MODULE - I

INTRODUCTION

Data or information often travels from one system to another, leaving the safety of its protected physical surroundings. Once the data is out of hand, people with bad intention could modify or forge your data, either for amusement or for their own benefit.

Cryptography can reformat and transform our data, making it safer on its transmission between different systems. The technology is based on the essentials of secret codes, augmented by modern mathematical concepts and different algorithms that protect our data so that only intended can read and process it.

Security Attacks, Services and Mechanisms

To assess the security needs of an organization effectively, the manager responsible for security needs some systematic way of defining the requirements for security and characterization of approaches to satisfy those requirements. One approach is to consider three aspects of information security:

- **Security attack:** Any action that compromises the security of information owned by an organization.
- **Security mechanism:** A mechanism that is designed to detect, prevent or recover from a security attack.
- **Security service:** A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks and they make use of one or more security mechanisms to provide the service.

THE OSI SECURITY ARCHITECTURE

ITU-T Recommendation X.800, Security Architecture for OSI, defines a systematic approach of organizing the task of providing security. This architecture was developed as an international standard, computer and communications vendors have developed security features for their products and services that relate to this structured definition of services and mechanisms.

X.800 defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers.

X.800 divides these services into five categories which are listed below

- **Authentication:** The authentication service is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from. In the case of an ongoing interaction, such as the connection of a terminal to a host, two aspects are involved. First, at the time of connection initiation, the service assures that the two entities are authentic, that is, that each is the entity that it claims to be. Second, the service must assure that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purposes of unauthorized transmission or reception.
- **Access control:** It is the ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.
- **Data Confidentiality** is the protection of transmitted data from passive attacks with respect to the content of a data transmission.
- **Data integrity** can apply to a stream of messages, a single message, or selected fields within a message. A connection-oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays and destruction of data. On the other hand, a connectionless integrity service, one that provides protection against message modification only.
- **Non-repudiation** prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

Security Attacks

1. Passive Attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Passive attacks are of two types:

- **Release of message contents:** A telephone conversation, an e-mail message and a transferred file may contain sensitive or confidential information. We would like to prevent the opponent from learning the contents of these transmissions.

- **Traffic analysis**: If we had encryption protection in place, an opponent might still be able to observe the pattern of the message. The opponent could determine the location and identity of communication hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of communication that was taking place.

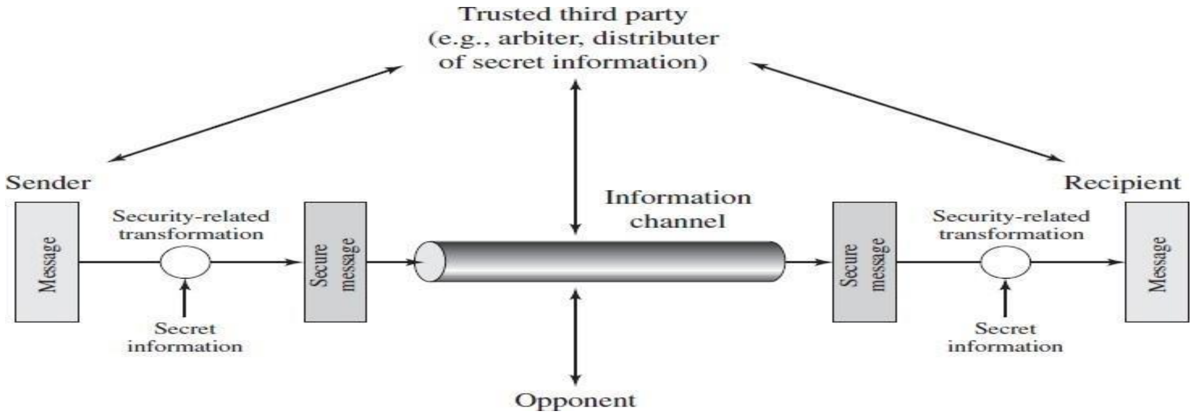
Passive attacks are very difficult to detect because they do not involve any alteration of data. However, it is feasible to prevent the success of these attacks.

2. Active attacks

These attacks involve some modification of the data stream or the creation of a false stream. These attacks can be classified in to four categories:

- **Masquerade** – One entity pretends to be a different entity.
- **Replay** – involves passive capture of a data unit and its subsequent transmission to produce an unauthorized effect.
- **Modification of messages** – Some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect.
- **Denial of service** – Prevents or inhibits the normal use or management of communication facilities. Another form of service denial is the disruption of an entire network, either by disabling the network or overloading it with messages so as to degrade performance. It is quite difficult to prevent active attacks absolutely, because to do so would require physical protection of all communication facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them.

A MODEL FOR NETWORK SECURITY



Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on.

All the techniques for providing security have two components:

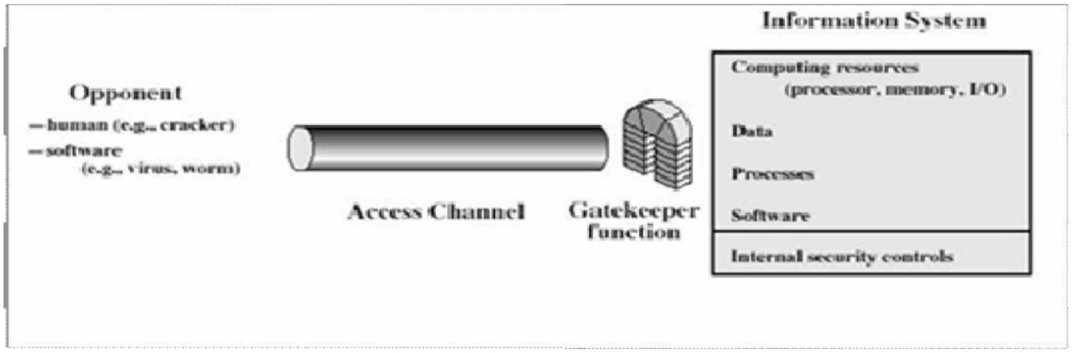
- A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.
- Some secret information shared by the two principals and, it is unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent.

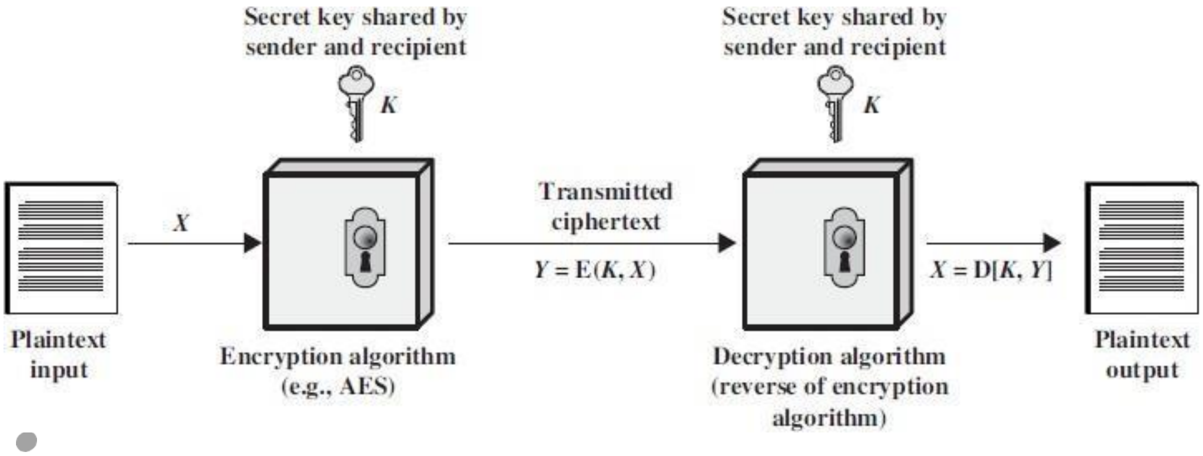
Using this model requires us to:

- Design a suitable algorithm for the security transformation
- Generate the secret information (keys) used by the algorithm
- Develop methods to distribute and share the secret information
- Specify a protocol enabling the principals to use the transformation and secret information for a security service
- Select appropriate gatekeeper functions to identify users
- Implement security controls to ensure only authorized users access designated information or resources

- Trusted computer systems can be used to implement this model



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

Here the original message, referred to as plaintext, is converted into apparently random scrambled message, referred to as cipher text. The encryption process consists of an algorithm and a key. The secret key is a value independent of the plaintext. Changing the key changes the output of the algorithm. Once the cipher text is produced, it may be transmitted. Upon reception, the cipher text can be transformed back to the original plaintext by using a decryption algorithm and the same key that was used for encryption. The security depends on several factors. First, the encryption algorithm must be powerful enough that it is impractical to decrypt a message on the basis of cipher text alone. Beyond that, the security depends on the secrecy of the key, not the secrecy of the algorithm.

Two requirements for secure use of symmetric encryption:

- A strong encryption algorithm
- A secret key known only to sender / receiver.

Assume encryption algorithm is known and implies a secure channel to distribute key A source produces a message in plaintext, X = [X1, X2… X_M] where M are the number of letters in the message. A key of the form K = [K1, K2… K_J] is generated. If the key is generated at the source, then it must be provided to the destination by means of some secure channel.

With the message X and the encryption key K as input, the encryption algorithm forms the cipher text Y = [Y1, Y2, YN]. This can be expressed as

$$Y = E_K(X)$$

The intended receiver, in possession of the key, is able to invert the transformation:

$$X = D_K(Y)$$

An opponent, observing Y but not having access to K or X, may attempt to recover X or K or both. It is assumed that the opponent knows the encryption and decryption algorithms.

If the opponent is interested in only this particular message, then the focus of effort is to recover X by generating a plaintext estimate. Often if 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.

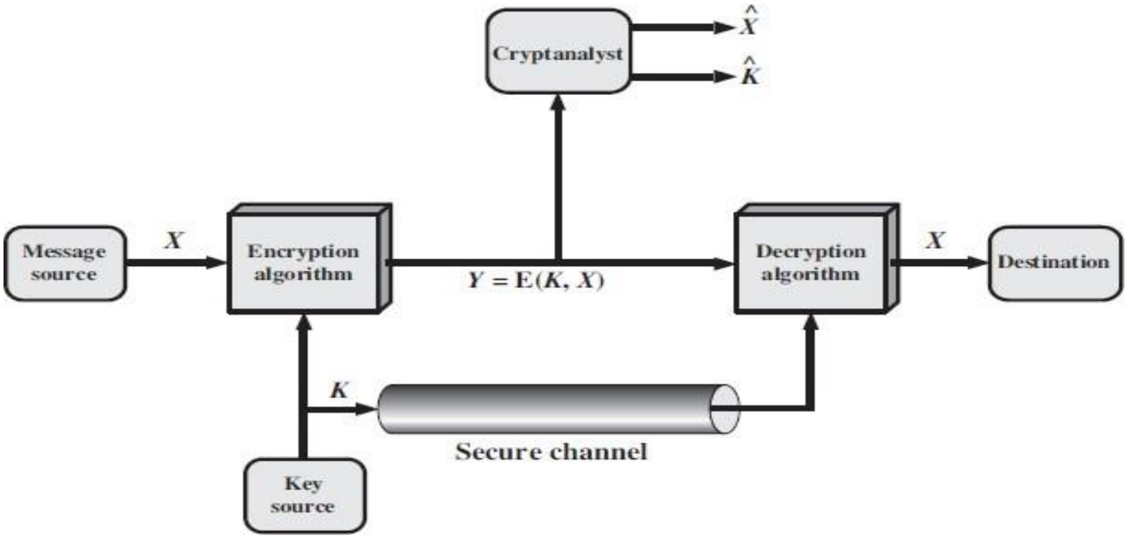


Fig. Model of symmetric crypto system

CLASSICAL ENCRYPTION TECHNIQUES

There are two basic building blocks of all encryption techniques:

- Substitution
- Transposition.

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 cipher text bit patterns.

Caesar cipher (or) shift cipher

The earliest known use of a substitution cipher and the simplest was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing 3 places further down the alphabet.

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

e.g., plain text: PAY MORE MONEY Cipher text: SDB PRUH PRQHB

Note that the alphabet is wrapped around, so that letter following „z‟ is „a‟. For each plaintext letter p , substitute the cipher text letter c such that

$$C = E(p) = (p+3) \bmod 26$$

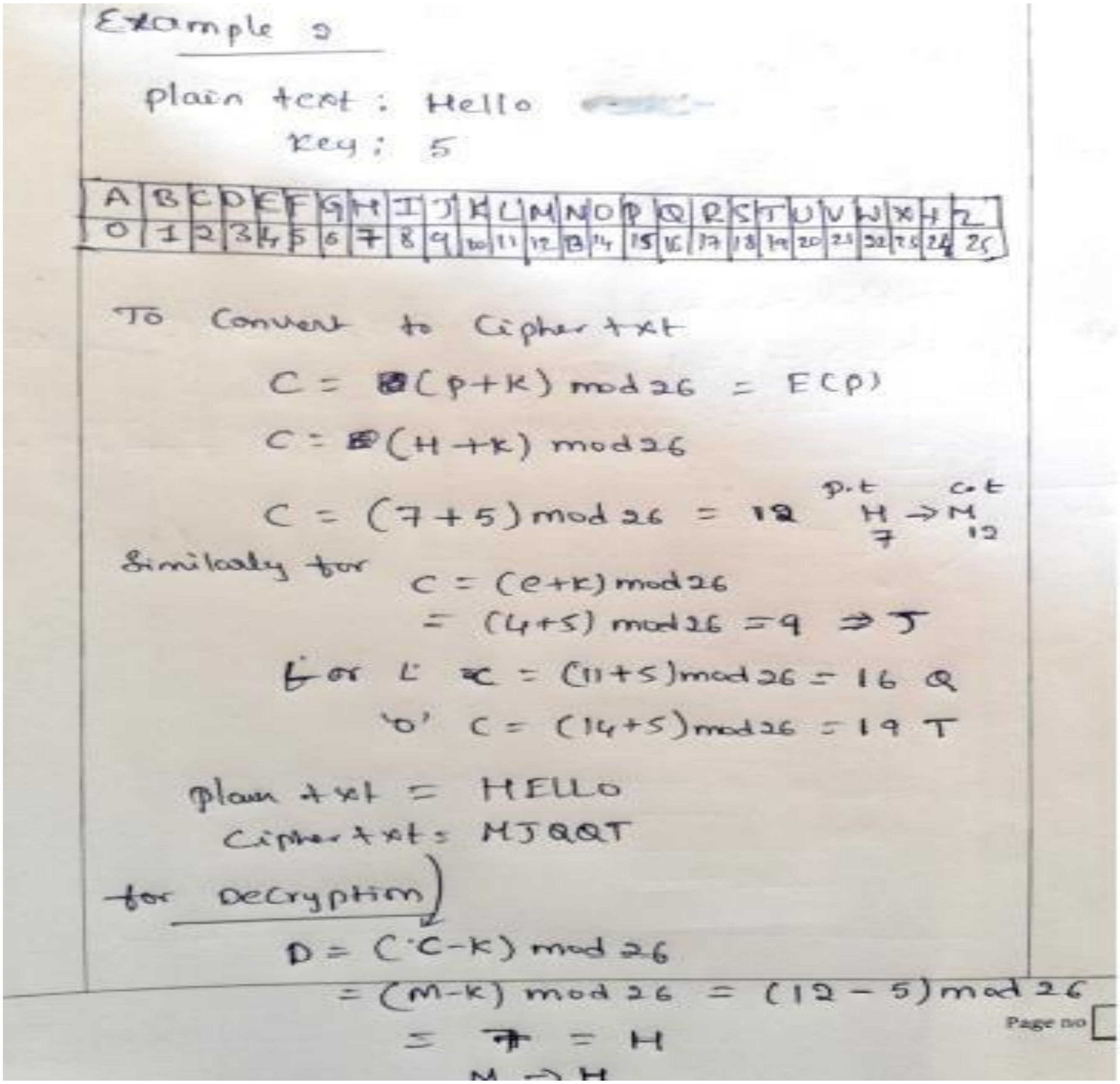
A shift may be any amount, so that general Caesar algorithm is

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

Where k takes on a value in the range 1 to 25.

The decryption algorithm is simply

$$P = D(C) = (C-k) \bmod 26$$



Example 2

plain text : Hello

key : 5

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
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

To Convert to Cipher txt

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

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

$C = (7+5) \bmod 26 = 12$ $\quad \overset{p.t}{\underset{7}{H}} \rightarrow \overset{c.t}{\underset{12}{M}}$

Similarly for $C = (e+k) \bmod 26$

$= (4+5) \bmod 26 = 9 \Rightarrow J$

for 'L' $C = (11+5) \bmod 26 = 16$ Q

'o' $C = (14+5) \bmod 26 = 19$ T

plain txt = HELLO

Cipher txt = MJQQT

for Decryption

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

$= (M-k) \bmod 26 = (12-5) \bmod 26$

$= 7 = H$

$M \rightarrow H$

Page no

Mono-alphabetic Ciphers: with only 25 possible keys, the Caesar cipher is far from secure.

If, instead, the "cipher" line can be any permutation of the 26 alphabetic characters, then there are 26! Or greater than 4 x 10^{26} possible keys. This is 10 orders of magnitude greater than the key space for DES and would seem to eliminate brute-force techniques for cryptanalysis. Such an approach is referred to as a mono-alphabetic substitution cipher, because a single cipher alphabet (mapping from plain alphabet to cipher alphabet) is used per message

EXAMPLE:

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

“A" can be encrypted to any of the 26 letter. In above case A in encrypted with X We can use any of 26 letters like A –M or A –P

PLAIN TEXT: **L I F E I S W H A T Y O U M A K E I T**

CIPHER TEXT: **D U R Q U K O B X L T G M E X C Q U L**

There is, however, another line of attack. If the cryptanalyst knows the nature of the plaintext then the analyst can exploit the regularities of the language

Play fair cipher

- The best known multiple letter encryption cipher is the play fair, which treats diagrams in the plaintext as single units and translates these units into cipher text diagrams.
- The play fair algorithm is based on the use of 5x5 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 letter “I” and “j” count as one letter.

Plaintext is encrypted two letters (pair) at a time According to the following rules:

- Repeating plaintext letters that would fall in the same pair are separated with a Filler letter such as “X”.

Example: plain text- MEET ME AT THE SCHOOL HOUSE

Pairing two letters – ME ET ME AT TH ES CH OO LH OU SE

⇓

Repeating plaintext letters in a pair so it is separated with filler letter as – OX

Now pairing two letters will be – ME ET ME AT TH ES CH OX OL HO US E

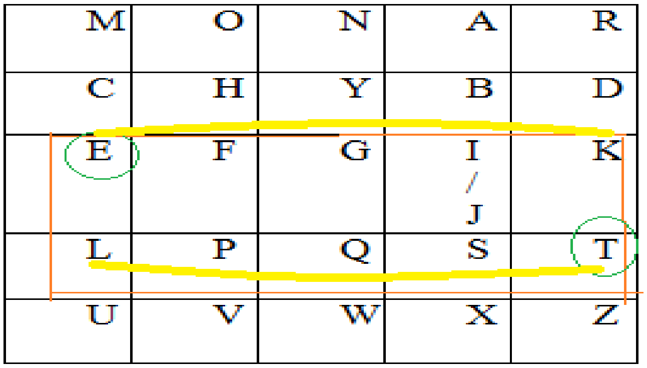
⇓

Single letter has to be paired with the filler letter

Finally splitting two letters as a unit => ME ET ME AT TH ES CH OX OL HO US EX

- 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 following the last.
- Plaintext letters that fall in the same column are replaced by the letter beneath, with the top element of the column following the last.
- Otherwise, each plaintext letter is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.

Example: Keyword is – MONARCHY
Plain text- MEET ME AT THE SCHOOL HOUSE



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 = MEET ME AT THE SCHOOL HOUSE
Splitting two letters as a unit => ME ET ME AT TH ES CH OX OL HO US EX

Corresponding cipher text => CL KL CL RS PD IL HY AV MP FH XL IU

Strength of play fair cipher

Play fair cipher is a great advance over simple mono alphabetic ciphers.
Since there are 26 letters, 26x26 = 676 diagrams are possible, so identification of individual diagram is more difficult.

Hill Cipher:

Hill cipher was developed by the mathematician Lester Hill in 1929. 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

c1 = (k_{11}P1 + k_{12}P2 + k_{13}P3) mod 26 c2 = (k_{21}P1 + k_{22}P2 + k_{23}P3) mod 26 c3 = (k_{31}P1 + k_{32}P2 + k_{33}P3) mod 26

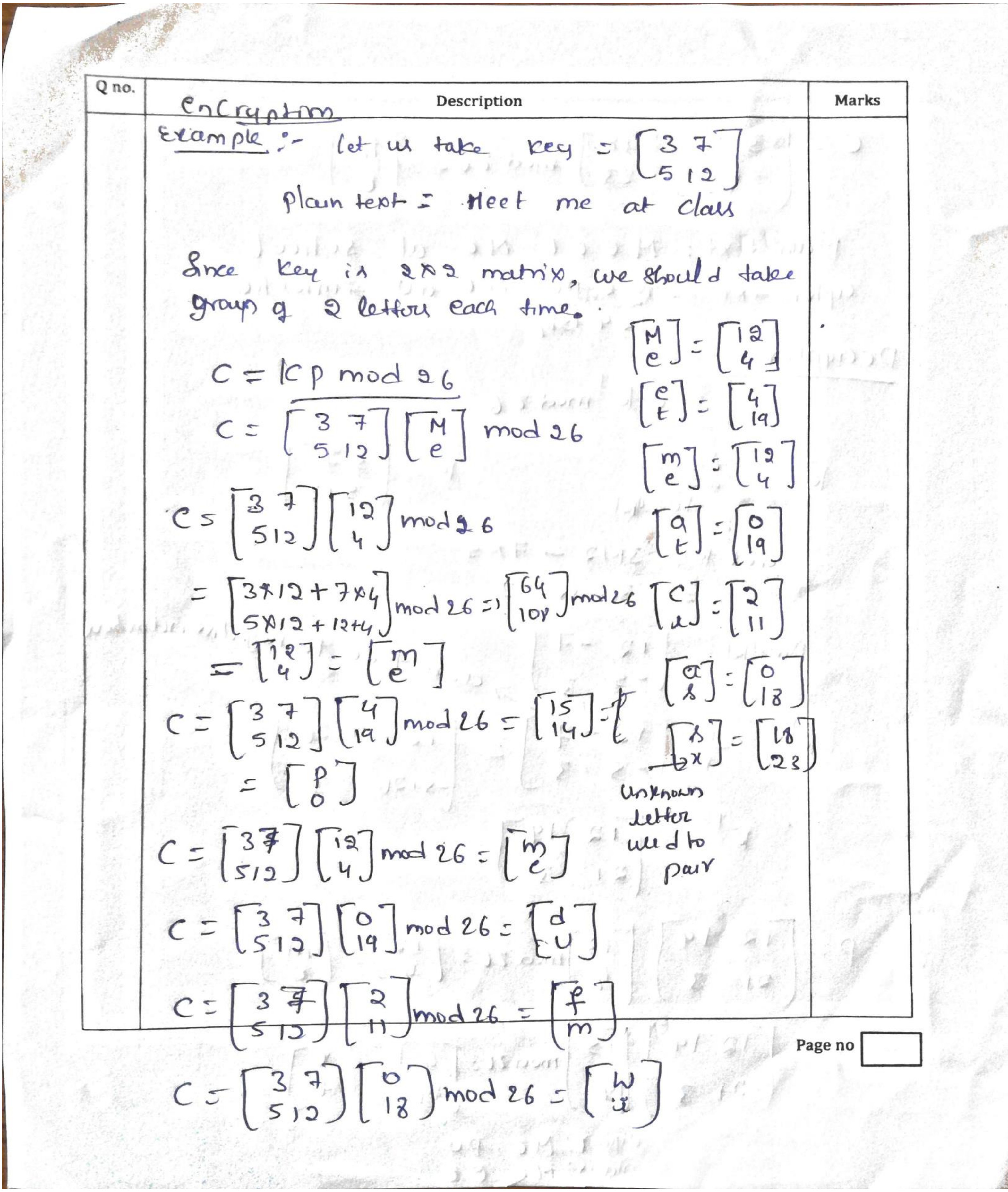
This can be expressed in term of column vectors and matrices:

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

Or

C = KP mod 26

Where C and P are column vectors of length 3, representing the plaintext and cipher text, and K is a 3 x 3 matrix, representing the encryption key. Operations are performed mod 26.



Q no.	Description	Marks

encryption

Example :- let us take key $= \begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}$

plain text = Meet me at class

Since key is 2×2 matrix, we should take group of 2 letters each time.

$\begin{bmatrix} M \\ e \end{bmatrix} = \begin{bmatrix} 12 \\ 4 \end{bmatrix}$

$\begin{bmatrix} e \\ t \end{bmatrix} = \begin{bmatrix} 4 \\ 19 \end{bmatrix}$

$\begin{bmatrix} m \\ e \end{bmatrix} = \begin{bmatrix} 12 \\ 4 \end{bmatrix}$

$\begin{bmatrix} a \\ t \end{bmatrix} = \begin{bmatrix} 0 \\ 19 \end{bmatrix}$

$\begin{bmatrix} c \\ l \end{bmatrix} = \begin{bmatrix} 2 \\ 11 \end{bmatrix}$

$\begin{bmatrix} a \\ s \end{bmatrix} = \begin{bmatrix} 0 \\ 18 \end{bmatrix}$

$\begin{bmatrix} s \\ x \end{bmatrix} = \begin{bmatrix} 18 \\ 23 \end{bmatrix}$

unknown letter used to pair

$$\underline{C = KP \bmod 26}$$

$$C = \begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix} \begin{bmatrix} M \\ e \end{bmatrix} \bmod 26$$

$$C = \begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix} \begin{bmatrix} 12 \\ 4 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 3\times12+7\times4 \\ 5\times12+12\times4 \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 64 \\ 108 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 12 \\ 4 \end{bmatrix} = \begin{bmatrix} m \\ e \end{bmatrix}$$

$$C = \begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix} \begin{bmatrix} 4 \\ 19 \end{bmatrix} \bmod 26 = \begin{bmatrix} 15 \\ 14 \end{bmatrix} = \Big[$$

$$= \begin{bmatrix} p \\ o \end{bmatrix}$$

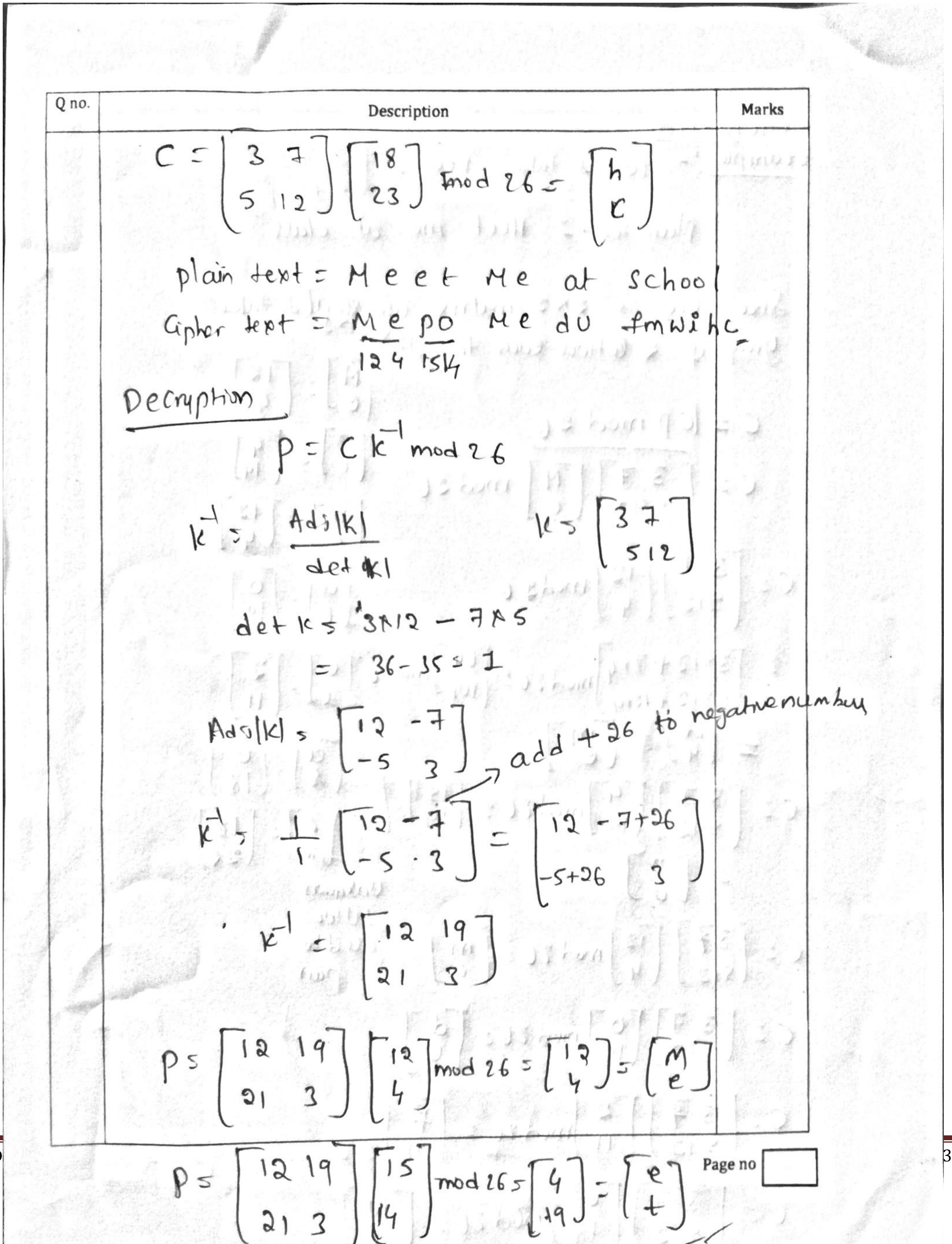
$$C = \begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix} \begin{bmatrix} 12 \\ 4 \end{bmatrix} \bmod 26 = \begin{bmatrix} m \\ e \end{bmatrix}$$

$$C = \begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \end{bmatrix} \bmod 26 = \begin{bmatrix} d \\ u \end{bmatrix}$$

$$C = \begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix} \begin{bmatrix} 2 \\ 11 \end{bmatrix} \bmod 26 = \begin{bmatrix} f \\ m \end{bmatrix}$$

Page no □

$$C = \begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix} \begin{bmatrix} 0 \\ 18 \end{bmatrix} \bmod 26 = \begin{bmatrix} w \\ i \end{bmatrix}$$



Q no.	Description	Marks
	$C = \begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix} \begin{bmatrix} 18 \\ 23 \end{bmatrix} \bmod 26 = \begin{bmatrix} h \\ c \end{bmatrix}$ plain text = Meet Me at school Cipher text = $\underset{12\ 4}{\underline{Me}}\ \underset{15\ 14}{\underline{po}}$ Me du fmwihc **Decryption** $P = C K^{-1} \bmod 26$ $K^{-1} = \frac{Adj\lvert K\rvert}{det\lvert K\rvert}$ $\quad K = \begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}$ $det\,K = 3\times12 - 7\times5$ $= 36 - 35 = 1$ $Adj\lvert K\rvert = \begin{bmatrix} 12 & -7 \\ -5 & 3 \end{bmatrix}$ → add +26 to negative number $K^{-1} = \frac{1}{1}\begin{bmatrix} 12 & -7 \\ -5 & 3 \end{bmatrix} = \begin{bmatrix} 12 & -7+26 \\ -5+26 & 3 \end{bmatrix}$ $K^{-1} = \begin{bmatrix} 12 & 19 \\ 21 & 3 \end{bmatrix}$ $P = \begin{bmatrix} 12 & 19 \\ 21 & 3 \end{bmatrix}\begin{bmatrix} 12 \\ 4 \end{bmatrix} \bmod 26 = \begin{bmatrix} 12 \\ 4 \end{bmatrix} = \begin{bmatrix} m \\ e \end{bmatrix}$	

$P = \begin{bmatrix} 12 & 19 \\ 21 & 3 \end{bmatrix}\begin{bmatrix} 15 \\ 14 \end{bmatrix} \bmod 26 = \begin{bmatrix} 4 \\ 19 \end{bmatrix} = \begin{bmatrix} e \\ t \end{bmatrix}$

Page no

Q no.	Description	Marks
2)		

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}_{3\times 3}$$

plain text = beautifully

Since 3×3 key take pair of 3 letters

encryption

$$C = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} b \\ e \\ a \end{bmatrix} \bmod 26$$

$$C = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 1 \\ 4 \\ 0 \end{bmatrix} \bmod 26 = \begin{bmatrix} 7 \\ 15 \\ 10 \end{bmatrix} = \begin{bmatrix} H \\ P \\ K \end{bmatrix}$$

$$C = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 20 \\ 19 \\ 8 \end{bmatrix} \bmod 26 = \begin{bmatrix} 1 \\ 20 \\ 22 \end{bmatrix} = \begin{bmatrix} B \\ U \\ W \end{bmatrix}$$

$$C = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 8 \\ 5 \\ 20 \end{bmatrix} \bmod 26 = \begin{bmatrix} 9 \\ 2 \\ 16 \end{bmatrix} = \begin{bmatrix} J \\ C \\ Q \end{bmatrix}$$

$$C = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 11 \\ 11 \\ 24 \end{bmatrix} \bmod 26 = \begin{bmatrix} 0 \\ 23 \\ 6 \end{bmatrix} = \begin{bmatrix} A \\ X \\ G \end{bmatrix}$$

plain text : B E A U T I F U L L Y

Page no

cipher text = H P K B U W C Q A X G

Q no. Description Marks

Decryption :- Cipher text = H D K B U [illegible] J C Q A X G

$P = C K^{-1} \bmod 26$

$K^{-1} = \frac{\text{AdJ } K}{\det K}$; $K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$

$\det K = 17(300 - 17(357) + 5(6))$

$= -939$

$\text{adJ}(K) = \begin{bmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{bmatrix}$

when you get K^{-1} matrix in fraction value then use below procedure

$\det \times x - 1 = 0 \bmod 26$

$-939 \times 17 - 1 = \frac{-15964}{26} = \text{Rem} = 0$

So $\underrightarrow{x = 17}$ (find out x value by trial & error so that when you do mod 26 you should get remainder is zero).

Now multiply x with adJ K

$\begin{bmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{bmatrix} \times 17$

Page no

Q no.	Description	Marks

$$= \begin{bmatrix} 5100 & -5321 & 4539 \\ -6069 & 5321 & -4284 \\ 102 & 0 & -867 \end{bmatrix} \bmod 26$$

add +26 to negative values

$$= \begin{bmatrix} 4 & -17_{+26} & 15 \\ -11_{+26} & 17 & -20_{+26} \\ 24 & 0 & -9_{+26} \end{bmatrix}$$

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

$$P = K^{-1} C \bmod 26$$

1st three letter of cipher text

$$P = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \begin{bmatrix} 7 \\ 15 \\ 10 \end{bmatrix} \bmod 26 = \begin{bmatrix} 1 \\ 4 \\ 0 \end{bmatrix} = \begin{bmatrix} B \\ E \\ A \end{bmatrix}$$

Similarly

$$P = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \begin{bmatrix} 1 \\ 20 \\ 22 \end{bmatrix} \bmod 26 = \begin{bmatrix} 20 \\ 19 \\ 8 \end{bmatrix} = \begin{bmatrix} U \\ T \\ I \end{bmatrix}$$

Page no

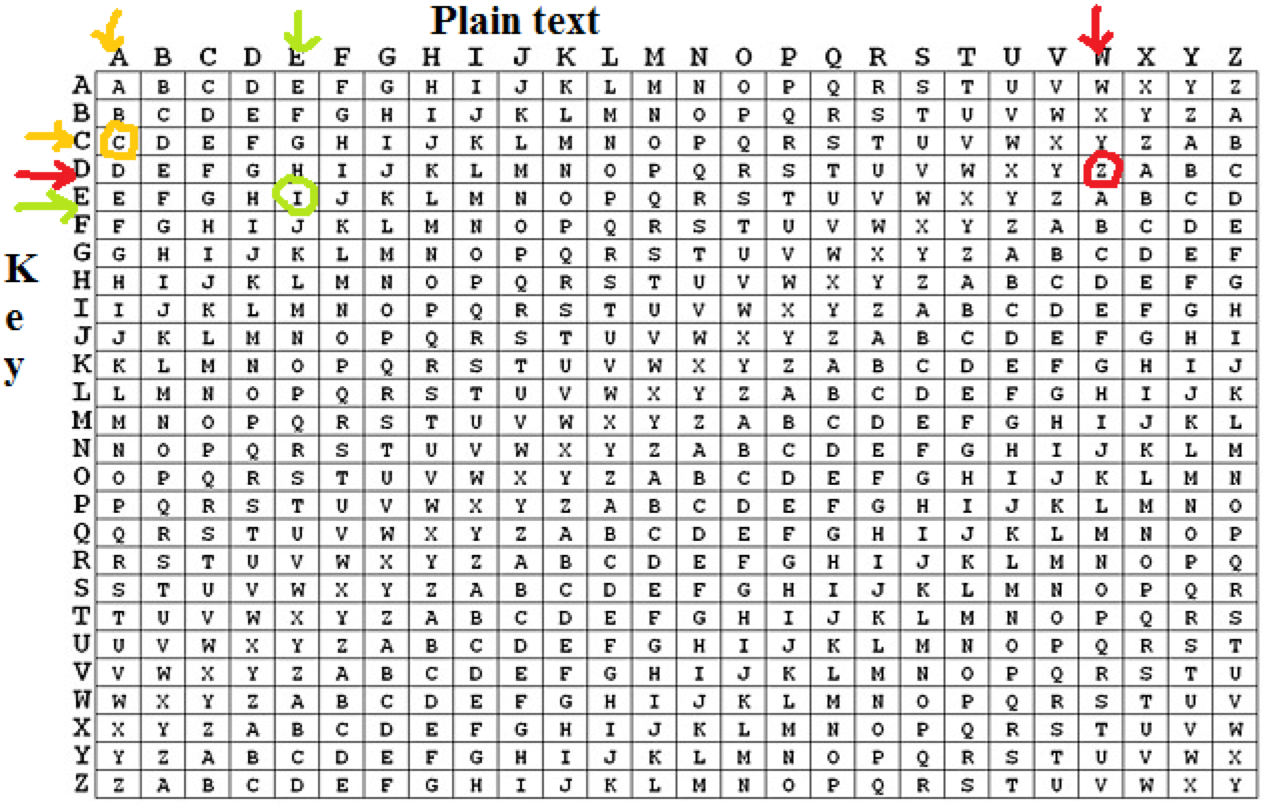
Polyalphabetic ciphers

Another way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message. The general name for this approach is polyalphabetic cipher. All the techniques have the following features in common.

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

Vigenere cipher

In this scheme, the set of related monoalphabetic substitution rules consisting of 26 caesar ciphers with shifts of 0 through 25. Each cipher is denoted by a key letter. e.g., Caesar cipher with a shift of 3 is denoted by the key value 'd‟‟ (since a=0, b=1, c=2 and so on). To aid in understanding the scheme, a matrix known as vigenere tableau is Constructed Each of the 26 ciphers is laid out horizontally, with the key letter for each cipher to its left. A normal alphabet for the plaintext runs across the top.



Plain text

Key

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

The process of Encryption is simple: Given a key letter X and a plaintext letter y, the cipher text is at the intersection of the row labeled x and the column labeled y; in this case, the ciphertext is V.

To encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeating keyword.

e.g., key = D E C E P T I V E D E C E P T I V E D E C E P T I V E

Plain Text= W E A R E D I S C O V E R E D S A V E Y O U R S E L F

Cipher Text = Z I C V T W Q N G R Z G V T W A V Z H C Q Y G L M G J

Decryption is equally simple. The key letter again identifies the row. The position of the cipher text letter in that row determines the column, and the plaintext letter is at the top of that column.

Strength of Vigenere cipher

- There are multiple cipher text letters for each plaintext letter.
- Letter frequency information is obscured.

One Time Pad Cipher

It is an unbreakable cryptosystem. It represents the message as a sequence of 0s and 1s. This can be accomplished by writing all numbers in binary, for example, or by using ASCII. The key is a random sequence of 0‟s and 1‟s of same length as the message. Once a key is used, it is discarded and never used again.

11 8

EXAMPLE: PLAIN TEXT: L I F E I S W H A T Y O U M A K E I T

KEY: O P G Q E R T Y U I A S D F G H J K L (different key)

14 15

CIPHER TEXT: Z X L U M J P F U B Y G X R G R N S E

25 23

PLAIN TEXT: LIFE IS BEAUTIFUL

KEY: ZXCV BN M Q W D F T Y H R (different key)

CIPHER TEXT: KFHZ JF NUWXYCDBC

Advantage:

Encryption method is completely unbreakable for a ciphertext only attack.

Disadvantages

It requires a very long key which is expensive to produce and expensive to transmit.

Once a key is used, it is dangerous to reuse it for a second message; any knowledge on the first message would give knowledge of the second.

TRANSPOSITION TECHNIQUES

All the techniques examined so far involve the substitution of a cipher text symbol for a plaintext symbol. A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.

Rail fence

It is a simplest of such cipher, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

Plaintext= meet me after the toga party

To encipher this message with a rail fence of depth 2, we write the message as follows:

m e m a t r h g p r y

e t e f e t e o a a t

The encrypted message is MEMATRHTGPRYETEFETEOAAT

COLUMNAR Transposition Ciphers-

A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns. The order of columns then becomes the key of the algorithm. Key: 4312567 Plaintext: attack postponed until two am

Cipher text:
ttnaaptmtsuoaodwcoixknlypetz

4	3	1	2	5	6	7
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

Pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext. The transposition cipher can be made significantly more secure by performing more than one stage of transposition. The result is more complex permutation that is not easily reconstructed.