequency</i>	<i>Letter</i>	<i>Frequency</i>	<i>Letter</i>	<i>Frequency</i>	<i>Letter</i>	<i>Frequency</i>
E	12.7	H	6.1	W	2.3	K	0.08
T	9.1	R	6.0	F	2.2	J	0.02
A	8.2	D	4.3	G	2.0	Q	0.01
O	7.5	L	4.0	Y	2.0	X	0.01
I	7.0	C	2.8	P	1.9	Z	0.01
N	6.7	U	2.8	B	1.5		
S	6.3	M	2.4	V	1.0		

Frequency distributions of Plaintext :-

- E •
- T •
- A, O, R, N, I •
- H, C, D, L, M •
- . •
- . •
- X, J, Z, Q •

Example : - Eve has intercepted the following ciphertext. Using a statistical attack, find the plaintext.

**Ciphertext= hqfubswlrq lv d phdqv ri dwwdlqlqj
vhfxuh frppxulfdwlrq**

When Eve tabulates the frequency of letters in this ciphertext, she gets:

h=26, v=17 and so on.

Frequencies of characters

Letter	Count	Percent	Letter	Count	Percent
a	0	0.00	n	0	0.00
b	3	1.80	o	4	2.41
c	0	0.00	p	5	2.99
d	11	6.59	q	16	9.58
e	2	1.20	r	9	5.39
f	6	3.61	s	3	1.80
g	4	2.40	t	0	0.00
h	26	15.56	u	8	4.79
i	2	1.20	v	17	10.18
j	5	2.99	w	14	8.38
k	5	2.99	x	5	2.99
l	16	9.58	y	4	2.40
m	0	0.00	z	2	1.20