Data Security and Privacy
DSE 3258

L3 -Symmetric Encryption-Substitution Cipher

(Caesar Cipher, Playfair Cipher, Hill Cipher, Transposition Techniques)

Introduction

- An original message is known as the **plaintext**, while the coded message is called the **ciphertext**.
- The process of converting from plaintext to ciphertext is known as **enciphering** or **encryption**; restoring the plaintext from the ciphertext is **deciphering** or **decryption**.
- The many schemes used for encryption constitute the area of study known as **cryptography**.
- Such a scheme is known as a **cryptographic system** or a **cipher**.
- Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of **cryptanalysis**.
- The areas of cryptography and cryptanalysis together are called **cryptology**.

Cryptography

Cryptographic systems are characterized along three independent dimensions:

1. **The type of operations used for transforming plaintext to ciphertext.**

All encryption algorithms are based on two general principles:

substitution: in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element,

transposition: in which elements in the plaintext are rearranged.

Most systems, referred to as ***product systems***, involve multiple stages of substitutions and transpositions.

2. **The number of keys used.**

- If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption.
- If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption.

3. **The way in which the plaintext is processed.**

- A *block cipher* processes the input one block of elements at a time, producing an output block for each input block.
- A *stream cipher* processes the input elements continuously, producing output one element at a time, as it goes along.

Symmetric Cipher Model

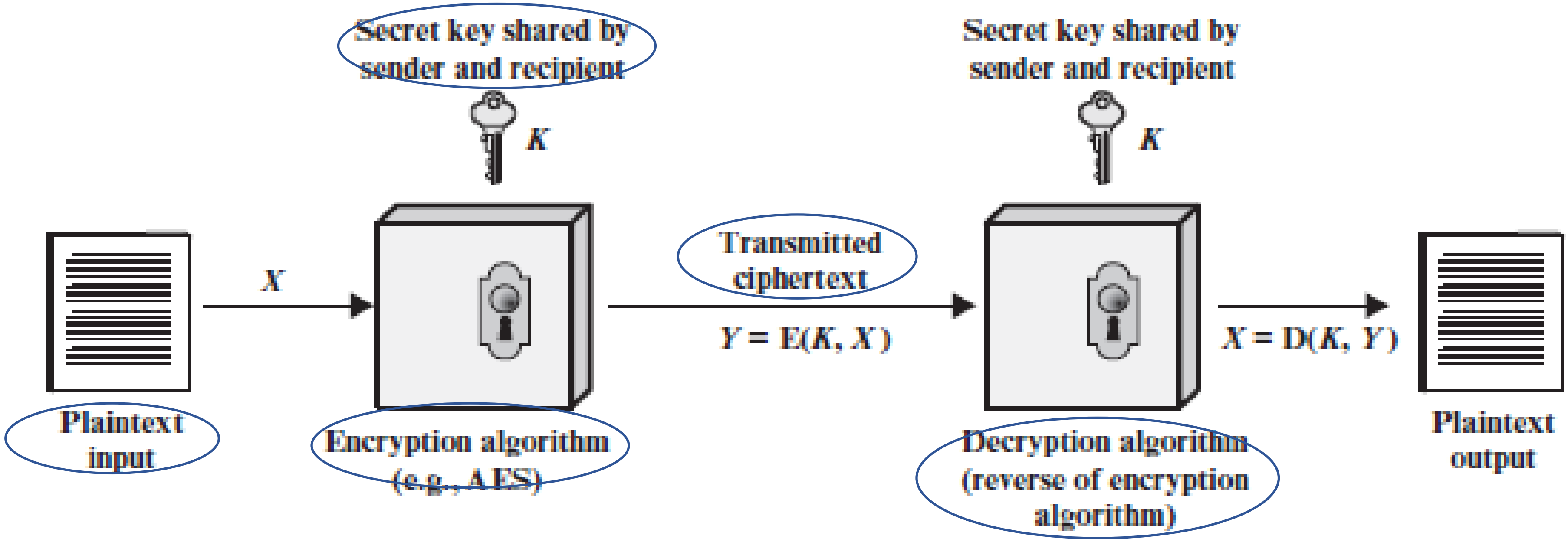

Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
$Y = E(K, X)$
$X = D(K, Y)$
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 3.1 Simplified Model of Symmetric Encryption

Symmetric Cipher Model

- **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.
  - **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

There are two requirements for secure use of conventional encryption:

1. A strong encryption algorithm. At a minimum, we would like the algorithm to be such that an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key. This requirement is usually stated in a stronger form: **The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.**
2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.

Symmetric Cipher Model

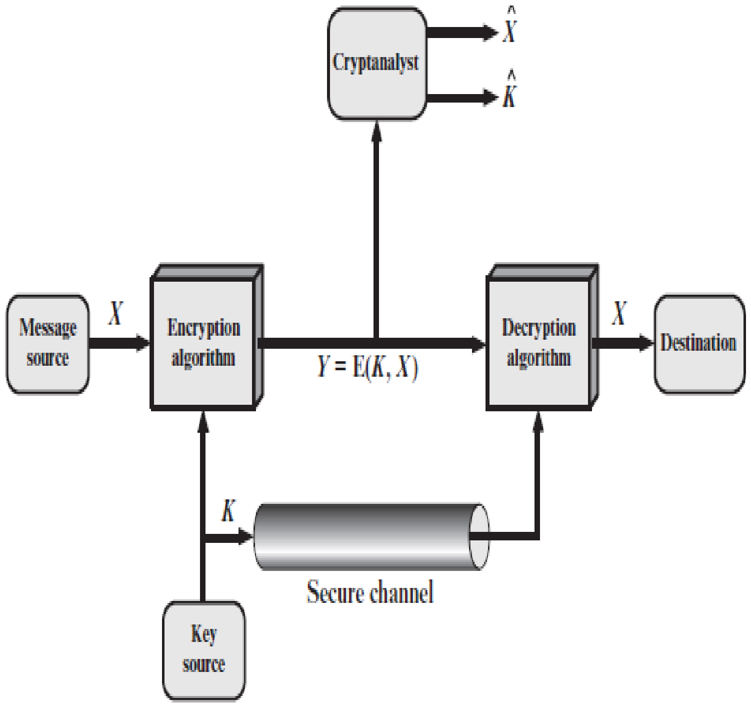


Figure 3.2 Model of Symmetric Cryptosystem

- A source produces a message in plaintext, $X = [X_1, X_2, \ldots, X_M]$.
- The M elements of X are letters in some finite alphabet.
- Traditionally, the alphabet usually consisted of the 26 capital letters. Nowadays, the binary alphabet {0, 1} is typically used.
- For encryption, a key of the form $K = [K1, K2, \ldots, KJ]$ is generated.
-
- If the key is generated at the message source, then it must also be provided to the destination by means of some secure channel.
- Alternatively, a third party could generate the key and securely deliver it to both source and destination.

Symmetric Cipher Model

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:

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

An opponent, observing Y but not having access to K or X, may attempt to recover X or K or both X and K.

It is assumed that the opponent knows the encryption (E) and decryption (D) algorithms. If the opponent is interested in only this particular message, then the focus of the effort is to recover X by generating a plaintextestimate Xn .

Often, however, the opponent is interested in being able to read
future messages as well, in which case an attempt is made to recover K by generating
an estimate Kn .

Cryptanalysis and Brute-Force Attack

- Typically, the objective of attacking an encryption system is to recover the key in use rather than simply to recover the plaintext of a single ciphertext. There are two general approaches to attacking a conventional encryption scheme:

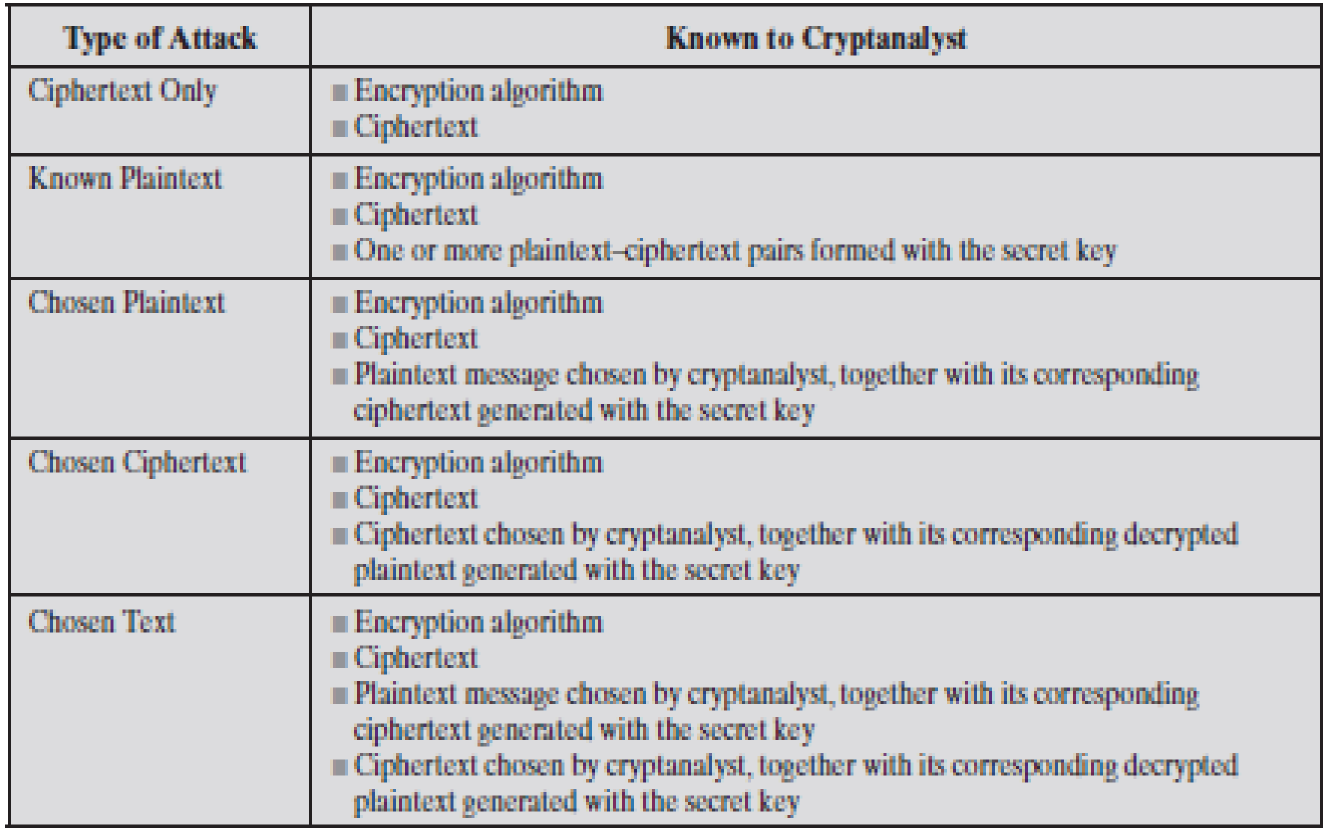
■ **Cryptanalysis:** Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext–ciphertext pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

■ **Brute-force attack:** The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

Cryptanalysis and Brute-Force Attack

- Summary of various types of **cryptanalytic attacks** based on the amount of information known to the cryptanalyst.

Table 3.1 Types of Attacks on Encrypted Messages



Type of Attack	Known to Cryptanalyst
Ciphertext Only	■ Encryption algorithm ■ Ciphertext
Known Plaintext	■ Encryption algorithm ■ Ciphertext ■ One or more plaintext–ciphertext pairs formed with the secret key
Chosen Plaintext	■ Encryption algorithm ■ Ciphertext ■ Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	■ Encryption algorithm ■ Ciphertext ■ Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	■ Encryption algorithm ■ Ciphertext ■ Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key ■ Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

The analyst may know that certain plaintext patterns will appear in a message

If the analyst is able somehow to get the source system to insert into the system a message chosen by the analyst, then a chosen-plaintext attack is possible.

The attacker has capability to make the victim (who obviously knows the secret key) decrypt any ciphertext and send him back the result. By analysing the chosen ciphertext and the corresponding received plaintext, the intruder tries to guess the secret key which has been used by the victim

- An encryption scheme is **unconditionally secure** if the ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available. That is, no matter how much time an opponent has, it is impossible for him or her to decrypt the ciphertext simply because the required information is not there.
- Therefore, all that the users of an encryption algorithm can strive for is an algorithm that meets one or both of the following criteria:
  - ■ The cost of breaking the cipher exceeds the value of the encrypted information.
  - ■ The time required to break the cipher exceeds the useful lifetime of the information.
- An encryption scheme is said to be **computationally secure** if either of the above two criteria are met.

- A **brute-force attack** involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained.
- On average, half of all possible keys must be tried to achieve success. That is, if there are *X* different keys, on average an attacker would discover the actual key after *X*/2 tries.

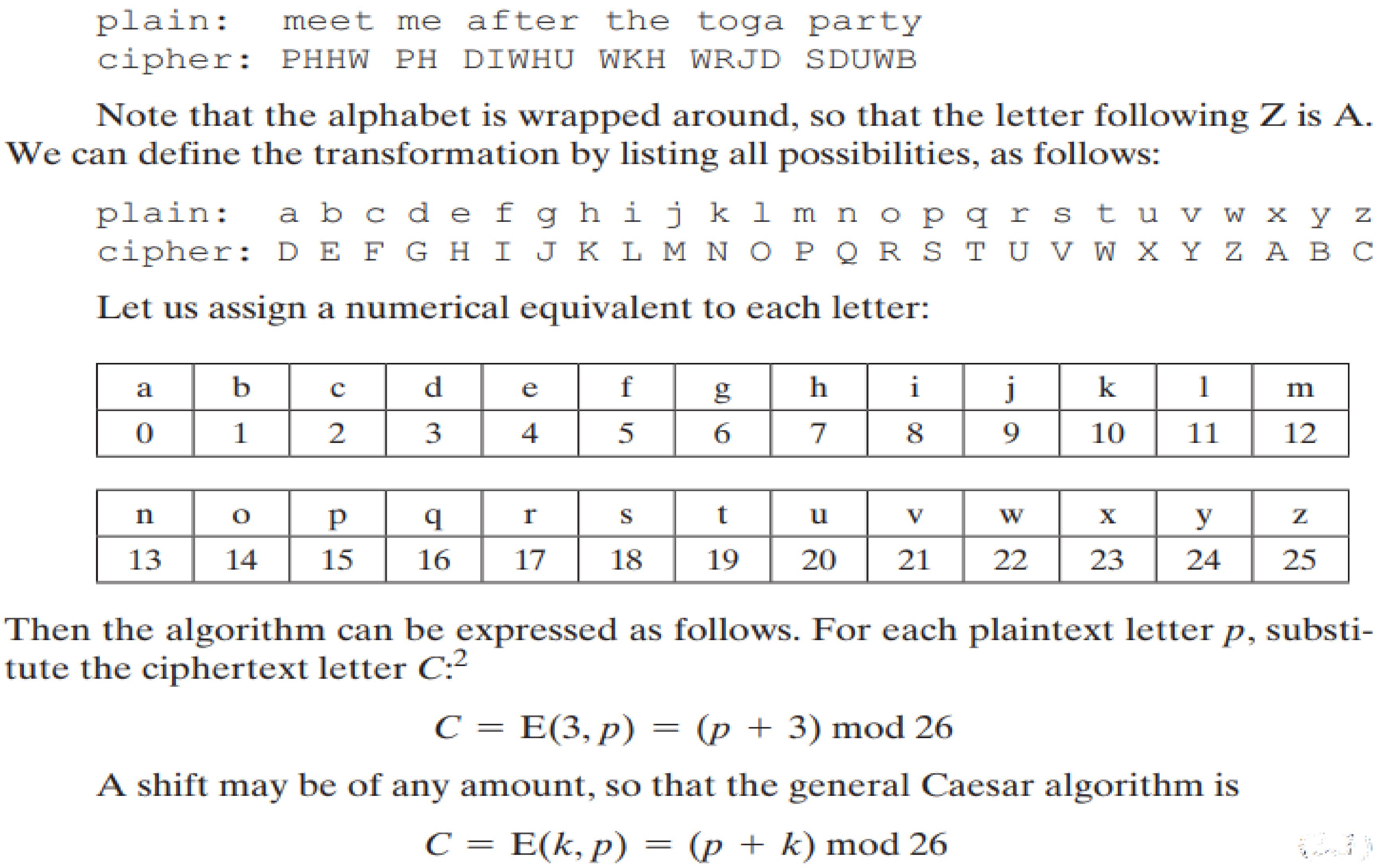
SUBSTITUTION TECHNIQUES

- A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.
- If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.

➢ Caesar Cipher

- The earliest known, and the simplest, use of a substitution cipher was by Julius Caesar.
- The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.
- Caesar Cipher is a method in which each letter in the alphabet is rotated by ***(P+K)mod 26*** letters as shown:

SUBSTITUTION TECHNIQUES (Caesar Cipher Contd..)



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

Note that the alphabet is wrapped around, so that the letter following Z is A. We can define the transformation by listing all possibilities, as follows:

```
plain:  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
cipher: 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
```

Let us assign a numerical equivalent to each letter:

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

Then the algorithm can be expressed as follows. For each plaintext letter p, substitute the ciphertext letter C:[2]

$$C = \mathrm{E}(3, p) = (p + 3) \bmod 26$$

A shift may be of any amount, so that the general Caesar algorithm is

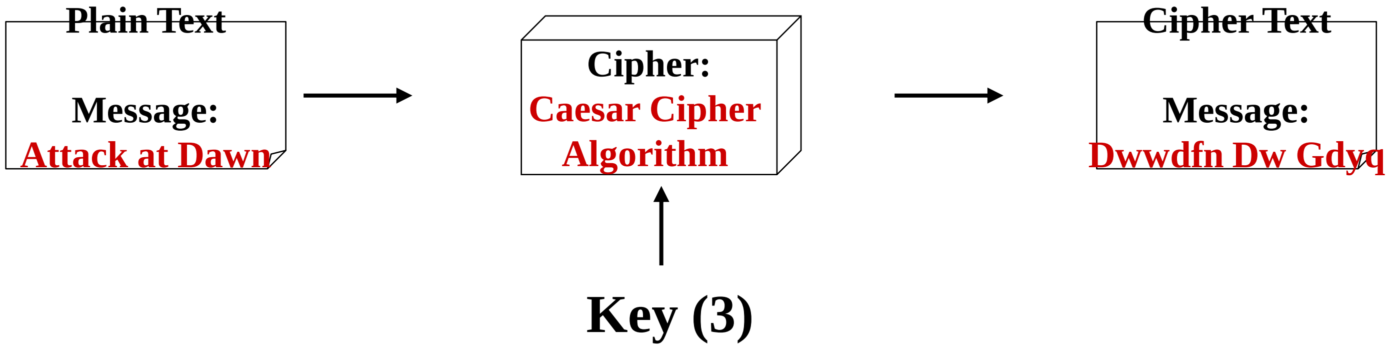
$$C = \mathrm{E}(k, p) = (p + k) \bmod 26$$

SUBSTITUTION TECHNIQUES (Caesar Cipher Contd..)

where k takes on a value in the range 1 to 25. The decryption algorithm is simply

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

Encryption



Plain Text

Message:
Attack at Dawn

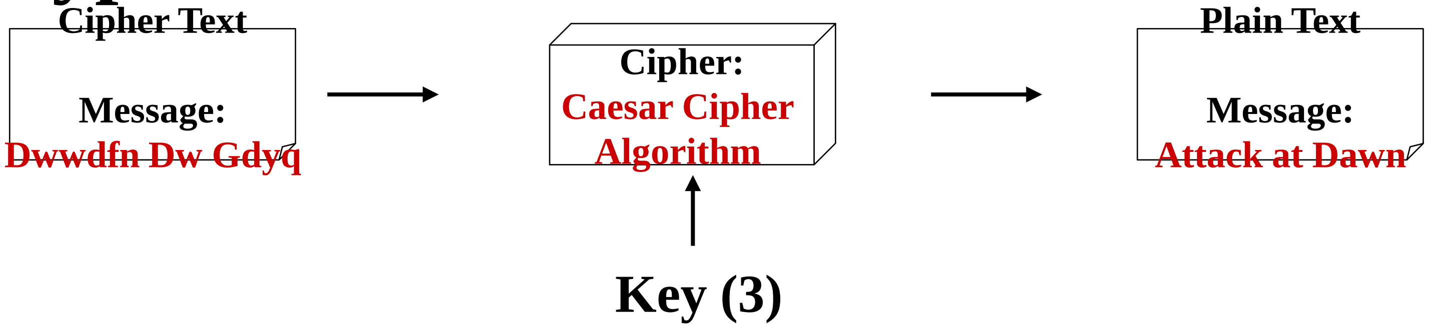
Cipher:
Caesar Cipher
Algorithm

Cipher Text

Message:
Dwwdfn Dw Gdyq

Key (3)

Decryption



Cipher Text

Message:
Dwwdfn Dw Gdyq

Cipher:
Caesar Cipher
Algorithm

Plain Text

Message:
Attack at Dawn

Key (3)

SUBSTITUTION TECHNIQUES (Caesar Cipher Contd..)

Advantages:

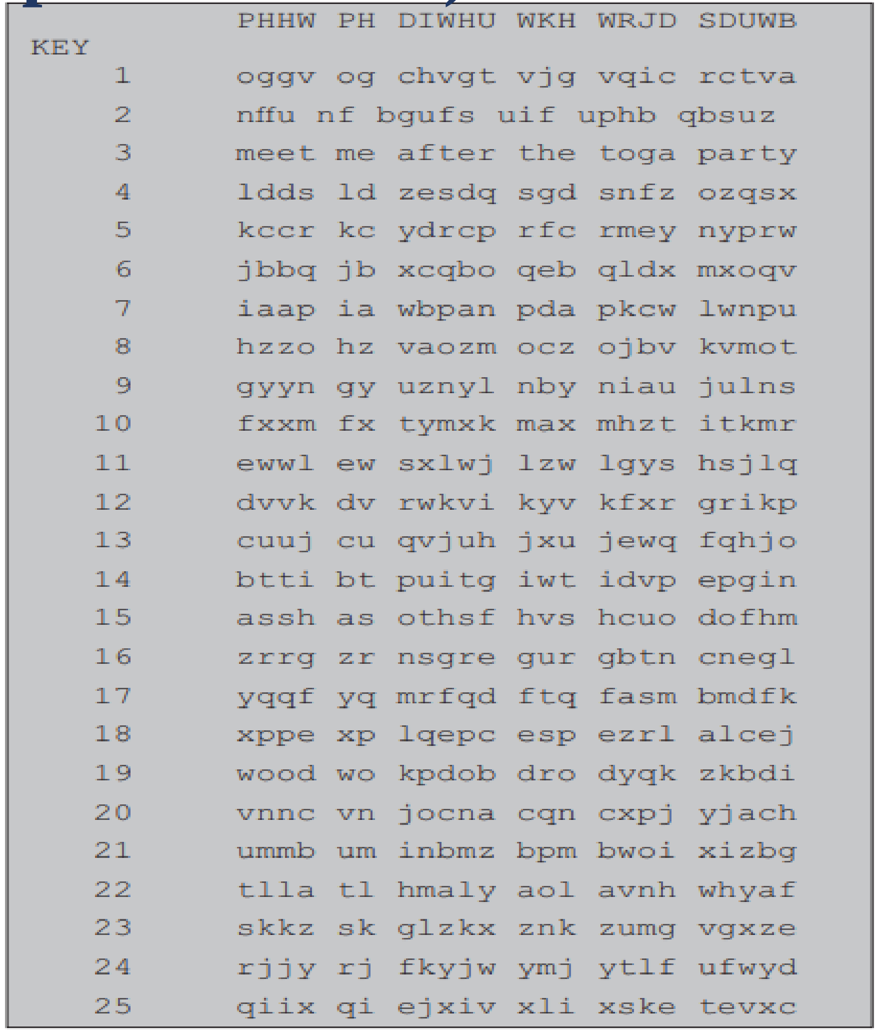
1. It is very easy to implement.
2. This method is the simplest method of cryptography.
3. Only one short key is used in its entire process.
4. If a system does not use complex coding techniques, it is the best method for it.
5. It requires only a few computing resources.

Disadvantages:

1. It can be easily hacked. It means the message encrypted by this method can be easily decrypted.
2. It provides very little security.
3. By looking at the pattern of letters in it, the entire message can be decrypted

SUBSTITUTION TECHNIQUES (Caesar Cipher Contd..)

- If it is known that a given ciphertext is a Caesar cipher, then a brute-force cryptanalysis is easily performed: simply try all the 25 possible keys.



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
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm bmdfk
18	xppe xp lqepc esp ezrl alcej
19	wood wo kpdob dro dyqk zkbdi
20	vnnc vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

Figure 3.3 Brute-Force Cryptanalysis of Caesar Cipher

SUBSTITUTION TECHNIQUES

➢Monoalphabetic Cipher

- Caesar’s cipher has only 25 keys which were easy to brute-forced.
- But it could increase the security if the key space increased.
- This was done using arbitrary substitution --- by permutating the alphabet.
- A permutation is a finite set of elements S in ordered sequence of all the elements of S with each element appended exactly once.
- Example: S= {a,b,c}

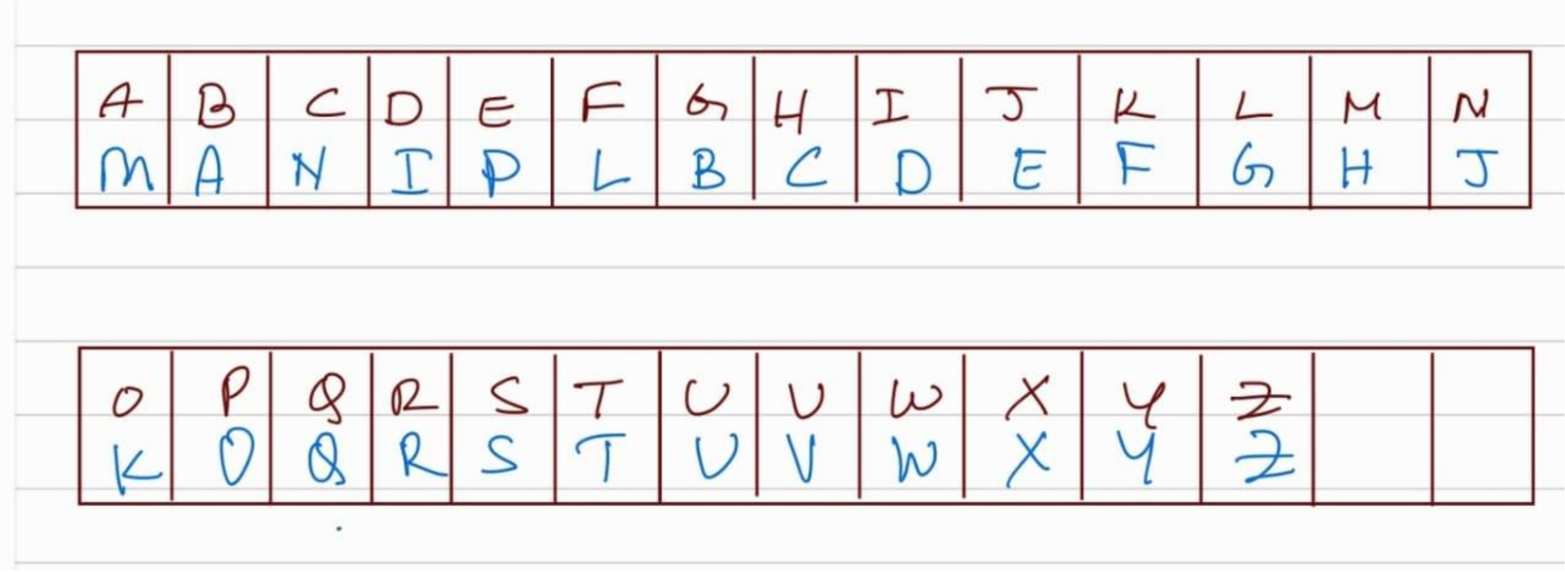
  can generate → {abc, acb, bac, bca, cab, cba}

Technique used→ **Mixing the alphabets as key**

SUBSTITUTION TECHNIQUES (**Monoalphabetic Cipher Contd..)**

- Example:
  - PT: Data Science
  - Key: Manipal

IMTMSNDPJNP



A	B	C	D	E	F	G	H	I	J	K	L	M	N
M	A	N	I	P	L	B	C	D	E	F	G	H	J

O	P	Q	R	S	T	U	V	W	X	Y	Z		
K	O	Q	R	S	T	U	V	W	X	Y	Z		

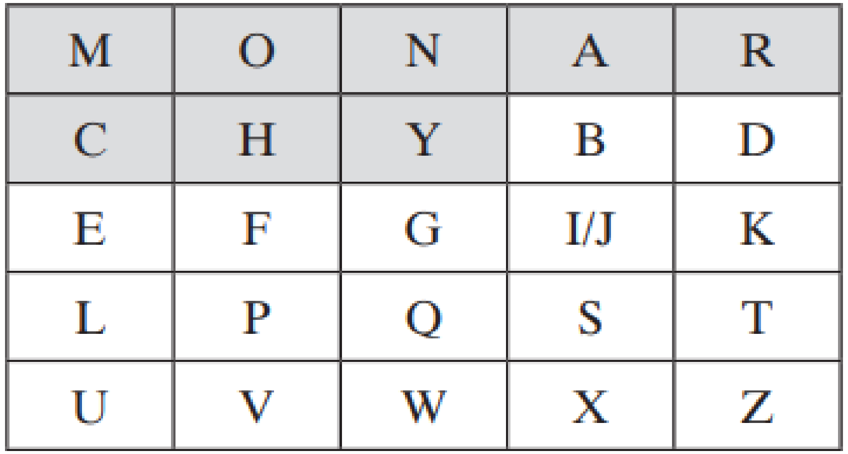
SUBSTITUTION TECHNIQUES (**Monoalphabetic Cipher Contd..)**

- Unfortunately, monoalphabetic substitution ciphers are also subject to a letter frequency analysis...
- If the cryptanalyst knows the nature of the plaintext (e.g., non-compressed English text), then the analyst can exploit the regularities of the language.

SUBSTITUTION TECHNIQUES

➢ Playfair Cipher

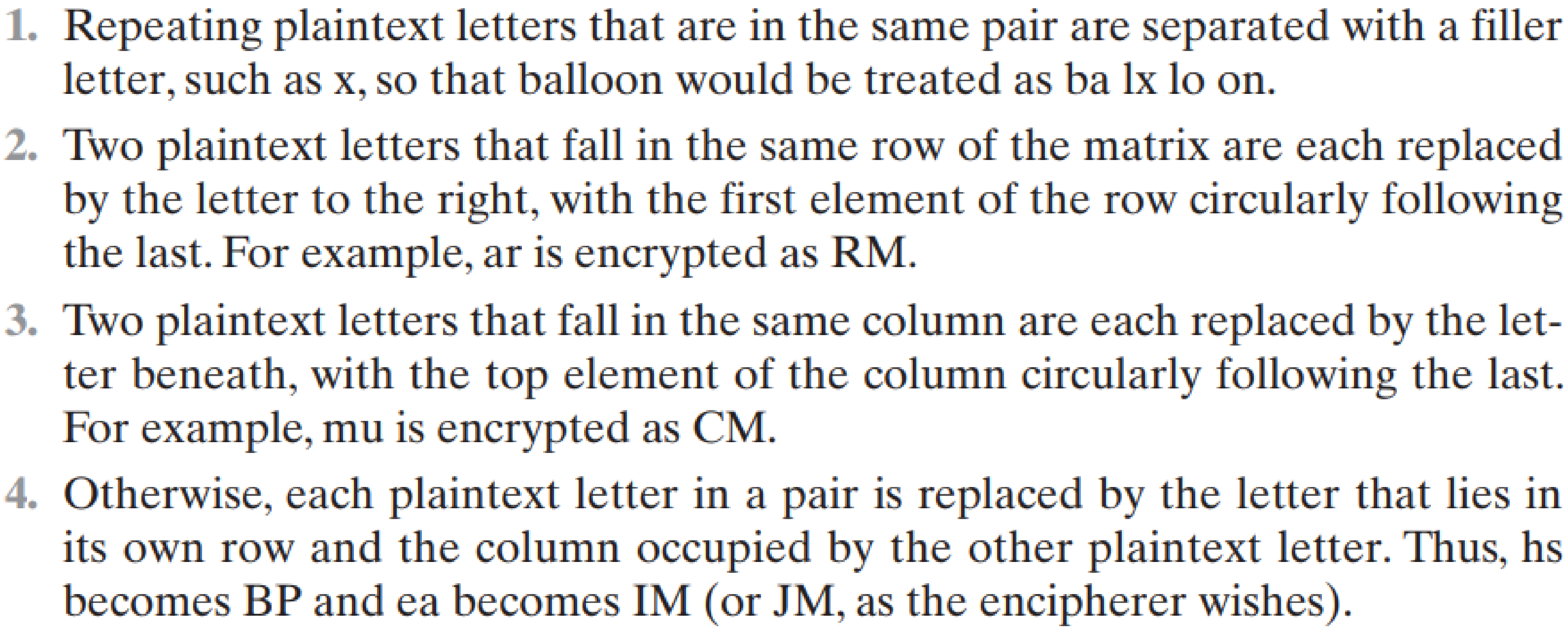
- The best known multiple letter encryption cipher is the playfair, which treats digrams in the plaintext as single units and translates these units into cipher text digrams.
- The Playfair algorithm is based on the use of a 5 * 5 matrix of letters constructed using a keyword.
- Let the keyword be “monarchy‟. The matrix is constructed by filling in the letters of the keyword(minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetical 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

SUBSTITUTION TECHNIQUES (Playfair **Cipher Contd..)**

- **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 encipherer wishes).

SUBSTITUTION TECHNIQUES (Playfair **Cipher Contd..)**

Construction of Diagrams for Plain text

Ex 1: PT = attack

at	**ta**	**ck**

Ex 2: PT = manipal

ma	**ni**	**pa**	**lx**

Ex 3: PT = balloon

ba	**lx**	**lo**	**on**

SUBSTITUTION TECHNIQUES (Playfair **Cipher Contd..)**

Construction of 5x5 Keyword matrix

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**

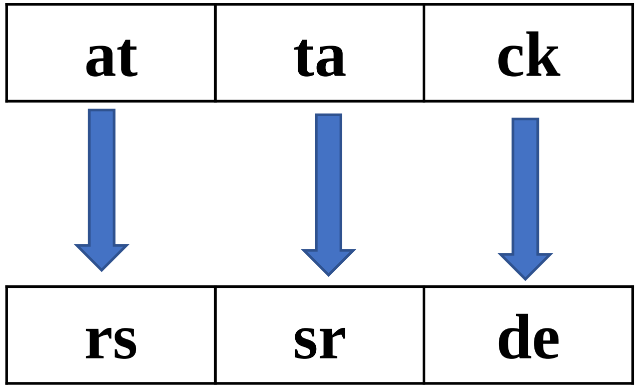
MANIPAL

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

SUBSTITUTION TECHNIQUES (Playfair Cipher Contd..)

PT = attack
KW = MONARCHY

Diagram=



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**

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**

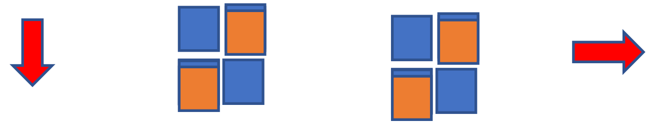
SUBSTITUTION TECHNIQUES (Playfair **Cipher Contd..)**

Encryption process

PT = balloon
KW = MONARCHY

Diagram=

ba	**lx**	**lo**	**on**



I/JB	**SU**	**PM**	**NA**

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**

SUBSTITUTION TECHNIQUES (Playfair **Cipher Contd..)**

- The Playfair cipher is a great advance over simple monoalphabetic ciphers.
- For one thing, whereas there are only 26 letters, there are 26 * 26 = 676 diagrams, so the identification of individual diagrams is more difficult.
- The relative frequencies of individual letters exhibit a much greater range than that of diagrams, making frequency analysis much more difficult. For these reasons, the Playfair cipher was for a long time considered unbreakable.
- Despite this level of confidence in its security, the Playfair cipher is relatively easy to break, because it still leaves much of the structure of the plaintext language intact. A few hundred letters of ciphertext are generally sufficient.

SUBSTITUTION TECHNIQUES (Playfair **Cipher Contd..)**

- **Rules for Decryption**

1. Two ciphertext letters in the same row of the matrix are each replaced by the letter to the left, with the last element of the row circularly following the first.
2. Two ciphertext letters that fall in the same column of the matrix are replaced by the letters above, with the bottom element of the column circularly following the top.
3. Otherwise, each ciphertext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other ciphertext letter.

SUBSTITUTION TECHNIQUES (Playfair **Cipher Contd..)**

- Find ciphertext for following :

Assume “communication” is the plaintext and “computer” is the encryption key.

Hill cipher:

- Can encipher **multiple letters** at a time
- No letter gets same cipher value after encryption
  - Ex: E(A) = Z
    E(A) = F
- **Developed by Lester Hill in 1929**
- Can encrypt a group of letters.
  - Ex: 2, 3 or more letters at a time (**diagraph, trigraph or polygraph)**
- Key is a squared matrix.
  - **2x2 ---- two letters can be encrypted at a time**
  - **3x3 --- three letters can be encrypted at a time**

SUBSTITUTION TECHNIQUES (Hill cipher Cont..)

Required math

- Linear algebra
  - Matrix multiplication
  - Arithmetic modulo (mod 26)
  - Square matrix
  - Determinant of matrix
  - Multiplicative inverse of matrix

Encryption

Decryption

SUBSTITUTION TECHNIQUES (Hill cipher Cont..)

- **Hill Algorithm**

$$\mathbf{C = E(K,P) = P\,K \bmod 26}$$

$$\mathbf{P = D(K,C) = C\,K^{-1} \bmod 26}$$

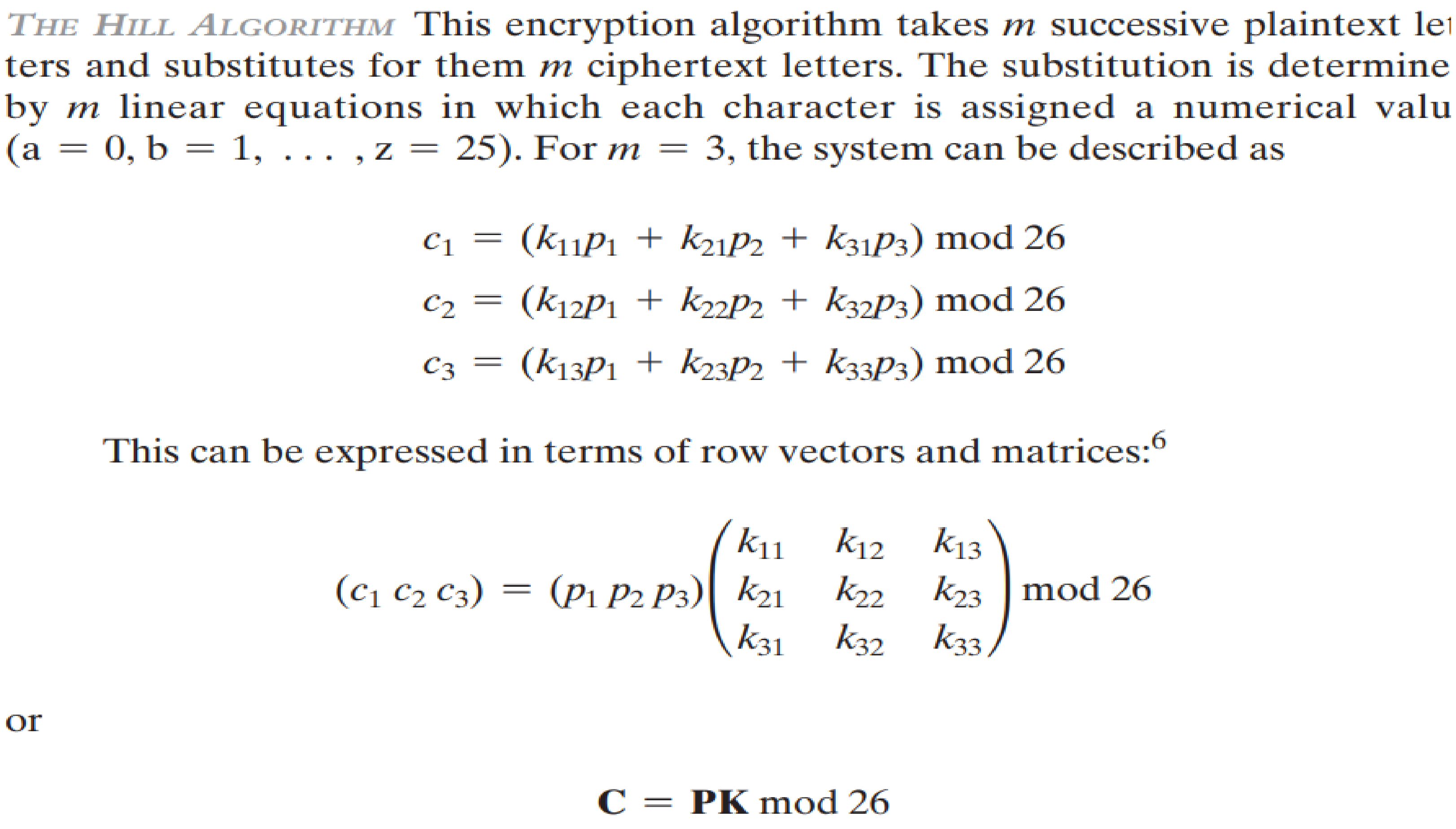
$$\mathbf{= P\,\underbrace{K\,K^{-1}}_{\text{Matrix Multiplication}} \bmod 26}$$

Note:

C and P are row vector of length 3.

K is a 3 x 3 matrix of encryption key

SUBSTITUTION TECHNIQUES (Hill cipher Cont..)



The Hill Algorithm This encryption algorithm takes m successive plaintext letters and substitutes for them m ciphertext letters. The substitution is determine by m linear equations in which each character is assigned a numerical valu (a = 0, b = 1, . . . , z = 25). For $m = 3$, the system can be described as

$$
\begin{aligned}
c_1 &= (k_{11}p_1 + k_{21}p_2 + k_{31}p_3) \bmod 26\\
c_2 &= (k_{12}p_1 + k_{22}p_2 + k_{32}p_3) \bmod 26\\
c_3 &= (k_{13}p_1 + k_{23}p_2 + k_{33}p_3) \bmod 26
\end{aligned}
$$

This can be expressed in terms of row vectors and matrices:[6]

$$(c_1\ c_2\ c_3) = (p_1\ p_2\ p_3)\begin{pmatrix} k_{11} & k_{12} & k_{13}\\ k_{21} & k_{22} & k_{23}\\ k_{31} & k_{32} & k_{33}\end{pmatrix} \bmod 26$$

or

$$\mathbf{C} = \mathbf{PK} \bmod 26$$

where C and P are row vectors of length 3 representing the plaintext and ciphertext, and K is a 3 * 3 matrix representing the encryption key. Operations are performed mod 26.

SUBSTITUTION TECHNIQUES (Hill cipher Cont..)

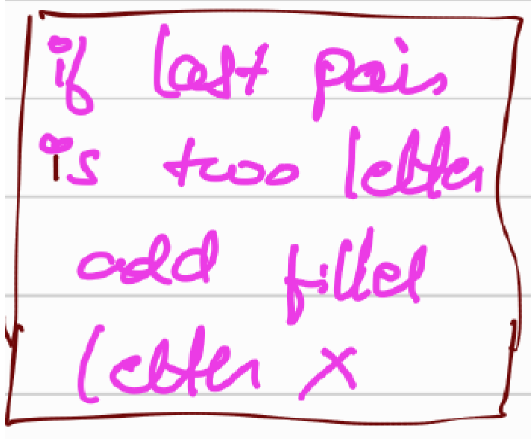
Example:

PT = “**paymoremoney**”

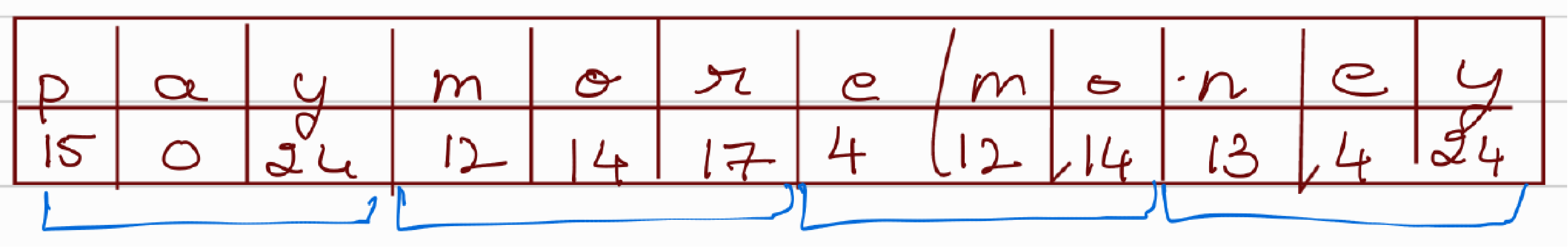
$$K = \begin{matrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{matrix}$$

Assume A = 0, Z = 25

Note:



if last pair is two letter add filler letter x



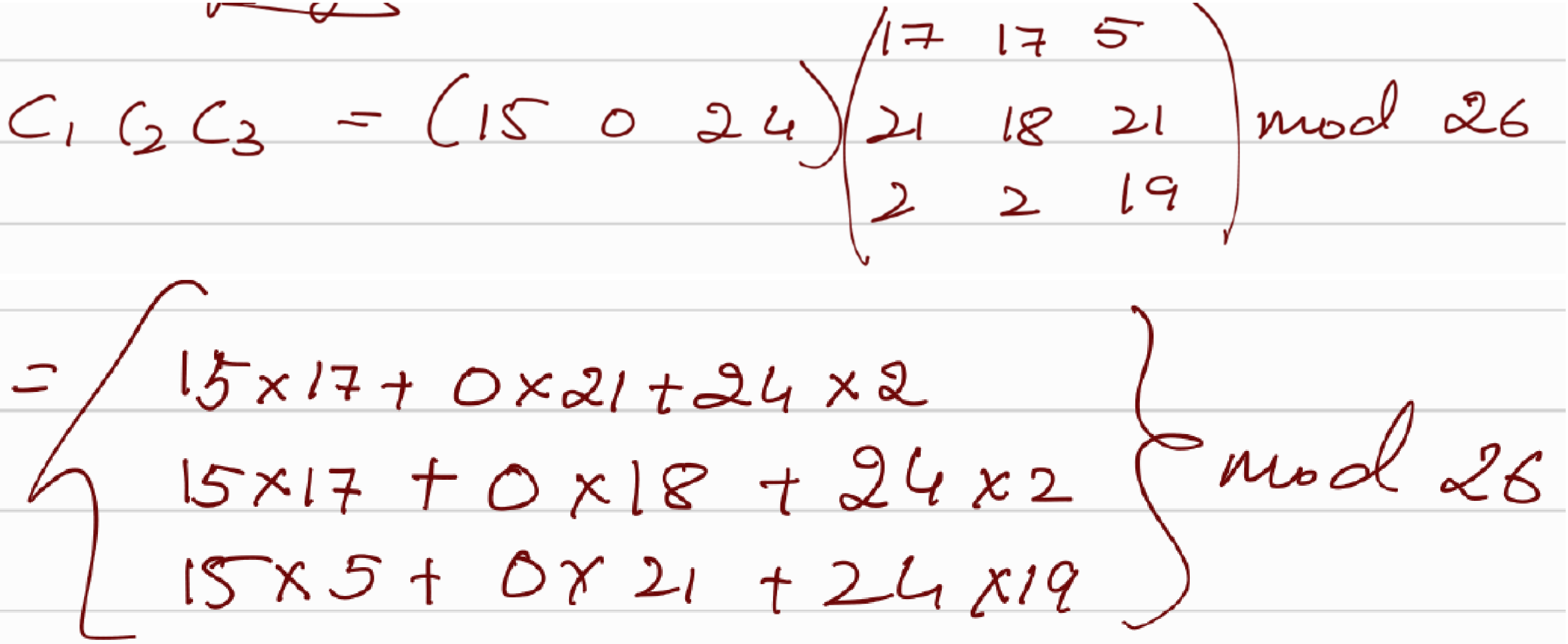
p	a	y	m	o	r	e	m	o	n	e	y
15	0	24	12	14	17	4	12	14	13	4	24

Note: as key is 3x3, it default that PT is grouped to 3 letters

SUBSTITUTION TECHNIQUES (Hill cipher Cont..)

- The first three letters of the plaintext are represented by the vector (15 0 24). Then (15 0 24)K = (303 303 531) mod 26 = (17 17 11) = RRL.

PT (p a y) = PT (15 0 24)



$$C_1 C_2 C_3 = (15 \quad 0 \quad 24)\begin{pmatrix}17 & 17 & 5\\ 21 & 18 & 21\\ 2 & 2 & 19\end{pmatrix} \bmod 26$$

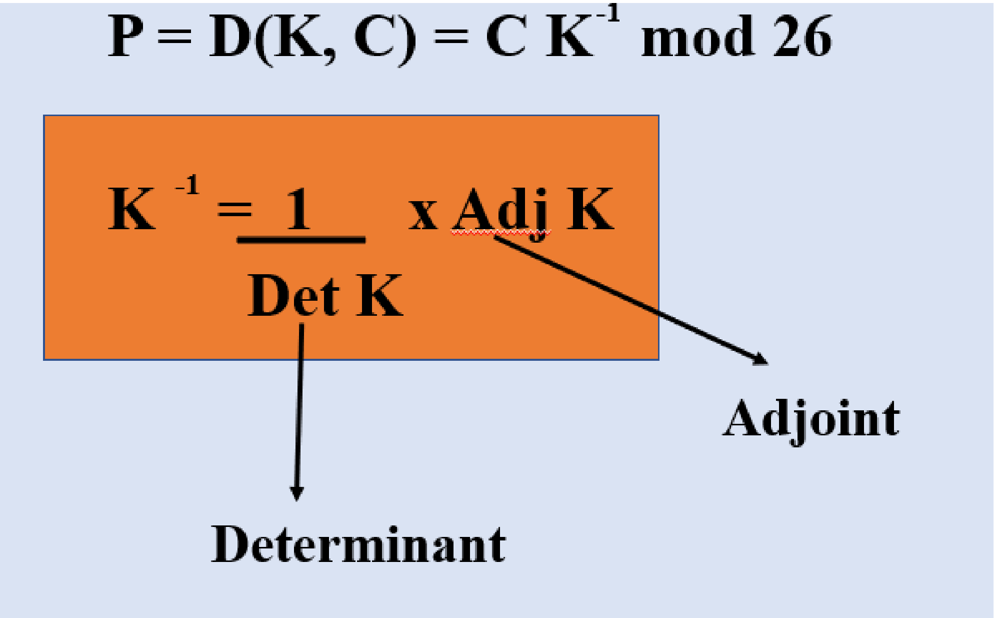
$$= \begin{Bmatrix} 15\times17+0\times21+24\times2\\ 15\times17+0\times18+24\times2\\ 15\times5+0\times21+24\times19 \end{Bmatrix} \bmod 26$$

PT = PAY MORE MONEY

CT = RRLMWBKASPDH

SUBSTITUTION TECHNIQUES (Hill cipher Cont..)

Decryption

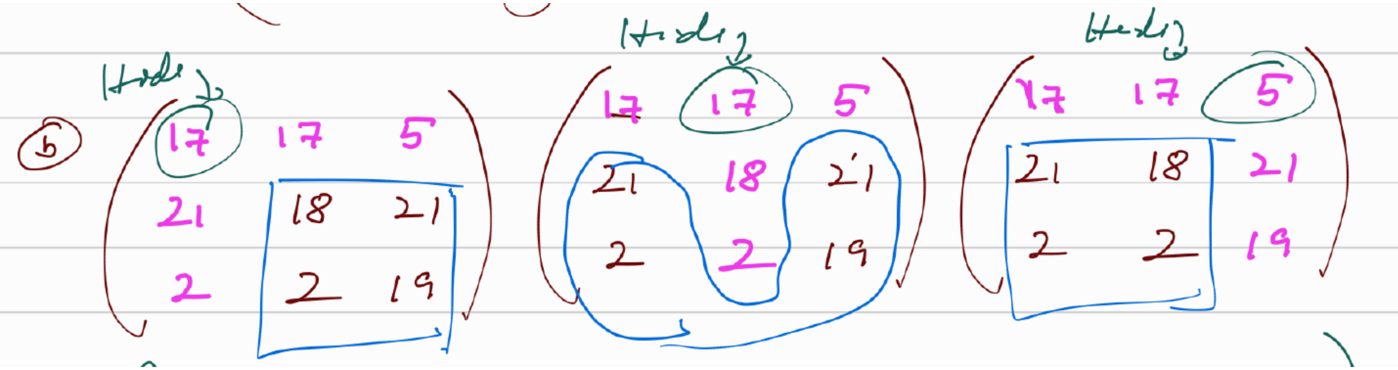


$$P = D(K, C) = C\,K^{-1} \bmod 26$$

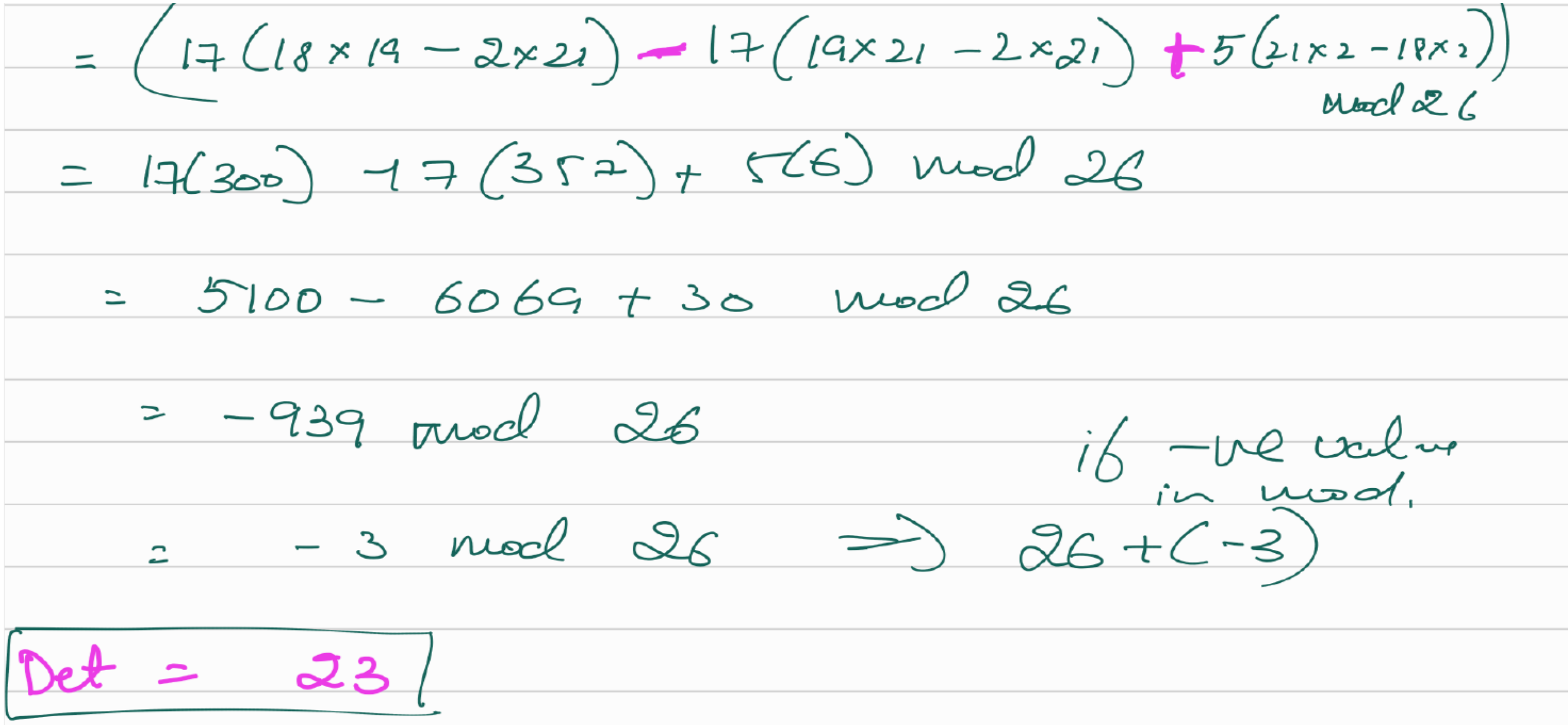
$$K^{-1} = \frac{1}{\text{Det } K} \times \text{Adj } K$$

$$\text{Det } K = \text{Det} \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \bmod 26$$

SUBSTITUTION TECHNIQUES (Hill cipher Cont..)



$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \quad \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \quad \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$



$$= \left(17(18\times19 - 2\times21) - 17(19\times21 - 2\times21) + 5(21\times2 - 18\times2)\right) \bmod 26$$

$$= 17(300) - 17(357) + 5(6) \bmod 26$$

$$= 5100 - 6069 + 30 \bmod 26$$

$$= -939 \bmod 26$$

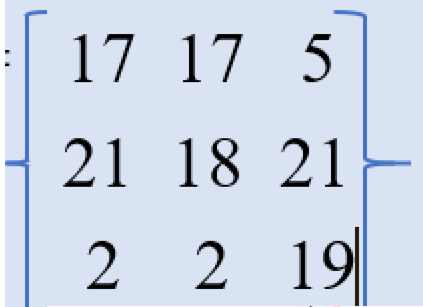
$$= -3 \bmod 26 \Rightarrow 26 + (-3)$$

if −ve value in mod.

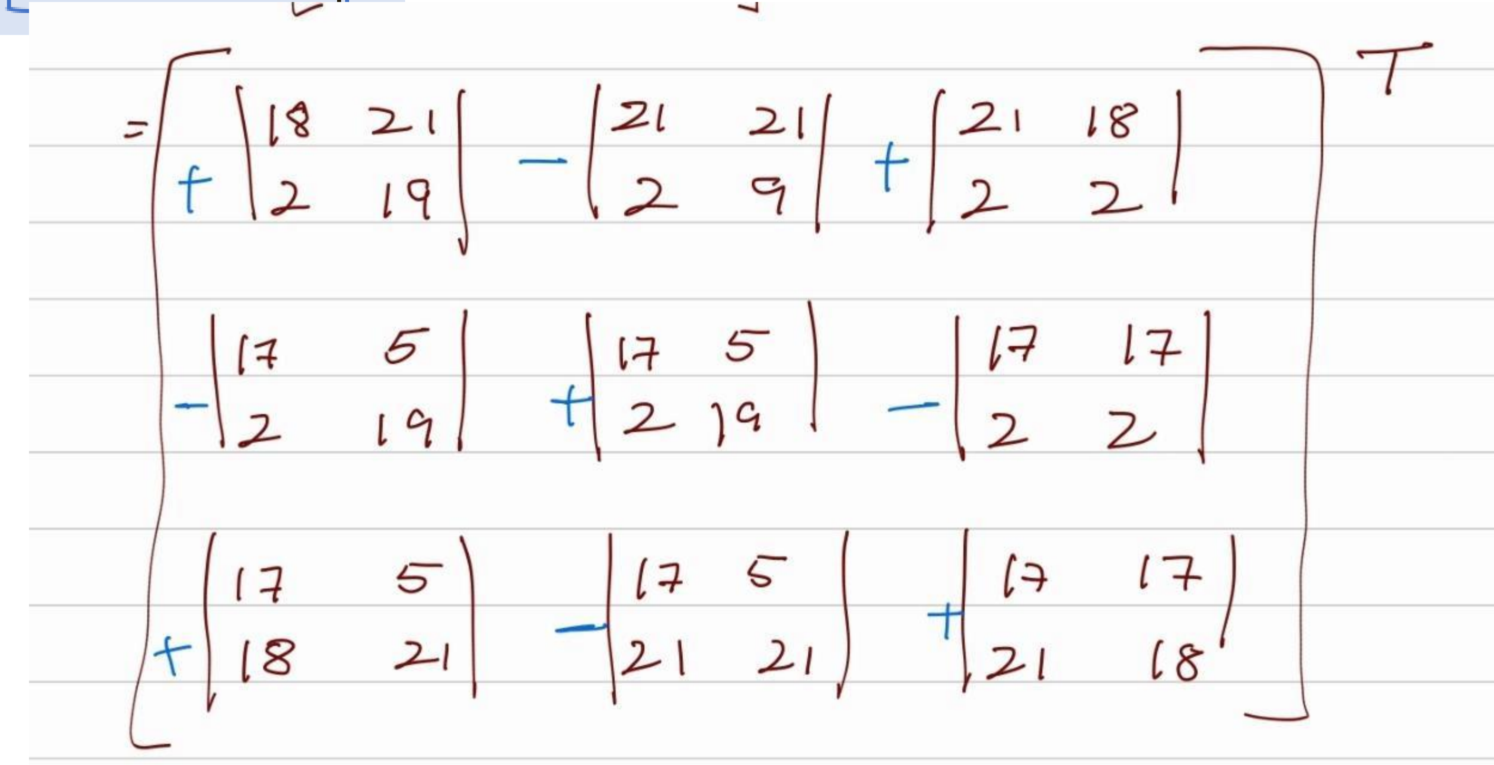
$$\boxed{\text{Det} = 23}$$

Example (contd..)

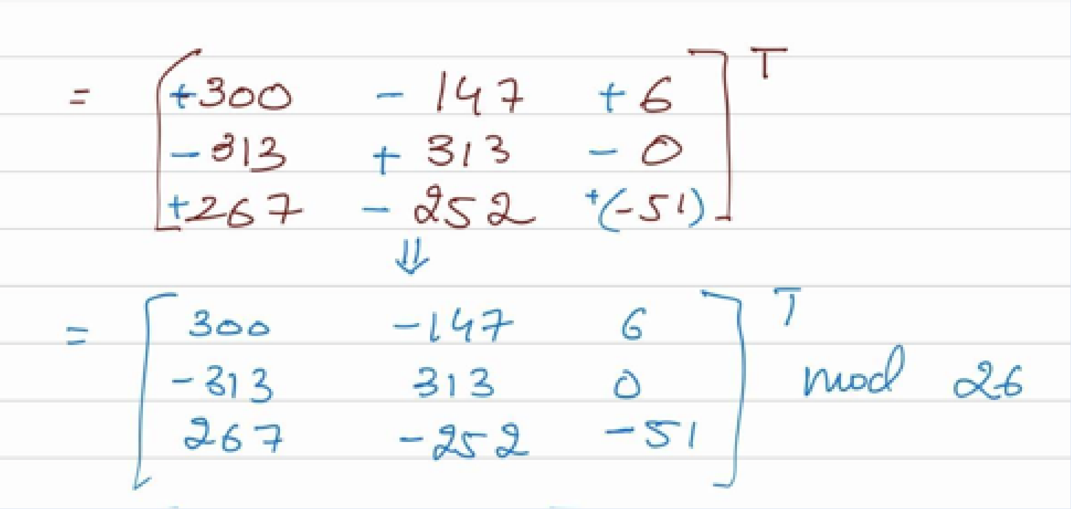
Adj K =



$$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$



$$= \begin{bmatrix} +\begin{vmatrix} 18 & 21 \\ 2 & 19 \end{vmatrix} & -\begin{vmatrix} 21 & 21 \\ 2 & 9 \end{vmatrix} & +\begin{vmatrix} 21 & 18 \\ 2 & 2 \end{vmatrix} \\ -\begin{vmatrix} 17 & 5 \\ 2 & 19 \end{vmatrix} & +\begin{vmatrix} 17 & 5 \\ 2 & 19 \end{vmatrix} & -\begin{vmatrix} 17 & 17 \\ 2 & 2 \end{vmatrix} \\ +\begin{vmatrix} 17 & 5 \\ 18 & 21 \end{vmatrix} & -\begin{vmatrix} 17 & 5 \\ 21 & 21 \end{vmatrix} & +\begin{vmatrix} 17 & 17 \\ 21 & 18 \end{vmatrix} \end{bmatrix}^T$$



$$= \begin{bmatrix} +300 & -147 & +6 \\ -313 & +313 & -0 \\ +267 & -252 & +(-51) \end{bmatrix}^T$$

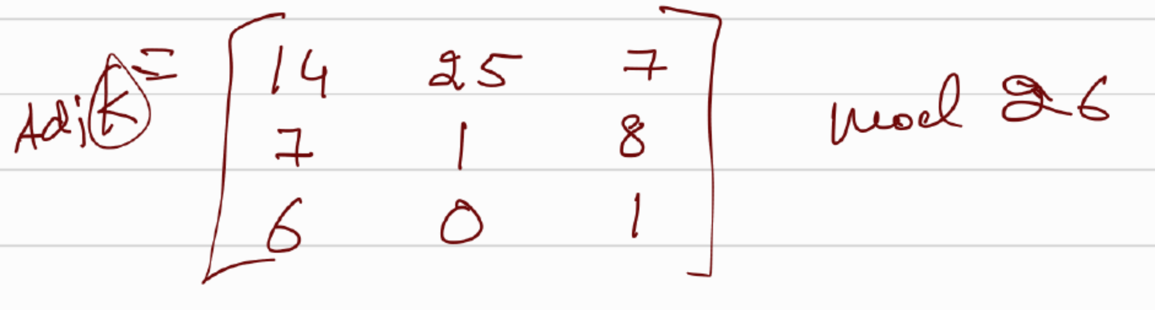
$$\Downarrow$$

$$= \begin{bmatrix} 300 & -147 & 6 \\ -313 & 313 & 0 \\ 267 & -252 & -51 \end{bmatrix}^T \bmod 26$$

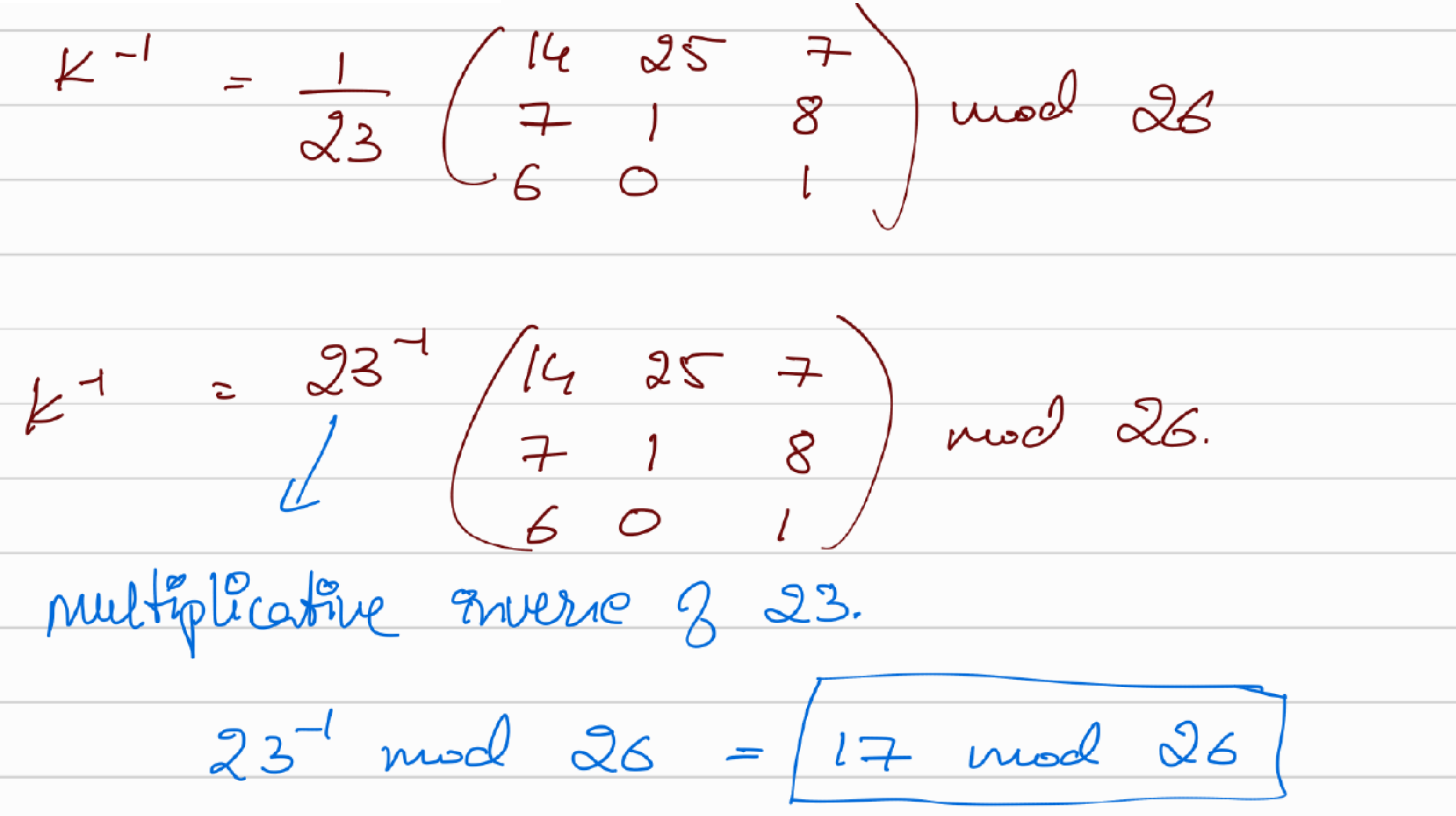
$$= \left\{ \begin{matrix} 14 & 7 & 6 \\ 25 & 1 & 0 \\ 7 & 8 & 1 \end{matrix} \right\}^T \Rightarrow = \left\{ \begin{matrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{matrix} \right\}$$

SUBSTITUTION TECHNIQUES (Hill cipher Cont..)

Example (contd..)



$$Adj(K) = \begin{bmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix} \bmod 26$$



$$K^{-1} = \frac{1}{23} \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \bmod 26$$

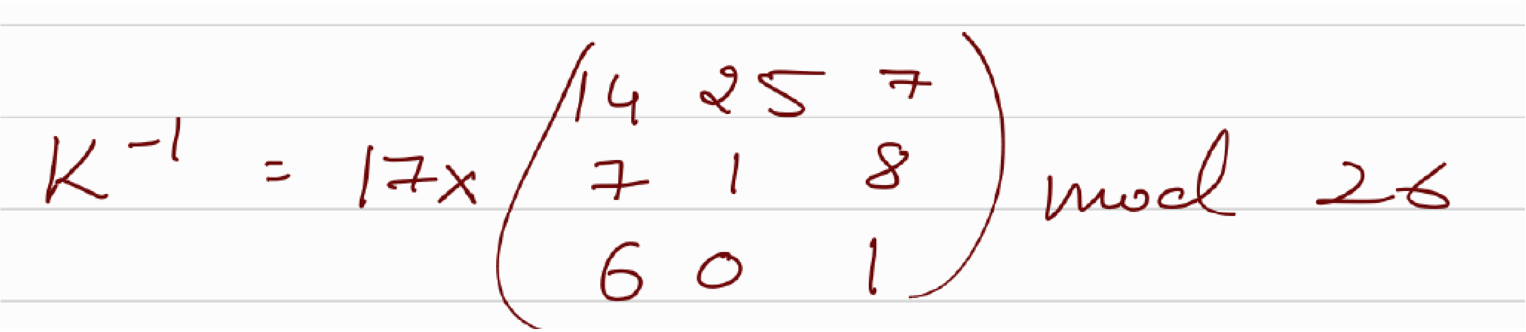
$$K^{-1} = 23^{-1} \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \bmod 26.$$

multiplicative inverse of 23.

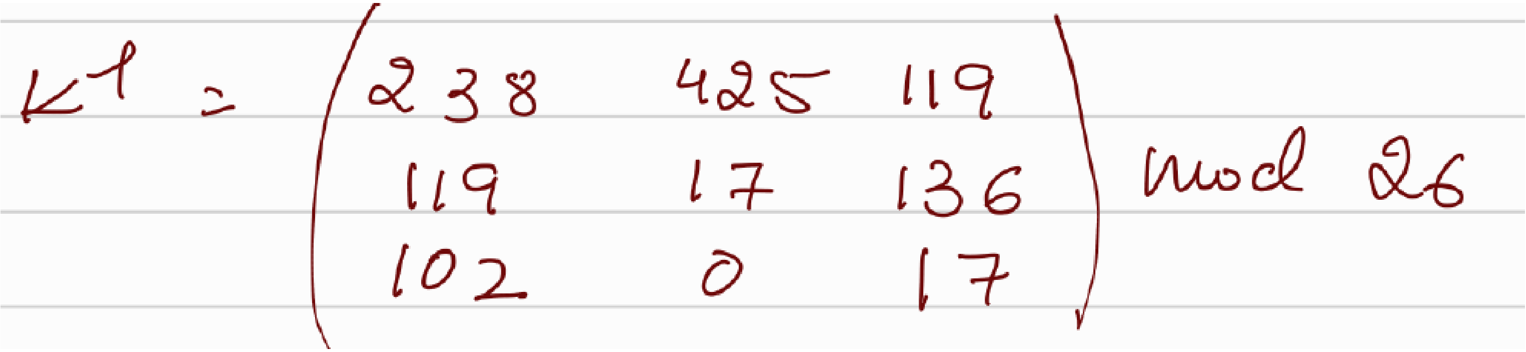
$$23^{-1} \bmod 26 = \boxed{17 \bmod 26}$$

SUBSTITUTION TECHNIQUES (Hill cipher Cont..)

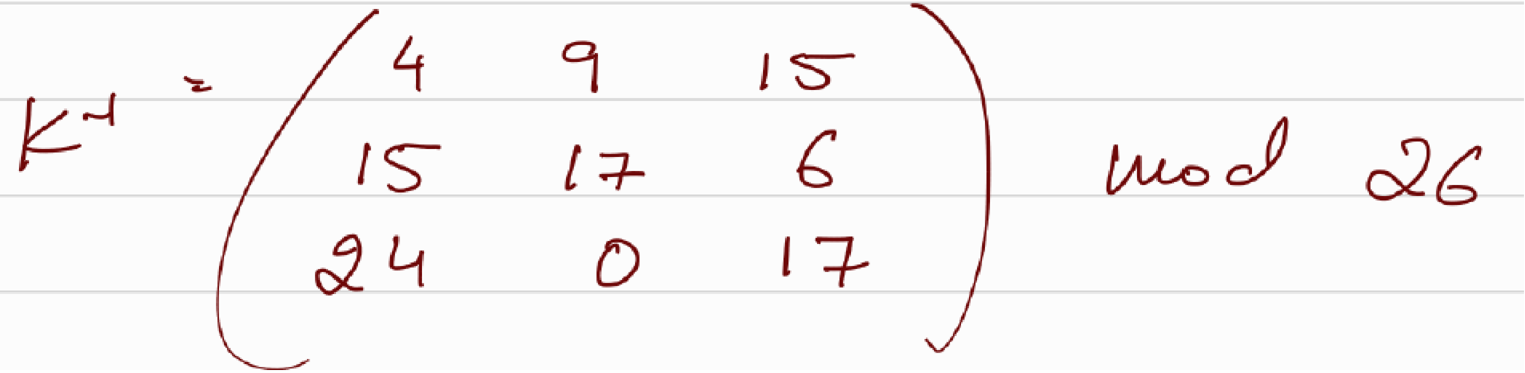
Example (contd..)



$$K^{-1} = 17 \times \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \bmod 26$$



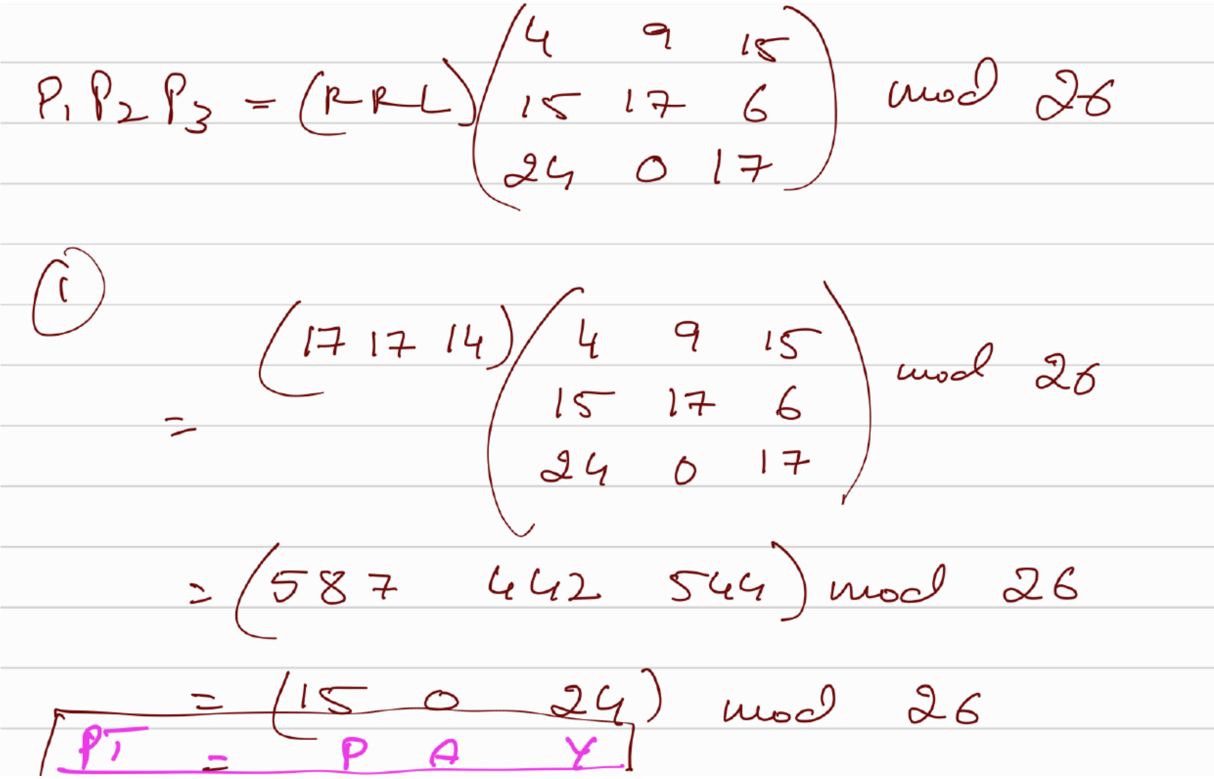
$$K^{-1} = \begin{pmatrix} 238 & 425 & 119 \\ 119 & 17 & 136 \\ 102 & 0 & 17 \end{pmatrix} \bmod 26$$



$$K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

Example (contd..)

CT = RRL MWB KAS PDH



$$P_1 P_2 P_3 = (R\ R\ L)\begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

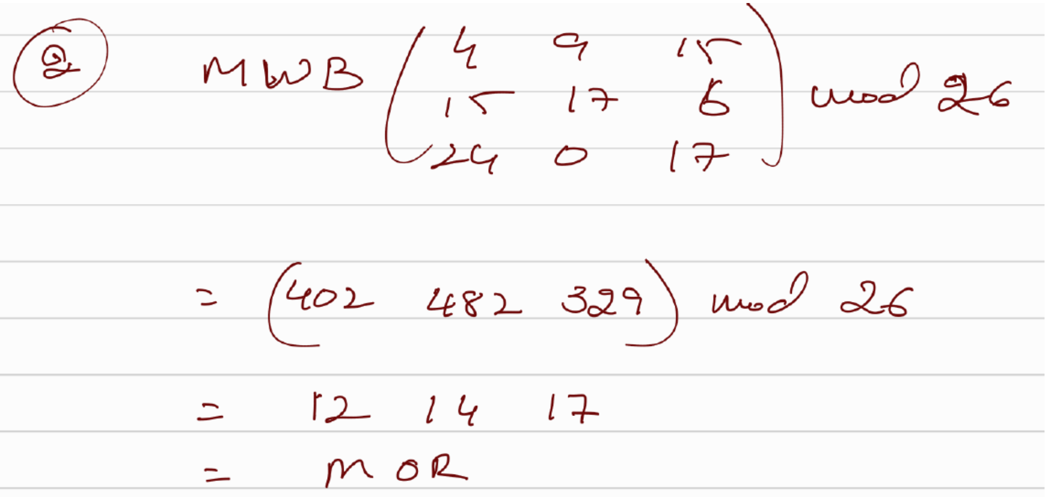
(i)

$$= (17\ 17\ 14)\begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

$$= (587 \quad 442 \quad 544) \bmod 26$$

$$= (15 \quad 0 \quad 24) \bmod 26$$

$$\boxed{PT = P \quad A \quad Y}$$

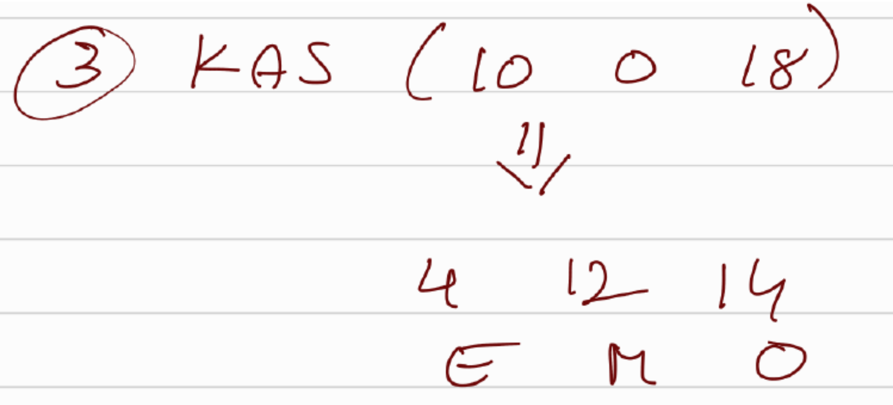


② $MWB \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$

$= \begin{pmatrix} 402 & 482 & 329 \end{pmatrix} \bmod 26$

$= 12 \quad 14 \quad 17$

$=$ MOR

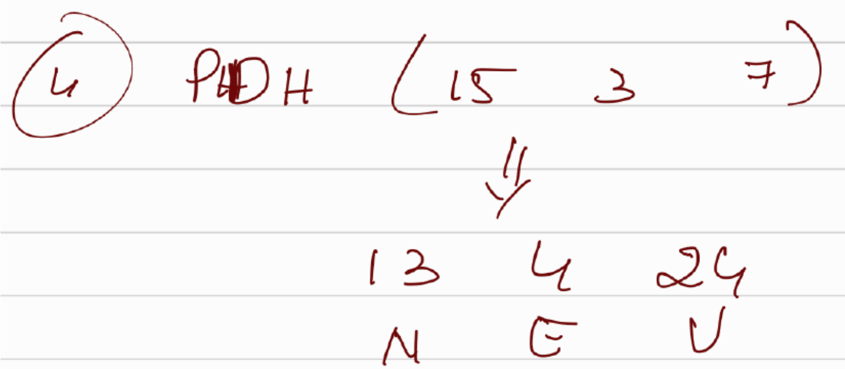


③ KAS $(10 \quad 0 \quad 18)$

$\Downarrow$

$4 \quad 12 \quad 14$

E M O



④ P~~H~~DH $(15 \quad 3 \quad 7)$

$\Downarrow$

$13 \quad 4 \quad 24$

N E V

Transposition Techniques

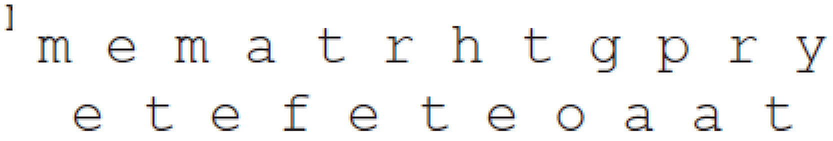
- Re-arrangement of letters based on permutation key.
- No replacement of letter
- Two variants:
  - Rail fence technique
  - Row transposition cipher.

Transposition Techniques (contd..)

Rail fence technique

- Here the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows to form a ciphertext.
- The number of columns in rail fence cipher remains equal to the length of plain-text message.

PT: “meet me after the toga party” with a rail fence of depth 2, we write the following:

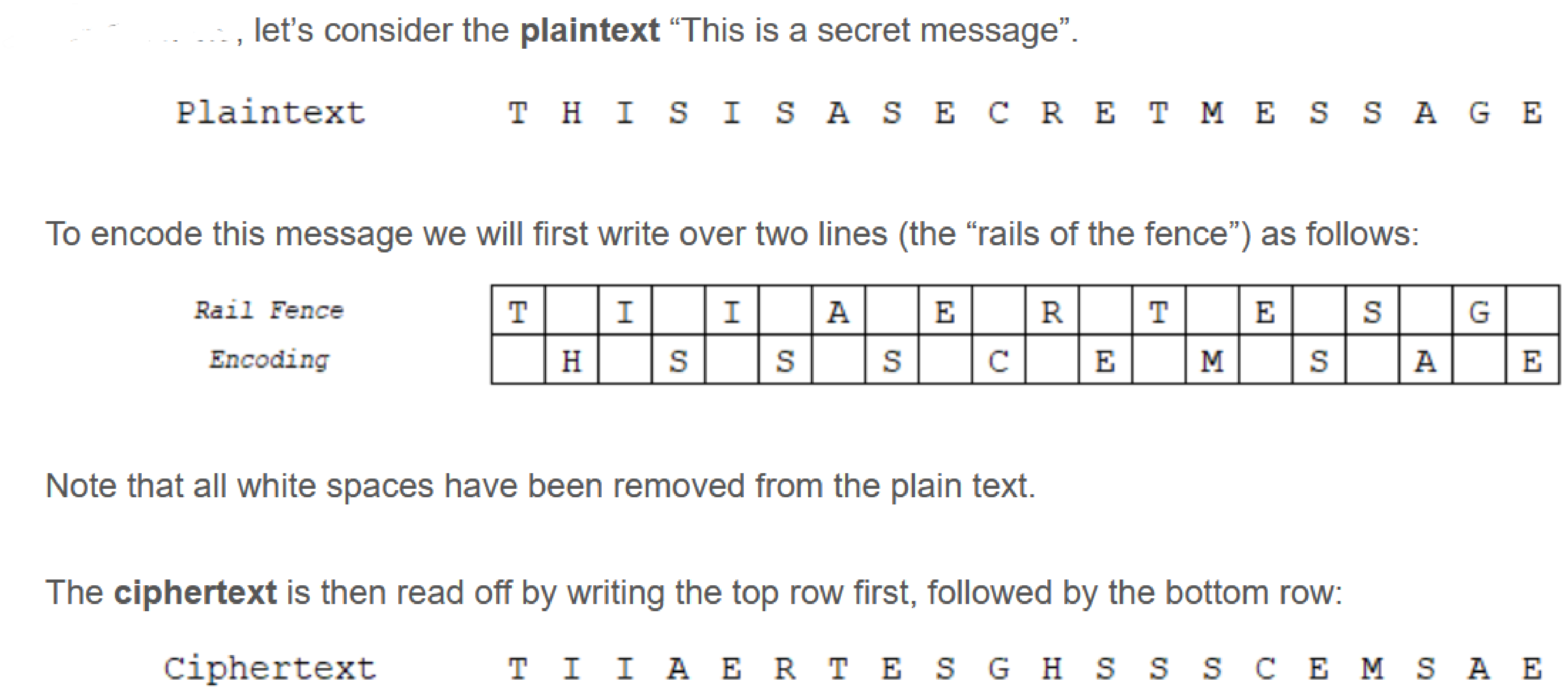


```
m e m a t r h t g p r y
 e t e f e t e o a a t
```

CT: MEMATRHTGPRYETEFETEOAAT

Note: used for short messages as easy to break

Transposition Techniques (contd..)



[illegible], let’s consider the **plaintext** “This is a secret message”.

```
Plaintext        T H I S I S A S E C R E T M E S S A G E
```

To encode this message we will first write over two lines (the “rails of the fence”) as follows:

Rail Fence	T		I		I		A		E		R		T		E		S		G	
Encoding		H		S		S		S		C		E		M		S		A		E

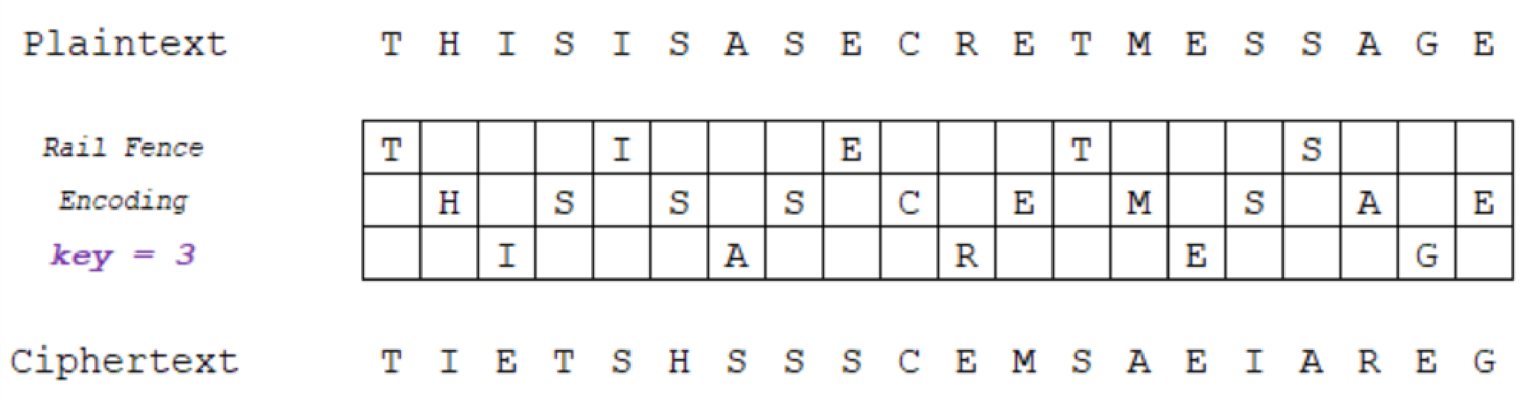
Note that all white spaces have been removed from the plain text.

The **ciphertext** is then read off by writing the top row first, followed by the bottom row:

```
Ciphertext       T I I A E R T E S G H S S S C E M S A E
```

Transposition Techniques (contd..)

Key = 3



Plaintext T H I S I S A S E C R E T M E S S A G E

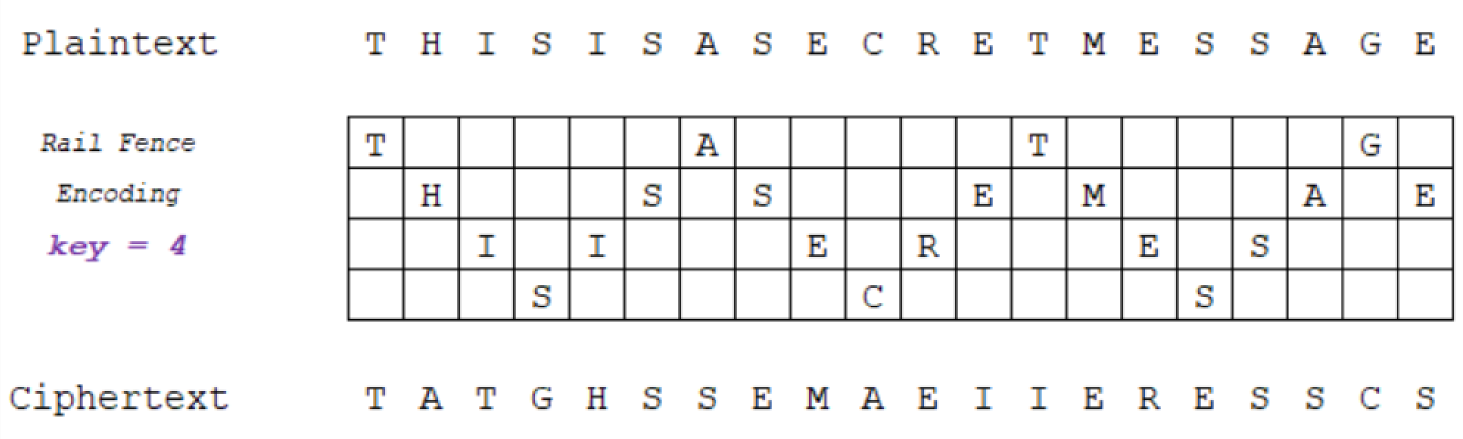
Rail Fence	T				I				E				T				S			
Encoding		H		S		S		S		C		E		M		S		A		E
key = 3			I				A				R				E				G	

Ciphertext T I E T S H S S S C E M S A E I A R E G

A Rail Fence Cipher with 3 “rails” (Key = 3)

Transposition Techniques (contd..)

Key = 4



Plaintext T H I S I S A S E C R E T M E S S A G E

Rail Fence	T						A						T						G	
Encoding		H				S		S				E		M				A		E
key = 4			I		I				E		R				E		S			
				S						C						S				

Ciphertext T A T G H S S E M A E I I E R E S S C S

A Rail Fence Cipher with 4 “rails” (Key = 4)

Transposition Techniques (contd..)

Row Transposition Cipher

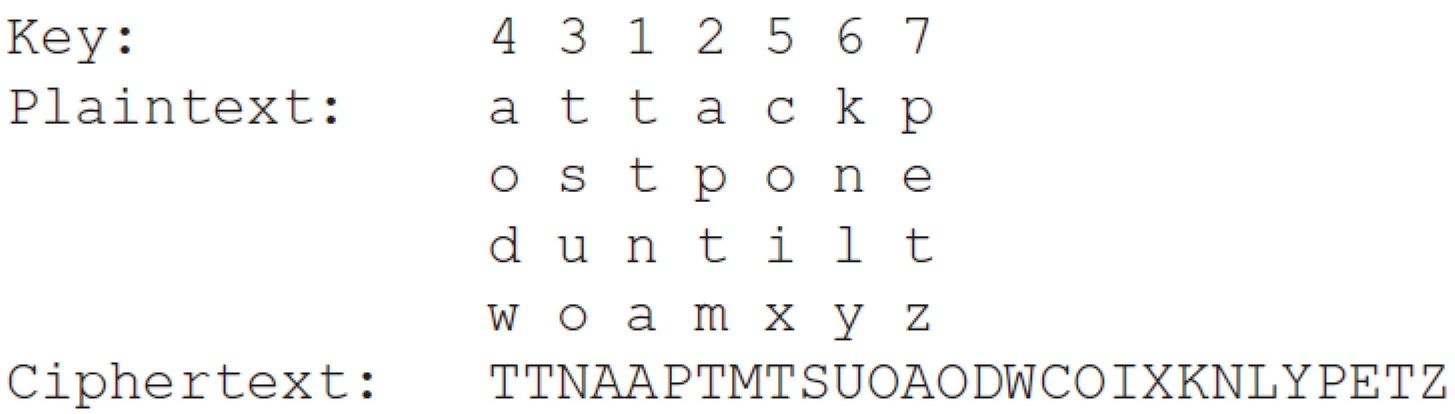
- A more complex scheme is to write the message in a rectangle
- The plaintext is written in a rectangle **row-by-row** matrix.
- The cipher is read **column-by-column** with permutation order mentioned by **key**.
- Key is value between 0 to 9.
  - Ex: 4 5 3 2 1

    4 2 1 3
- If key is a word then convert it to numeric value by assigning least letter as 1 and greatest letter as n.
  - Ex: **C R Y P T O**

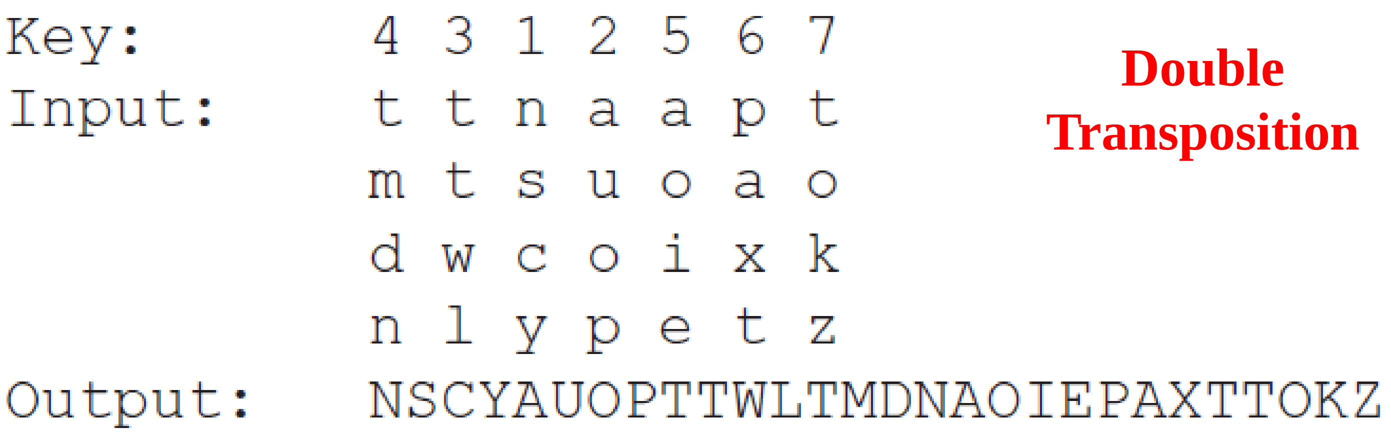
    1 4 6 3 5 2 ----- key

Transposition Techniques (contd..)

- **Example**



```
Key:          4 3 1 2 5 6 7
Plaintext:    a t t a c k p
              o s t p o n e
              d u n t i l t
              w o a m x y z
Ciphertext:   TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

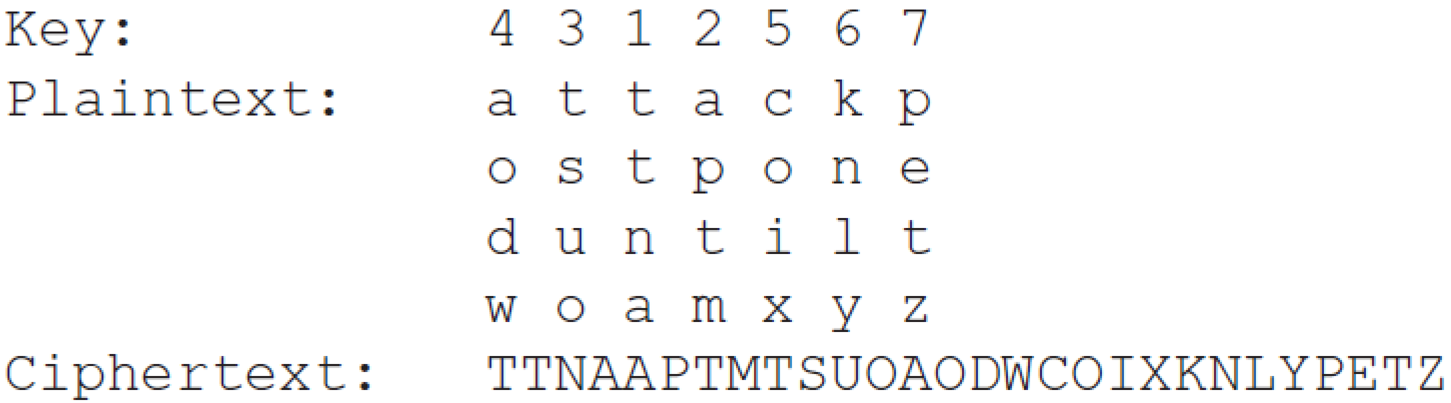


```
Key:       4 3 1 2 5 6 7
Input:     t t n a a p t
           m t s u o a o
           d w c o i x k
           n l y p e t z
Output:    NSCYAUOPTTWLTMDNAOIEPAXTTOKZ
```

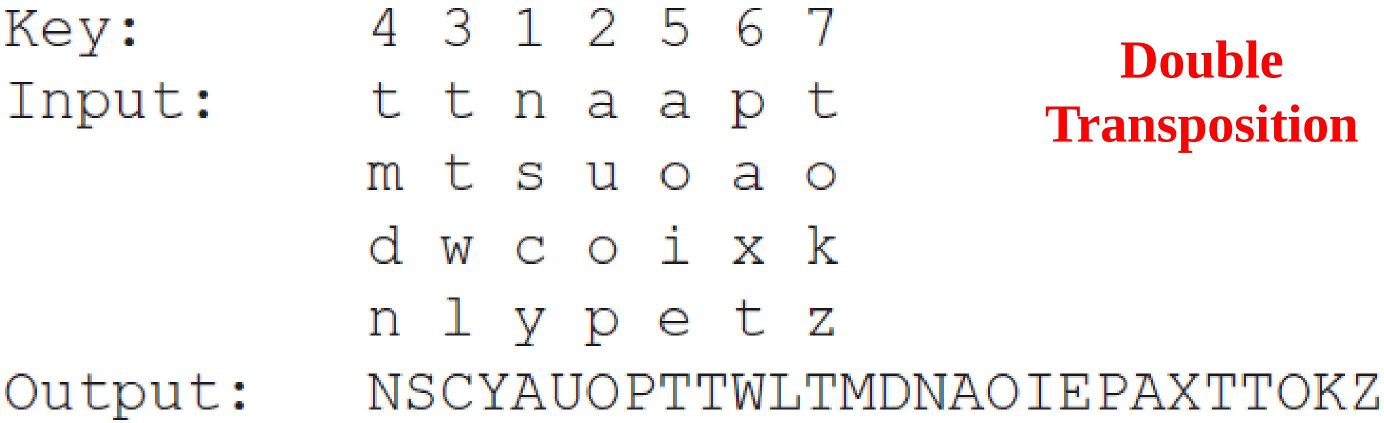
Double Transposition

Transposition Techniques (contd..)

- **Example**



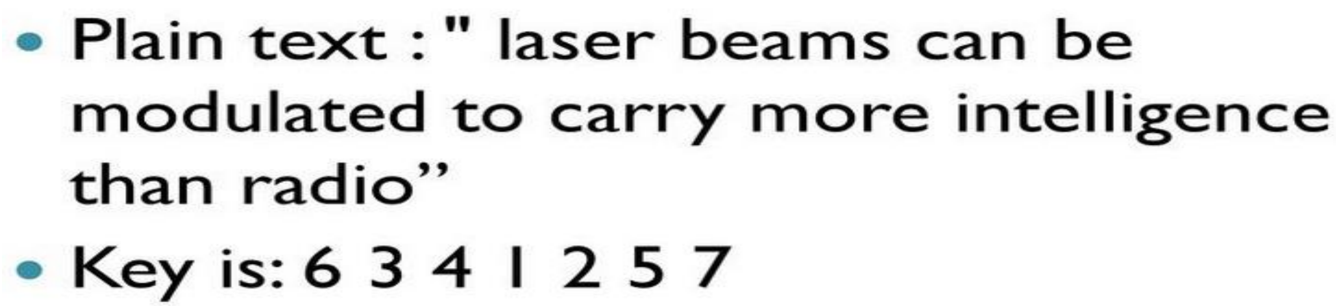
```
Key:          4 3 1 2 5 6 7
Plaintext:    a t t a c k p
              o s t p o n e
              d u n t i l t
              w o a m x y z
Ciphertext:   TTNAAPTMTSUOAODWCOIXKNLYPETZ
```



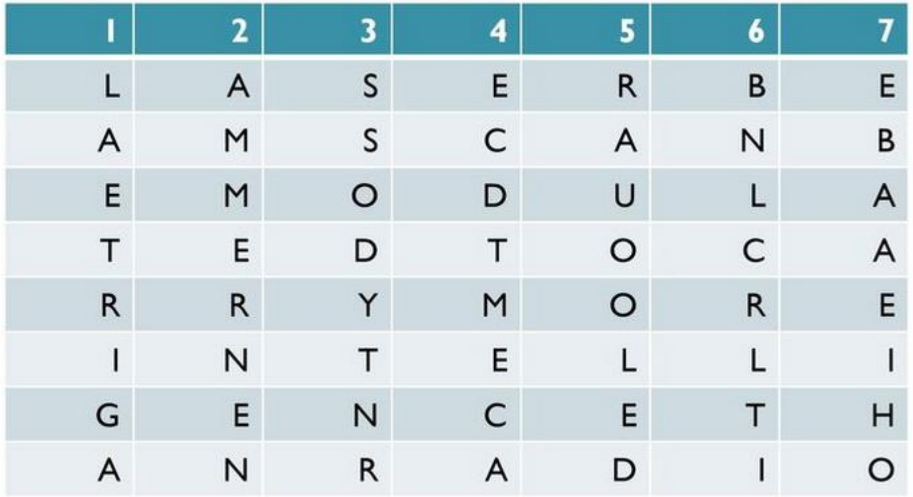
```
Key:        4 3 1 2 5 6 7
Input:      t t n a a p t
            m t s u o a o
            d w c o i x k
            n l y p e t z
Output:     NSCYAUOPTTWLTMDNAOIEPAXTTOKZ
```

Double Transposition

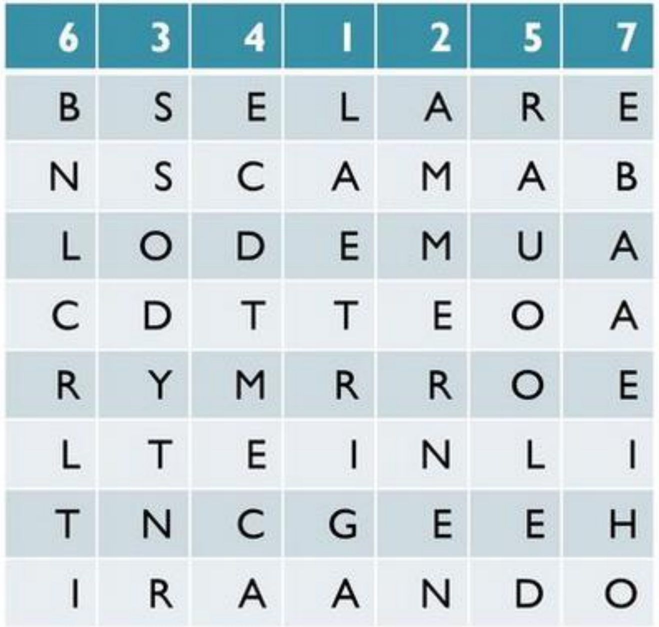
Assignment



- Plain text : " laser beams can be modulated to carry more intelligence than radio”
- Key is: 6 3 4 1 2 5 7



1	2	3	4	5	6	7
L	A	S	E	R	B	E
A	M	S	C	A	N	B
E	M	O	D	U	L	A
T	E	D	T	O	C	A
R	R	Y	M	O	R	E
I	N	T	E	L	L	I
G	E	N	C	E	T	H
A	N	R	A	D	I	O



6	3	4	1	2	5	7
B	S	E	L	A	R	E
N	S	C	A	M	A	B
L	O	D	E	M	U	A
C	D	T	T	E	O	A
R	Y	M	R	R	O	E
L	T	E	I	N	L	I
T	N	C	G	E	E	H
I	R	A	A	N	D	O

- " laser beams can be modulated to carry more intelligence than radio"

- Solution is :
- "bselare nscamab lodemua cdtteoa rymrroe lteinli tncg eeh iraando"