Caesar cipher

Classical Encryption Techniques

1. Substitution Technique
2. Transposition Technique

@nesoacademy

Follow

View key concept

Classical Encryption Technique

Substitution	Transposition
❖ Caesar Cipher	❖ Rail Fence
❖ Monoalphabetic Substitution	❖ Row Column Transposition
❖ Playfair Cipher	
❖ Hill Cipher	
❖ Polyalphabetic Ciphers	
❖ One-Time Pad	

Caesar Cipher

- ★ Letters are replaced by other letters or symbols.
- ★ The earlier known and simplest method used be Julius Caesar.
- ★ Replacing each letter of the alphabet with the letter standing three places further down the alphabet.

Example:

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M

13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Caesar Cipher

Algorithm:

For each plaintext letter 'p', substitute the ciphertext letter 'C':

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

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

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M

13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

View key concept

Caesar Cipher – Example

Question: Encrypt "neso academy" using Caesar cipher.

Solution:

n	e	s	o	a	c	a	d	e	m	y

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

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M

13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Caesar Cipher – Example

Question: Encrypt "neso academy" using Caesar cipher.

Solution:

n	e	s	o	a	c	a	d	e	m	y
Q										

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

$C = (13 + 3) \bmod 26$

$C = 16 \bmod 26$

$C = 16$

$C = Q$

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M

13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Caesar Cipher – Example

Question: Encrypt "neso academy" using Caesar cipher.

Solution:

n	e	s	o	a	c	a	d	e	m	y
Q	H	V	R	D	F	D	G	H	P	B

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

$C = (24 + 3) \bmod 26$

$C = 27 \bmod 26$

$C = 1$

$C = B$

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M

13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Shift Cipher

Key = 2, 3, 4, 5, . . .

Shift Cipher with Key = 3 is called Caesar Cipher.

Example:

Plaintext : Neso

Key : 4

Ciphertext : RIWS

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M

13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Caesar Cipher – Pros and Cons

Pros

1. Simple
2. Easy to implement.

Cons

1. The encryption and decryption algorithms are known.
2. There are only 25 keys to try. (Vulnerable to Brute-force attack)
3. The language of the plaintext is known and easily recognizable.

Brute force attack

Ciphertext: SQDYMZK

Shifts	Back	Result
0	[26]	SQDYMZK
1	[25]	TREZNAL
2	[24]	USFAOBM
3	[23]	VTGBPCN
4	[22]	WUHCQDO
5	[21]	XVIDREP
6	[20]	YWJESFQ
7	[19]	ZXKFTGR
8	[18]	AYLGUHS
9	[17]	BZMHVIT
10	[16]	CANIWJU
11	[15]	DBOJXKV
12	[14]	ECPKYLW
13	[13]	FDQLZMX

Shifts	Back	Result
13	[13]	FDQLZMX
14	[12]	GERMANY
15	[11]	HFSNBOZ
16	[10]	IGTOCPA
17	[9]	JHUPDQB
18	[8]	KIVQERC
19	[7]	LJWRFSD
20	[6]	MKXSGTE
21	[5]	NLYTHUF
22	[4]	OMZUIVG
23	[3]	PNAVJWH
24	[2]	QOBWKXI
25	[1]	RPCXLYJ

Vignere Cipher

Classical Encryption Technique

Substitution	Transposition
❖ Caesar Cipher	❖ Rail Fence
❖ Monoalphabetic Cipher	❖ Row Column Transposition
❖ Playfair Cipher	
❖ Hill Cipher	
❖ Polyalphabetic Ciphers	
❖ One-Time Pad	

Polyalphabetic Cipher

★ To improve on the simple monoalphabetic technique.

★ General name: Polyalphabetic substitution cipher.

Common features

1. A set of related monoalphabetic substitution rules is used.
2. A key determines which particular rule is chosen for a given transformation.

Vigenere Cipher

★ It consists of the 26 Caesar ciphers with shifts of 0 through 25.

Encryption process:

$$C_i = (P_i + K_{i \bmod m}) \bmod 26$$

Decryption process:

$$P_i = (C_i - K_{i \bmod m}) \bmod 26$$

Vigenere Cipher

Key : deceptivedeceptivedeceptive

Plaintext : wearediscoveredsaveyourself

Ciphertext : ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Vigenere Cipher

Key : deceptivedeceptivedeceptive

Plaintext : wearediscoveredsaveyourself

Ciphertext : ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Key	3	4	2	4	15	19	8	21	4	3	4	2	4
PT	22	4	0	17	4	3	8	18	2	14	21	4	17
CT													

Key	15	19	8	21	4	3	4	2	4	15	19	8	21	4
PT	4	3	18	0	21	4	24	14	20	17	18	4	11	5
CT														

Vigenere Cipher

Key : deceptivedeceptivedeceptive

Plaintext : wearediscoveredsaveyourself

Ciphertext : ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Key	3	4	2	4	15	19	8	21	4	3	4	2	4
PT	22	4	0	17	4	3	8	18	2	14	21	4	17
CT	25												

Key	15	19	8	21	4	3	4	2	4	15	19	8	21	4
PT	4	3	18	0	21	4	24	14	20	17	18	4	11	5
CT														

Vigenere Cipher

Key : deceptivedeceptivedeceptive

Plaintext : wearediscoveredsaveyourself

Ciphertext : ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Key	3	4	2	4	15	19	8	21	4	3	4	2	4
PT	22	4	0	17	4	3	8	18	2	14	21	4	17
CT	25	8	2	21	19	22	16	13	6	17	25	6	21

Key	15	19	8	21	4	3	4	2	4	15	19	8	21	4
PT	4	3	18	0	21	4	24	14	20	17	18	4	11	5
CT	19	22	0	21	25	7	2	16	24	6	11	12	6	9

Vigenere Cipher – Cryptanalysis

- ★ Determining the length of the keyword.
- ★ Key and the plaintext share the same frequency distribution of letters, a statistical technique can be applied.

Autokey system

- ★ The periodic nature of the keyword can be eliminated by using a non-repeating keyword that is as long as the message itself.
- ★ Vigenère proposed autokey system, in which a keyword is concatenated with the plaintext itself to provide a running key.

Example

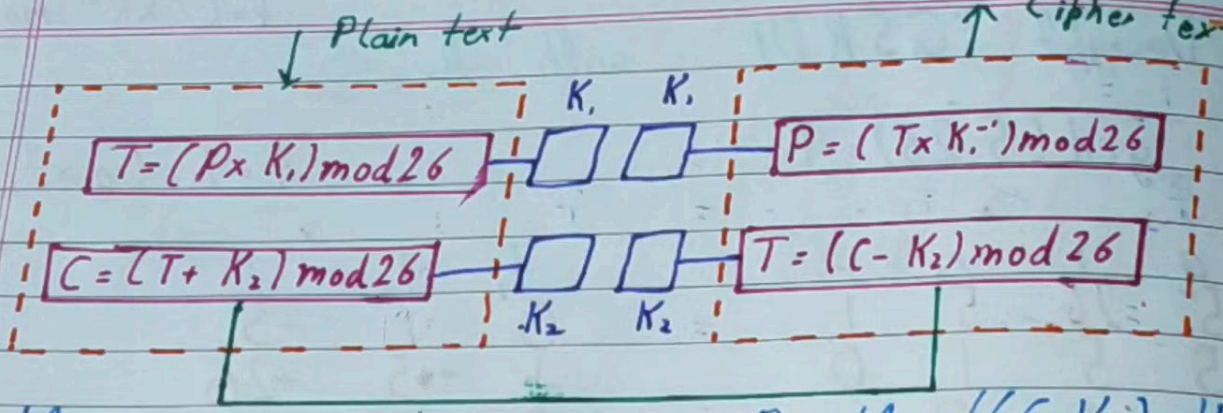
Key : deceptivewearediscoveredsav

Plaintext : wearediscoveredsaveyourself

Ciphertext : ZICVTWQNGKZEIIGASXSTSLVVWLA

Affine Cipher

Affine Cipher

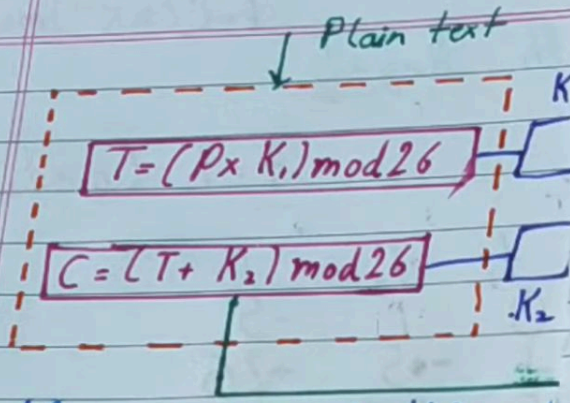


Encryption: $C = ((P \times K_1) + K_2) \bmod 26$ Decryption: $(((C - K_2) \times K^{-1}) \bmod 26$

Q Encrypt & Decrypt "hello" with Keys (7, 2).

$K_1 = 7$ $K_2 = 2$

Affine Cipher



Encryption = $C = ((P \times K_1) + K_2) \bmod$

Q Encrypt & Decrypt "hell

$K_1 = 7$ $K_2 = 2$

Plain text = h e (

↑ Cipher text

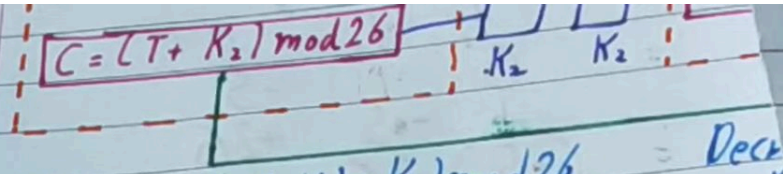
A	B	C	D	E	F
0	1	2	3	4	5

G	H	I	J	K	L
6	7	8	9	10	11

M	N	O	P	Q	R
12	13	14	15	16	17

S	T	U	V	W	X
18	19	20	21	22	23

Y = 24 Z = 25



Encryption = $C = ((P \times K_1) + K_2) \bmod 26$ Decr

Q Encrypt & Decrypt "hello" with

$K_1 = 7$ $K_2 = 2$

Plain text = h e l l o

7 4 11 11 14

P_1 P_2 P_3

$T_1 = (7 \times 7) \bmod 26$

$T_2 = (4 \times 7) \bmod 26$

$T_3 = (11 \times 7) \bmod 26$

$T_4 = (11 \times 7) \bmod 26$

$T_5 = (14 \times 7) \bmod 26$ =

M	N	O	P
12	13	14	15

S	T	U	V
18	19	20	21

Y = 24

$C = (T + K_2) \bmod 26$ K_2 K_2

Encryption = $C = ((P \times K_1) + K_2) \bmod 26$ = Decr

Q Encrypt & Decrypt "hello" with

$K_1 = 7$ $K_2 = 2$

Plain text = h e l l o

7 4 11 11 14

P_1 P_2 P_3 P_4 P_5

$T_1 = (7 \times 7) \bmod 26 = 23$

$T_2 = (4 \times 7) \bmod 26 = 2$

$T_3 = (11 \times 7) \bmod 26 = 25$

$T_4 = (11 \times 7) \bmod 26 = 25$

$T_5 = (14 \times 7) \bmod 26 = 20$

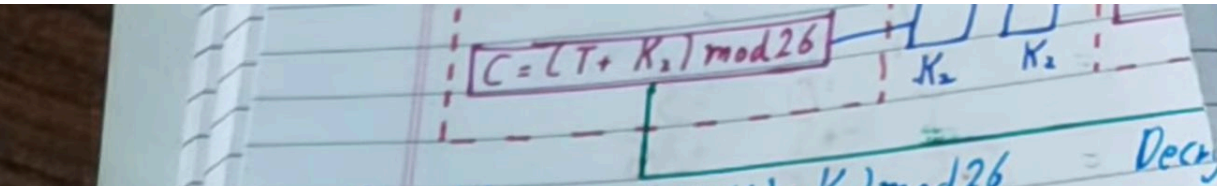
M N O P

12 13 14 15

S T U V

18 19 20 21

$Y = 24$



Encryption = $C = ((P \times K_1) + K_2) \bmod 26$ = Decr

Q Encrypt & Decrypt "hello" with

$K_1 = 7$ $K_2 = 2$

Plain text = h e l l o

7 4 11 11 14

P_1 P_2 P_3 P_4 P_5

$T_1 = (7 \times 7) \bmod 26 = 23 + 2 = 25 = Z$

$T_2 = (4 \times 7) \bmod 26 = 2 + 2 = 4 = E$

$T_3 = (11 \times 7) \bmod 26 = 25 + 2 = 27 = B$ (2

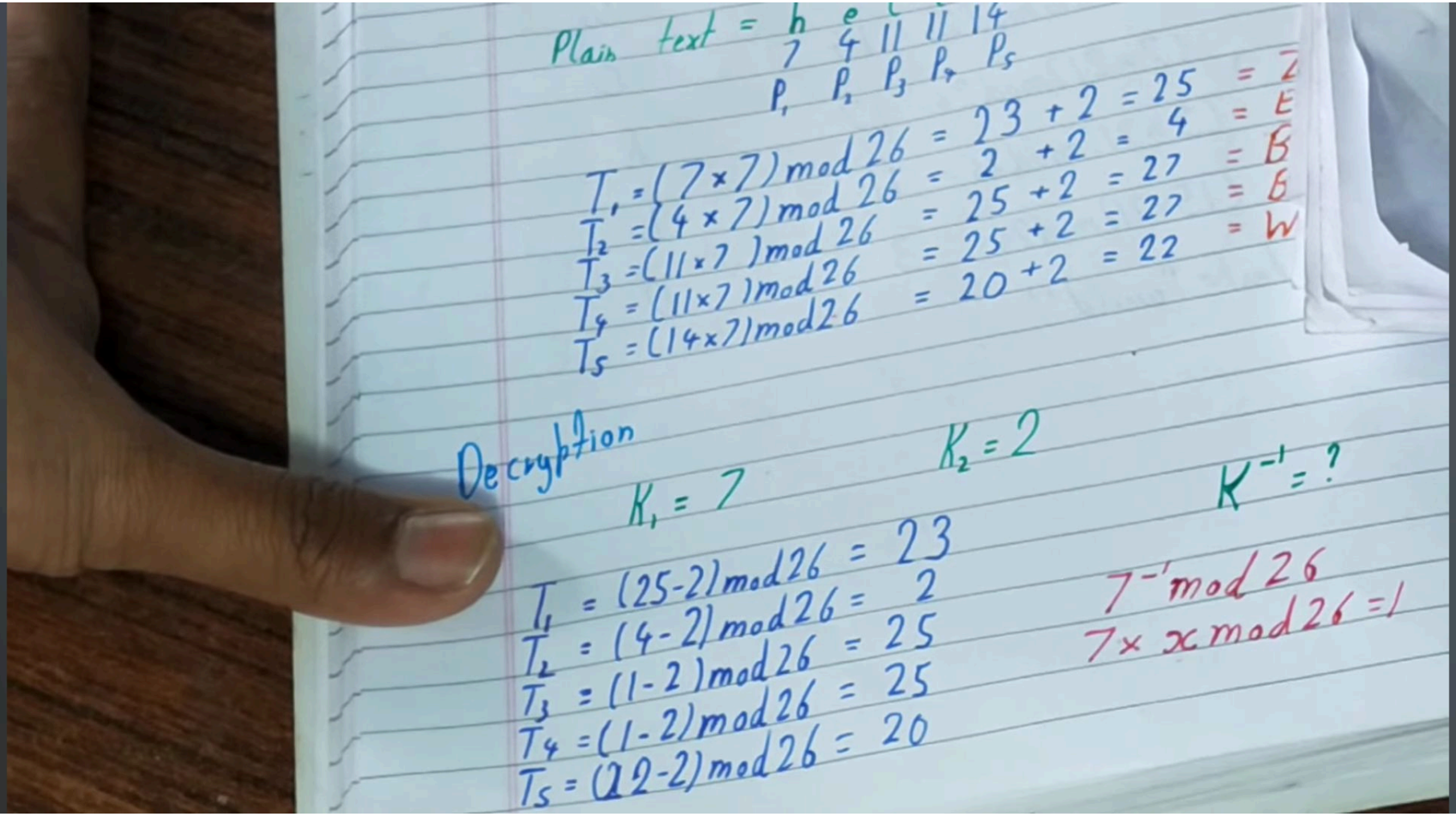
$T_4 = (11 \times 7) \bmod 26 = 25 + 2 = 27 = B$ (2

$T_5 = (14 \times 7) \bmod 26 = 20 + 2 = 22 = W$

M	N	O	P
12	13	14	15

S	T	U	V
18	19	20	21

Y = 24


Plain text = h e
7 4 11 11 14
P1 P2 P3 P4 P5
T1 = (7 × 7) mod 26 = 23 + 2 = 25 = Z
T2 = (4 × 7) mod 26 = 2 + 2 = 4 = E
T3 = (11 × 7) mod 26 = 25 + 2 = 27 = B
T4 = (11 × 7) mod 26 = 25 + 2 = 27 = B
T5 = (14 × 7) mod 26 = 20 + 2 = 22 = W
Decryption
K1 = 7
K2 = 2
K^-1 = ?
T1 = (25 - 2) mod 26 = 23
T2 = (4 - 2) mod 26 = 2
T3 = (1 - 2) mod 26 = 25
T4 = (1 - 2) mod 26 = 25
T5 = (22 - 2) mod 26 = 20
7^-1 mod 26
7 × x mod 26 = 1

Plain text = h e l l o
7 4 11 11 14
P_1 P_2 P_3 P_4 P_5

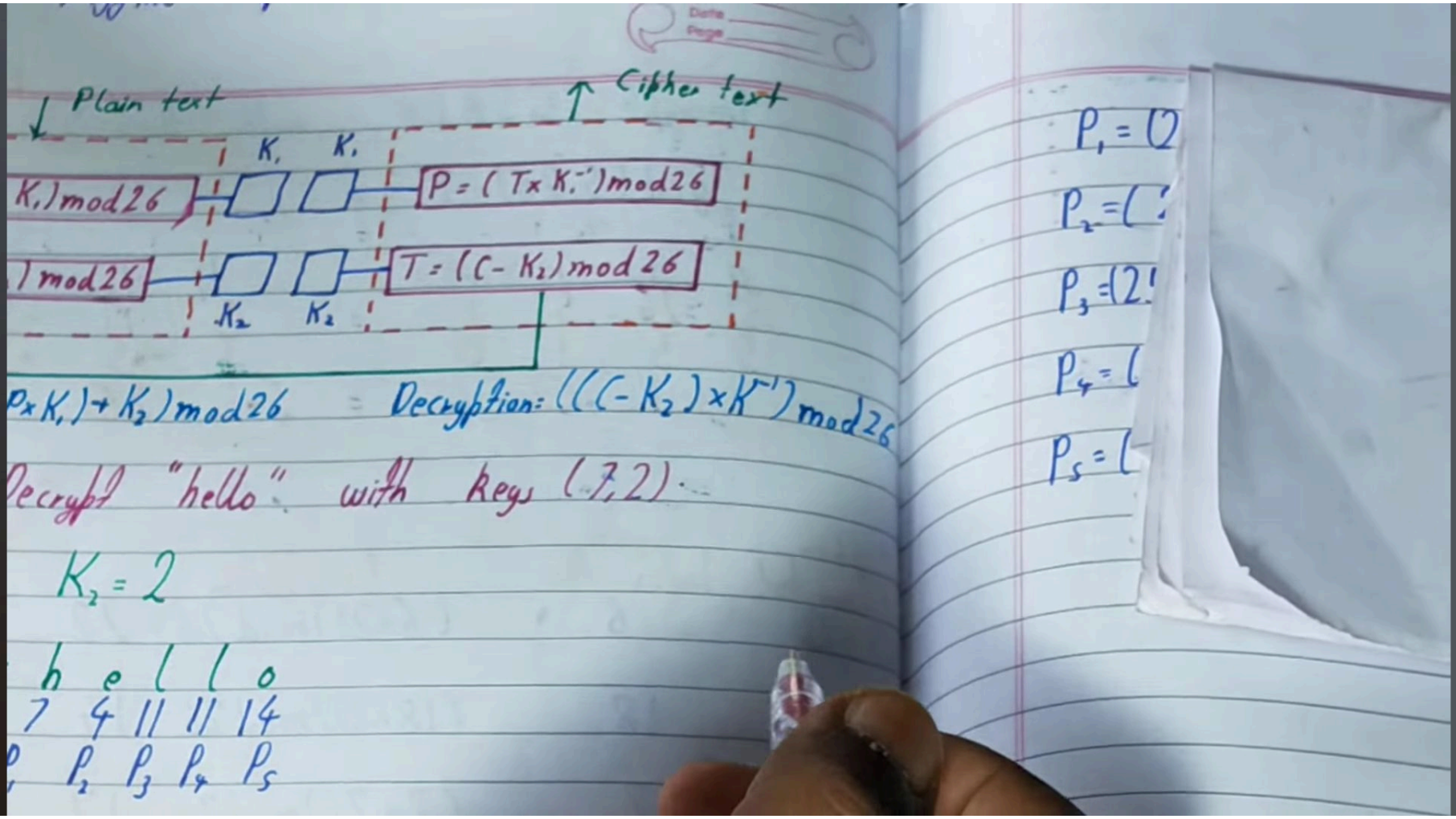
$T_1 = (7 \times 7) \bmod 26 = 23 + 2 = 25 = Z$
$T_2 = (4 \times 7) \bmod 26 = 2 + 2 = 4 = E$
$T_3 = (11 \times 7) \bmod 26 = 25 + 2 = 27 = B$
$T_4 = (11 \times 7) \bmod 26 = 25 + 2 = 27 = B$
$T_5 = (14 \times 7) \bmod 26 = 20 + 2 = 22 = W$

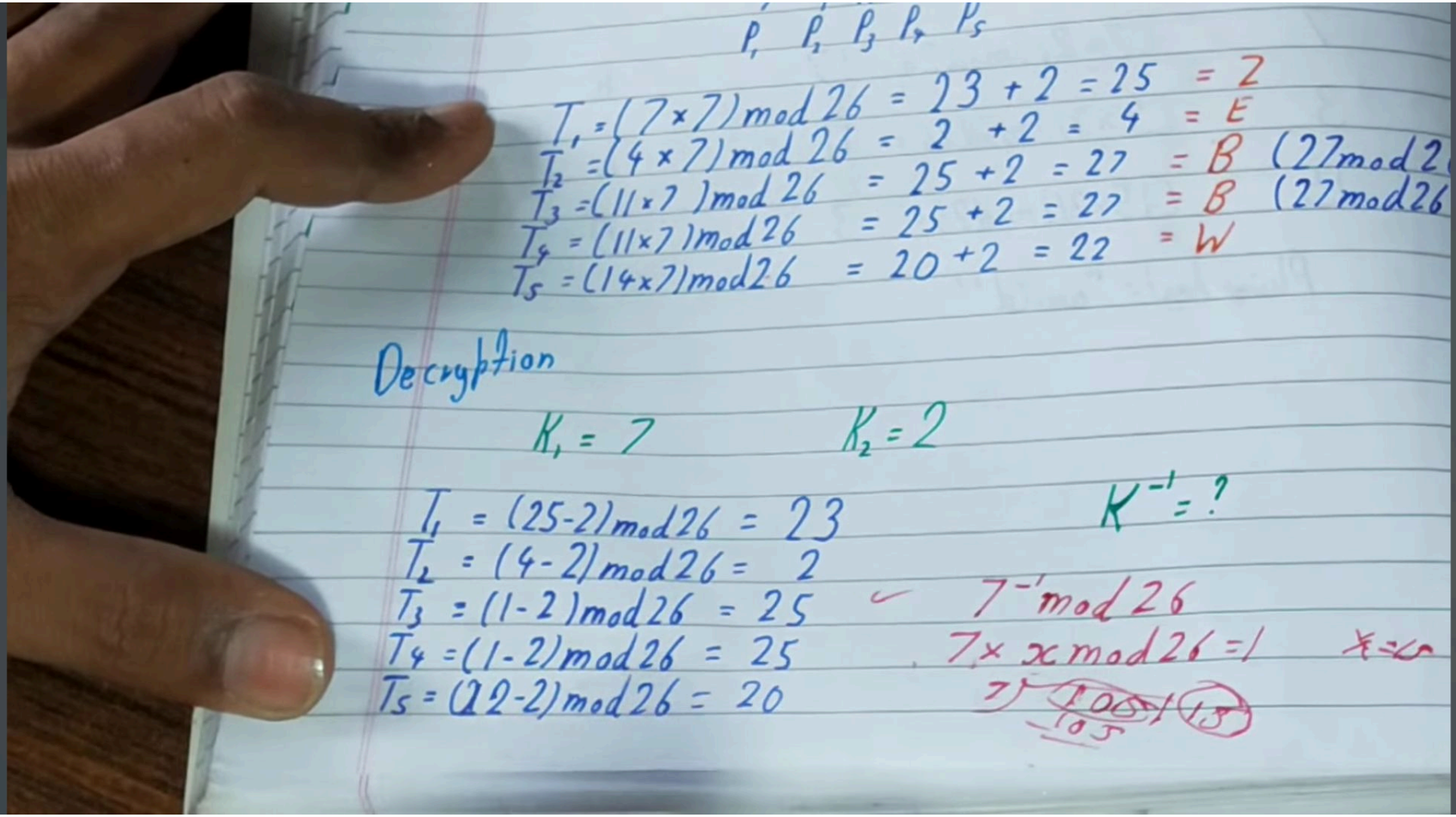
Decryption

$K_1 = 7$ $K_2 = 2$ $K^{-1} = ?$

$T_1 = (25-2) \bmod 26 = 23$
$T_2 = (4-2) \bmod 26 = 2$
$T_3 = (1-2) \bmod 26 = 25$
$T_4 = (1-2) \bmod 26 = 25$
$T_5 = (22-2) \bmod 26 = 20$

$7^{-1} \bmod 26$
$7 \times x \bmod 26 = 1$
105 + 1
105


Plain text
Cipher text
K1
K1
K1)mod26
P = (T × K1^-1) mod26
)mod26
T = (C - K2) mod26
K2
K2
P × K1) + K2) mod26
Decryption: (((-K2) × K^-1) mod26
Decrypt "hello" with Keys (7,2).
K2 = 2
h e l l o
7 4 11 11 14
P1 P2 P3 P4 P5
P1 = (7
P2 = (
P3 = (2
P4 = (
P5 = (



P_1 P_2 P_3 P_4 P_5

$T_1 = (7 \times 7) \bmod 26 = 23 + 2 = 25 = Z$

$T_2 = (4 \times 7) \bmod 26 = 2 + 2 = 4 = E$

$T_3 = (11 \times 7) \bmod 26 = 25 + 2 = 27 = B$ (27 mod 2

$T_4 = (11 \times 7) \bmod 26 = 25 + 2 = 27 = B$ (27 mod 26

$T_5 = (14 \times 7) \bmod 26 = 20 + 2 = 22 = W$

Decryption

$K_1 = 7$ $K_2 = 2$

$K^{-1} = ?$

$T_1 = (25 - 2) \bmod 26 = 23$

$T_2 = (4 - 2) \bmod 26 = 2$

$T_3 = (1 - 2) \bmod 26 = 25$

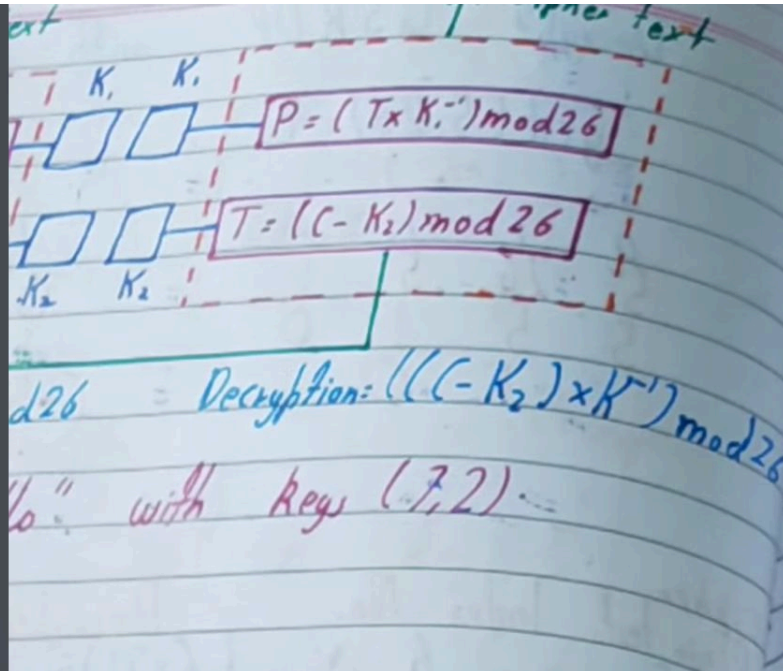
$T_4 = (1 - 2) \bmod 26 = 25$

$T_5 = (22 - 2) \bmod 26 = 20$

$7^{-1} \bmod 26$

$7 \times x \bmod 26 = 1$ $x = 15$

$7 \overline{)105} \; 15$



Decryption: $((C - K_2) \times K^{-1}) \bmod 26$

"o" with Key (7, 2).

$P_1 = (23 \times 15) \bmod 26 = 7$

$P_2 = (2 \times 15) \bmod 26 = 4$

$P_3 = (25 \times 15) \bmod 26 = 11$

$P_4 = (25 \times 15) \bmod 26 = 11$

$P_5 = (20 \times 15) \bmod 26 = 14$

Row column Transposition Cipher

Classical Encryption Technique

Substitution	Transposition
❖ Caesar Cipher	❖ Rail Fence
❖ Monoalphabetic Cipher	❖ Row Column Transposition
❖ Playfair Cipher	
❖ Hill Cipher	
❖ Polyalphabetic Ciphers	
❖ One-Time Pad	

Row Column Transposition

- ★ A more complex scheme.
- ★ Rectangle.
- ★ Write : Row by row.
- ★ Read : Column by column.
- ★ Key : Order of the column

Row Column Transposition

Example: Encrypt the message "Kill Corona Virus at twelve am tomorrow"

Row Column Transposition

Plaintext : "Kill Corona Virus at twelve am tomorrow"

K	i	l	l	c	o	r
o	n	a	v	i	r	u
s	a	t	t	w	e	l
v	e	a	m	t	o	m
o	r	r	o	w		

Row Column Transposition

Plaintext : "Kill Corona Virus at twelve am tomorrow"

Plaintext (Input) →

K	i	l	l	c	o	r
o	n	a	v	i	r	u
s	a	t	t	w	e	l
v	e	a	m	t	o	m
o	r	r	o	w	y	z

Row Column Transposition

Plaintext : "Kill Corona Virus at twelve am tomorrow"

Key →	4	3	1	2	5	6	7
Plaintext (Input) →	K	i	l	l	c	o	r
	o	n	a	v	i	r	u
	s	a	t	t	w	e	l
	v	e	a	m	t	o	m
	o	r	r	o	w	y	z

Row Column Transposition

Plaintext : "Kill Corona Virus at twelve am tomorrow"

Key →	4	3	1	2	5	6	7
Plaintext (Input) →	K	i	l	l	c	o	r
	o	n	a	v	i	r	u
	s	a	t	t	w	e	l
	v	e	a	m	t	o	m
	o	r	r	o	w	y	z

Ciphertext : LATARLVTMOINAERKOSVOCIWTWOREOYRULMZ

35/7 = 5

classmate
Date
Page

LATARLVTMOINAERKOSVOCIWTWOREOYRULMZ

LATAR key 1
LVTMO key 2
INAER key 3
KOSVO key 4
CIWTW key 5
OREOY key 6
RULMZ key 7

4	3	1	2	5	6	7	
K	T	L	L	C	O	R	
O	N	A	V	I	R	U	
S	A	T	T	W	E	L	← decrypted
V	E	A	M	T	O	M	
O	R	R	O	W	Y	Z	