GLS UNIVERSITY

Promoted By Gujarat Law Society Since 1927

Accredited with A+ NAAC GRADE CGPA : 3.44

Faculty of Computer Applications &
Information Technology

BCA Programme

210301502

INFORMATION SECURITY

Unit -3 Network Security - Cryptography

- **Introduction**
- **Plain Text and Cipher Text**
- **Substitution Techniques**
  - Ceaser Cipher
  - Polygram Cipher
  - Playfair Cipher
- **Transposition Techniques**
  - Rail-Fence Technique
  - Columnar Technique
  - Vernam Cipher

Unit -3 Network Security - Cryptography

- **Introduction**
  - The Internet is growing faster than telecommunication system in history.
  - Corporate’s internal networks now attached with the Internet.
  - So that internet attached corporate are attractive targets for intruders who use the internet to attack systems and create computer security incidents.
  - New internet sites are often prime targets for :
    - **Malicious activity**
    - **File tampering**
    - **Vandalism**
    - **Service disruptions**

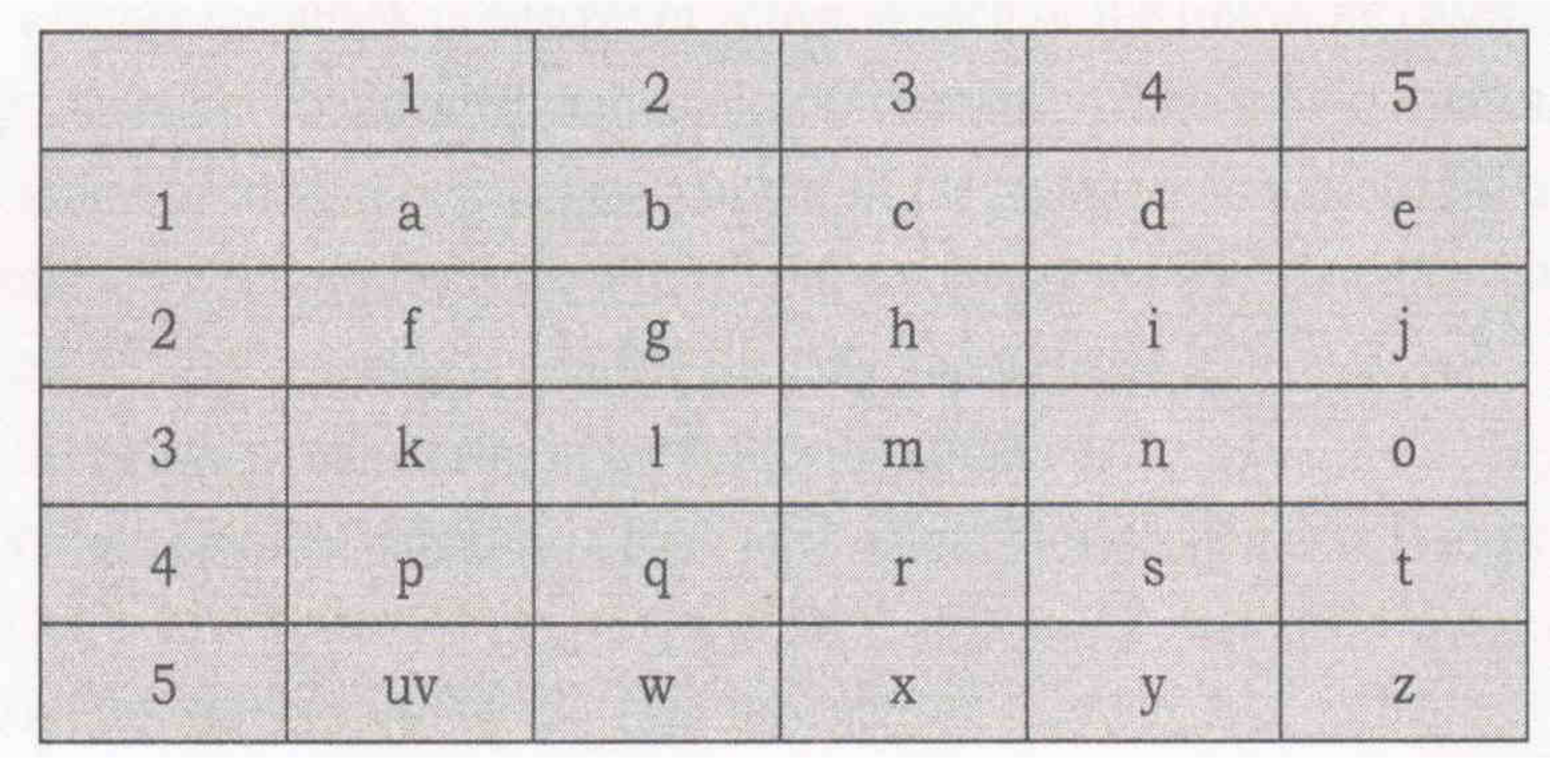
Unit -3 Network Security - Cryptography

- **Introduction**
  - Due to this activities organization victim of lost productivity and damage to data, company reputation and customer goodwill.
  - IS practitioners must be aware of the risk of computer security incidents from the Internet and steps they can take to secure public and private sites.
  - Here we discusses technical concerns related to network security.

Unit -3 Network Security - Cryptography

- **Introduction – a Case to start with**
  - In the 1850s and 1860s, a movement in Russia gained momentum.
  - Known as Nihilist people, this group of revolutionaries developed a pen-and-paper-based cryptographic scheme.
  - To communicate among themselves, they numerically enciphered plain text and added a keyword, which repeated through the length of the communication.
  - **Message - “*strike czar now*”**
  - **Keyword for encryption is “*unite*”**

Unit -3 Network Security - Cryptography



	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	j
3	k	l	m	n	o
4	p	q	r	s	t
5	uv	w	x	y	z

Unit -3 Network Security - Cryptography

- **Introduction – a case to start with**
  - Message - “*strike czar now*”
  - To enciphering the keyword as well as the message,
    - Each letter is locate first vertically (row number) and
    - Than horizontally (column number)
    - i.e - ‘u’ -> 51
    - ie. - ‘n’ -> 34

Unit -3 Network Security - Cryptography

- **Introduction – a case to start with**
  - Message - “*strike czar now*” would be

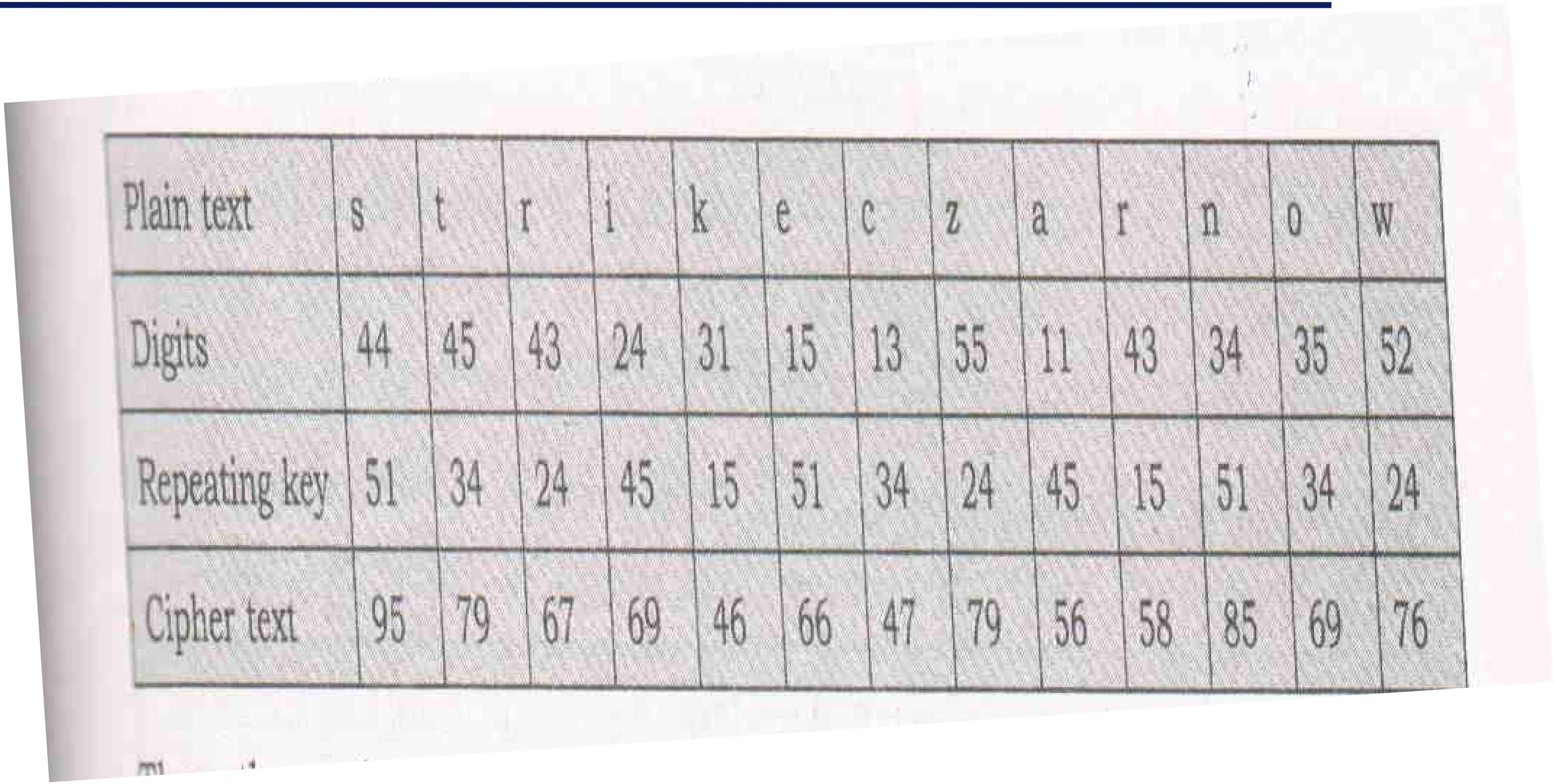
    44 45 43 24 31 15 13 55 11 43 34 35 52

  - Keyword for encryption is “*unite*” would be

    51 34 24 45 15

  - Now in the last step, the repeating keyword key numbers are added to the enciphered message numbers:

Unit -3 Network Security - Cryptography



Plain text	s	t	r	i	k	e	c	z	a	r	n	o	w
Digits	44	45	43	24	31	15	13	55	11	43	34	35	52
Repeating key	51	34	24	45	15	51	34	24	45	15	51	34	24
Cipher text	95	79	67	69	46	66	47	79	56	58	85	69	76

- **Introduction – a case to start with**
  - Message - “*strike czar now*” would be

    44 45 43 24 31 15 13 55 11 43 34 35 52

  - Keyword for encryption is “*unite*” would be

    51 34 24 45 15

  - Now in the last step, the repeating keyword key numbers are added to the enciphered message numbers:
  - **Sender would send the message**

    95 79 67 69 46 66 47 79 56 58 85 69 76

Unit -3 Network Security - Cryptography

- **Basic Terms**
  - **Cryptography**
    - *Cryptography is the art of achieving security by encoding messages to make them non-readable.*

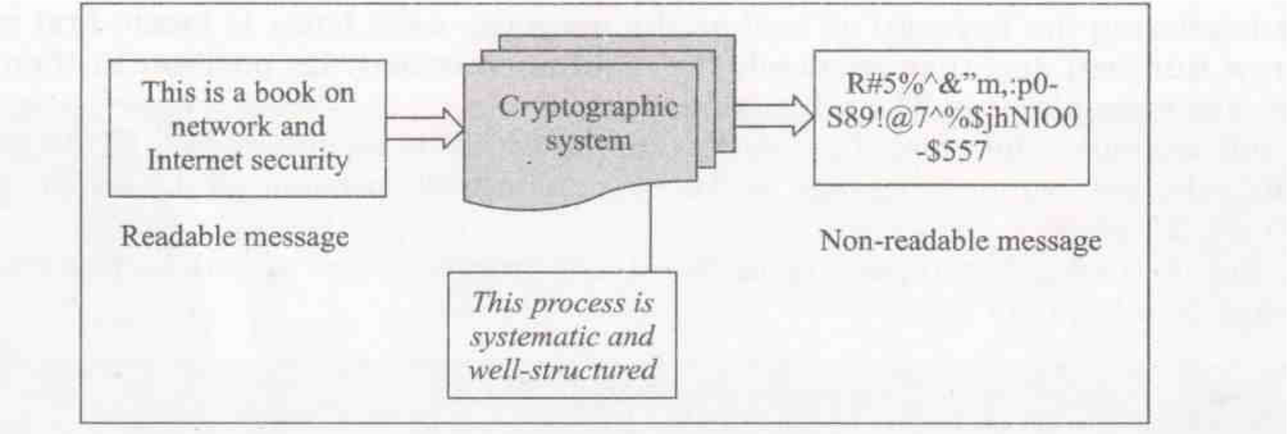
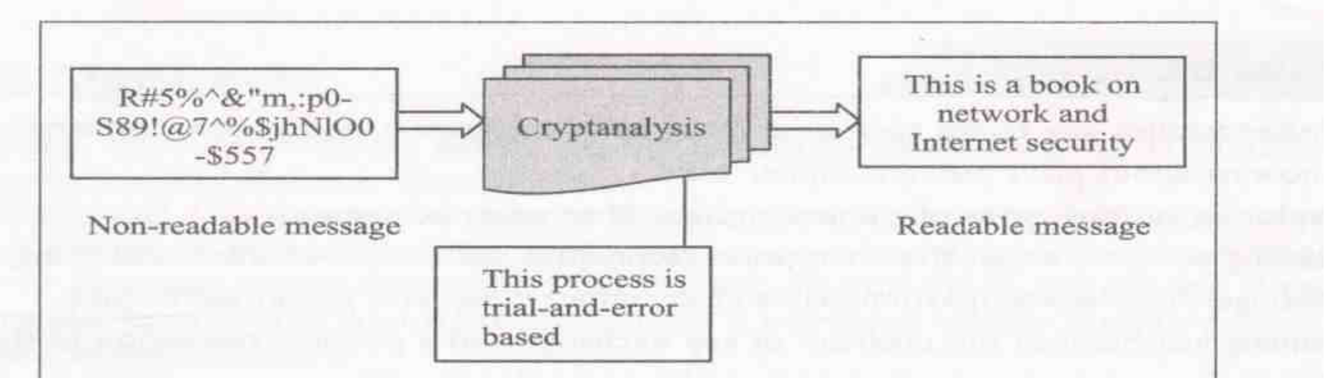

This is a book on network and Internet security
Readable message
Cryptographic system
This process is systematic and well-structured
R#5%^&”m,:p0- S89!@7^%$jhNIO0 -$557
Non-readable message

Fig. 2.1 Cryptographic system

Unit -3 Network Security - Cryptography

- **Basic Terms**
  - **Crytanalysis**
    - Cryptanalysis is the technique of decoding message from a non-readable format back to readable format without knowing how they were initially converted from readable format to non-readable format.



Unit -3 Network Security - Cryptography

- **Basic Terms**
  - **Cryptology**
    - *Cryptology is a combination of cryptography and cryptanalysis.*

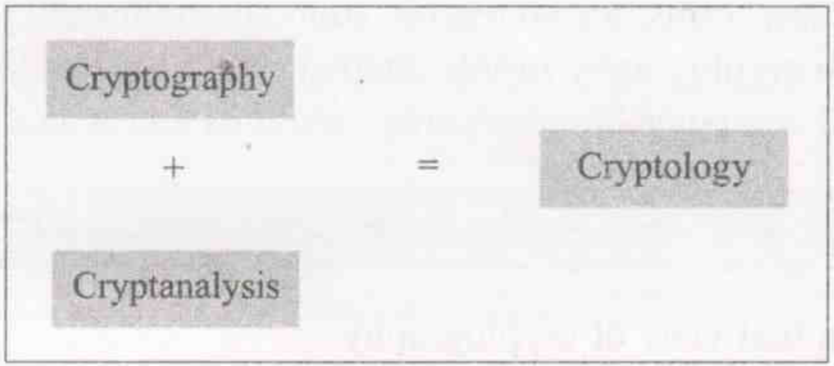


Fig. 2.3 Cryptography + Cryptanalysis = Cryptology

Unit -3 Network Security - Cryptography

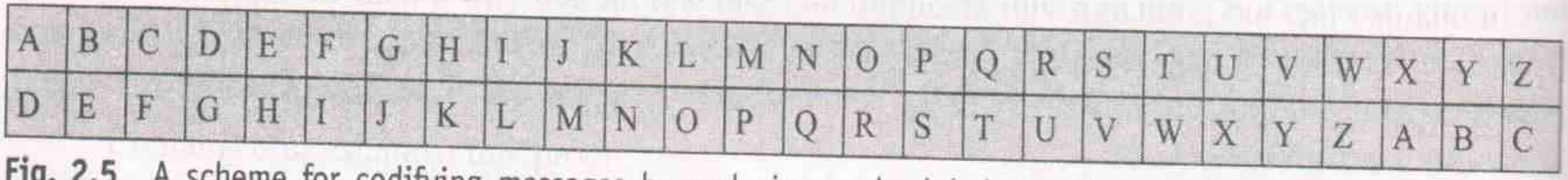
- **Plain Text**
  - Any communication in the language that you and I speak – that is the human language, takes the form of Plain Text or Clear Text.
  - Plain Text can be understand by anybody knowing the language as long as the message is not codified in any manner.
  - Clear Text or Plain Text signifies a message that can be understood by the sender, the recipient and also by anyone else who gets an access to that message.

Unit -3 Network Security - Cryptography

- **Plain Text**
  - In **some situation** where we are **concerned about the secrecy** of our conversations.
  - So we do not want any one else (other then receiver) to understand, even if third person get the text.
  - i.e – Each alphabet in their conversation with another character.
    - *A* -> *D*
    - *B* -> *E*
    - *C* -> *F*

Unit -3 Network Security - Cryptography

- **Plain Text and Cipher Text**



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
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

Fig. 2.5 A scheme for codifying messages by replacing each alphabet with an alphabet three places down the line

G	L	S		U	N	I	V	E	R	S	I	T	Y
J	O	V		X	Q	L	Y	H	U	V	L	W	B

Unit -3 Network Security - Cryptography

- **Cipher Text**
  - There can be many variants of such a scheme.
  - It is **not necessary to replace each alphabet with the one that is three places down the order.**
  - Here each alphabet in the original message can be replaced by another to hide the original contents of the message. **The codified message is called as cipher text**
  - **Cipher means a code or a secret message.**
  - **When a Plain Text message is codified using any suitable scheme, the resulting message is called as Cipher Text.**

Unit -3 Network Security - Cryptography

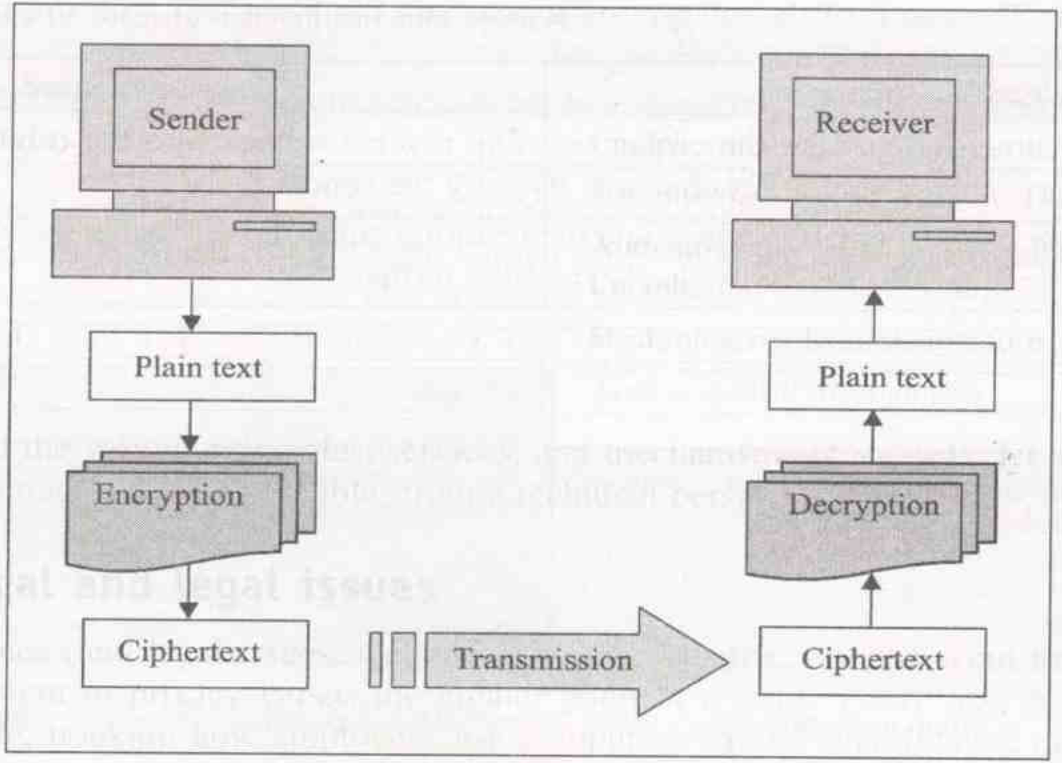
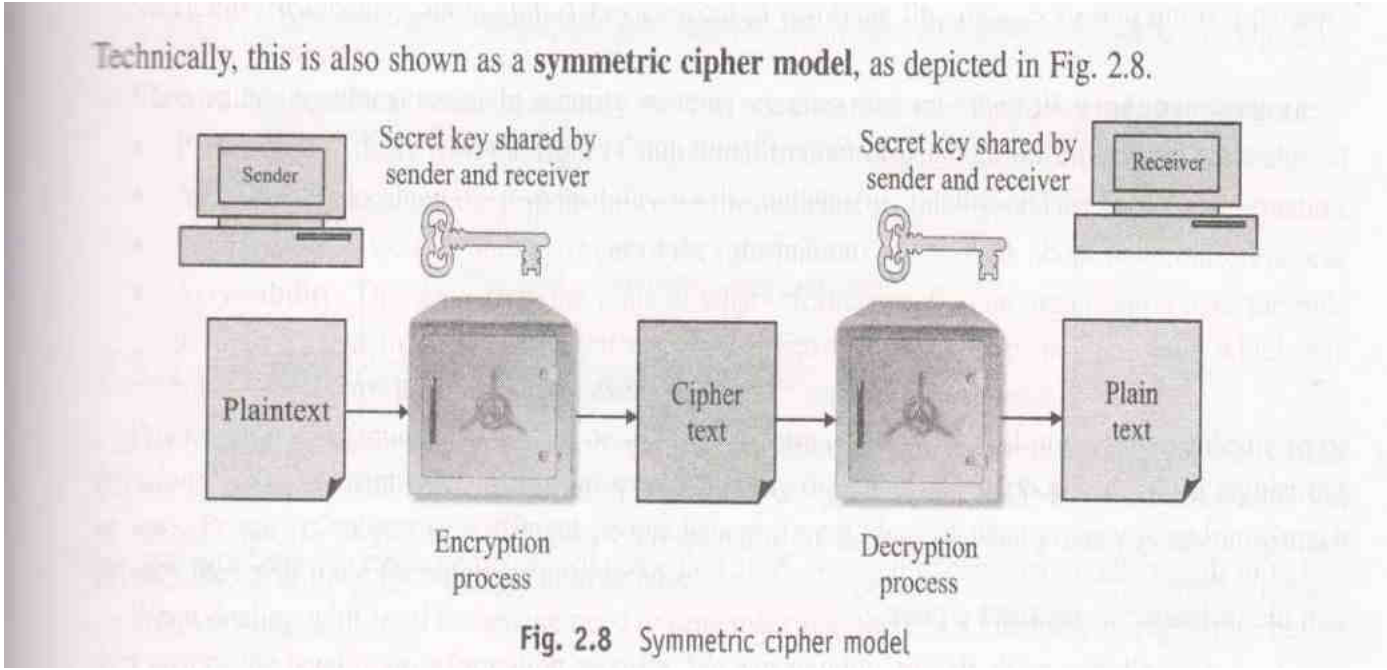


Fig. 2.7 Elements of a cryptographic operation

Unit -3 Network Security - Cryptography

- **Symmetric Cipher Model**



Technically, this is also shown as a **symmetric cipher model**, as depicted in Fig. 2.8.

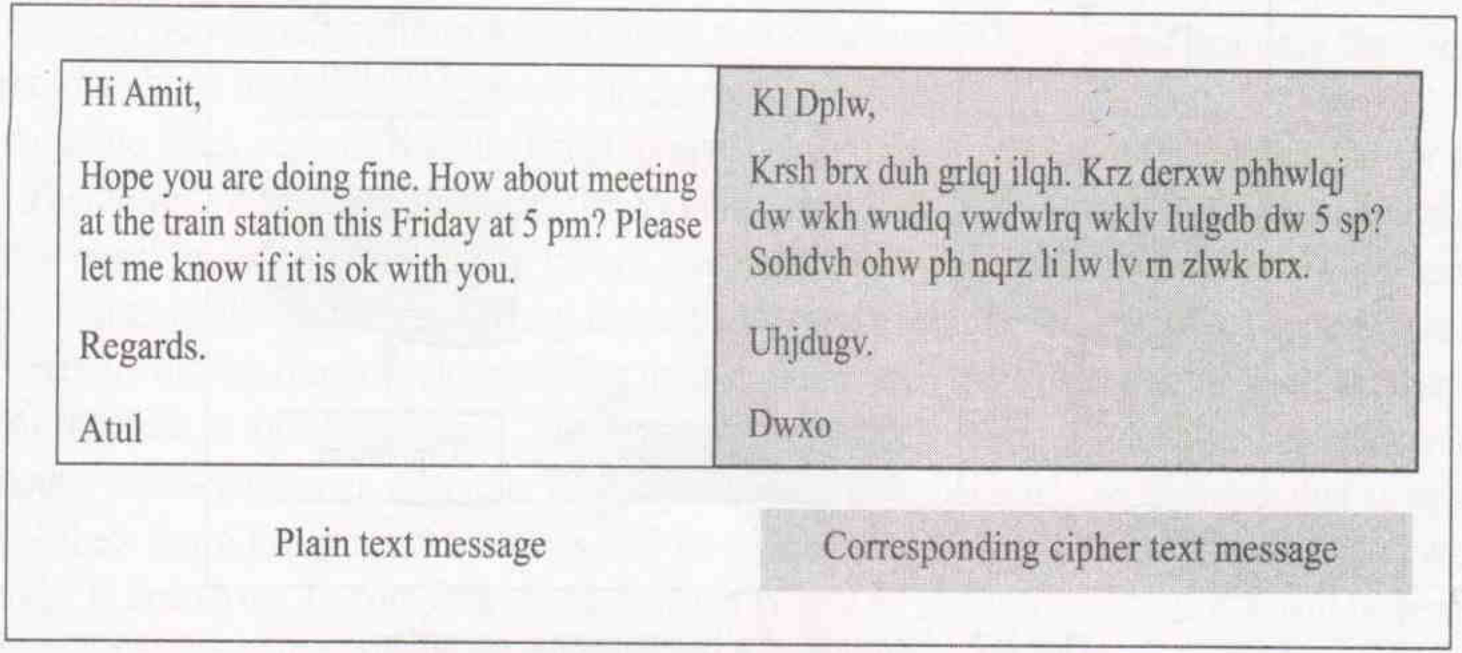
Sender
Secret key shared by sender and receiver
Secret key shared by sender and receiver
Receiver
Plaintext
Cipher text
Plain text
Encryption process
Decryption process

Fig. 2.8 Symmetric cipher model

Unit -3 Network Security - Cryptography

- **Symmetric Cipher Model**
  - **Plain Text : This is the original text**, which is readable and supposed to be protected from the attackers.
  - **Encryption Process:** Also **called as encryption algorithm,** this process performs various operations on the plain text to make it look like illegible text.
  - **Secret Key:** This is a **certain secret value shared by the sender and receiver**. It is not dependent on the plain text or the encryption/decryption process. The secret key must be somehow available both to the sender and the receiver
  - **Cipher Text:** The result of the **encryption process on the plain text** with the help of the secret key produces cipher text.
  - **Decryption Process:** This is the **opposite of the encryption process**. The receiver has to take the cipher text and reverse it back into the original plain text by using the same shared secret key that was used by the sender.

Unit -3 Network Security - Cryptography



Hi Amit,

Hope you are doing fine. How about meeting at the train station this Friday at 5 pm? Please let me know if it is ok with you.

Regards.

Atul

Plain text message

Kl Dplw,

Krsh brx duh grlqj ilqh. Krz derxw phhwlqj dw wkh wudlq vwdwlrq wklv Iulgdb dw 5 sp? Sohdvh ohw ph nqrz li lw lv rn zlwk brx.

Uhjdugv.

Dwxo

Corresponding cipher text message

Fig. 2.9 Example of a plain text message being transformed into cipher text

Unit -3 Network Security - Cryptography

- There are two primary ways in which a plain text message can be codified to obtain the corresponding cipher text:
  - **Substitution**
  - **Transposition**

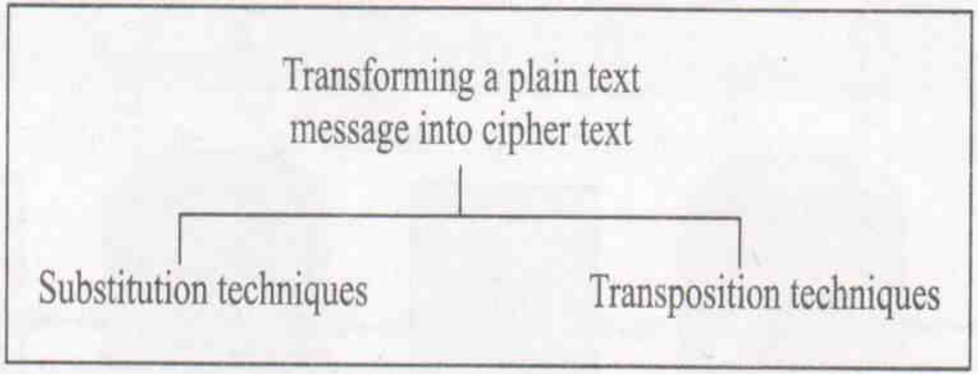


Fig. 2.10 Techniques for transforming plain text to cipher text

Unit -3 Network Security - Cryptography

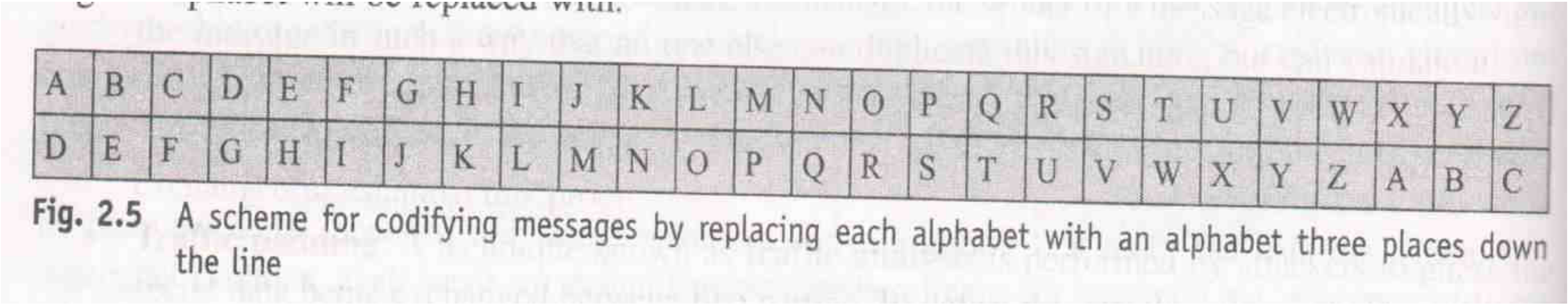
- **Substitution Techniques**
  - **Caesar Cipher**
  - Modified version of Caesar Cipher
  - Mono-Alphabetic Cipher
  - Homophonic Substitution Cipher
  - **Polygram Substitution Cipher**
  - Polyalphabetic Substitution Cipher
  - **Playfair Cipher**
  - Hill Cipher

Unit -3 Network Security - Cryptography

- **Caesar Cipher**
  - The scheme explained earlier (of replacing an alphabet with the one three places down the order) was first proposed by **Julius Caesar and termed as Caesar Cipher.**
  - **It was the first example of substitution cipher.**
  - In the substitution cipher technique, **the characters of a plain text message are replaced by other character, number or symbols.**
  - The Caesar Cipher is **a very weak scheme** of hiding plain text message.
  - All that is required **to break the Caesar Cipher is to do the reverse** of the Caesar Cipher process.

Unit -3 Network Security - Cryptography

- **Caesar Cipher**



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
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

Fig. 2.5 A scheme for codifying messages by replacing each alphabet with an alphabet three places down the line

G	L	S		U	N	I	V	E	R	S	I	T	Y
J	O	V		X	Q	L	Y	H	U	V	L	W	Z

Unit -3 Network Security - Cryptography

- **Caesar Cipher – Revese Algorithm (to break Caesar Cipher)**

1. **Read each alphabet** in the **cipher text** message and search for it in the second row of the replacement table.

2. When a match is found, replace that a**lphabet in the cipher text message with the corresponding alphabet in the same column** but the first row of the table.

3. Repeat the process for all alphabets in the cipher text message.

Unit -3 Network Security - Cryptography

- **Polygram Substitution Cipher**
  - In this cipher technique, rather than replacing one plain text alphabet with one cipher text alphabet at a time, a block of alphabets is replaced with another block.
  - i.e - “HELLO” ----> “YUQQW”
  - i.e - “HELL” ----> “TEUI”

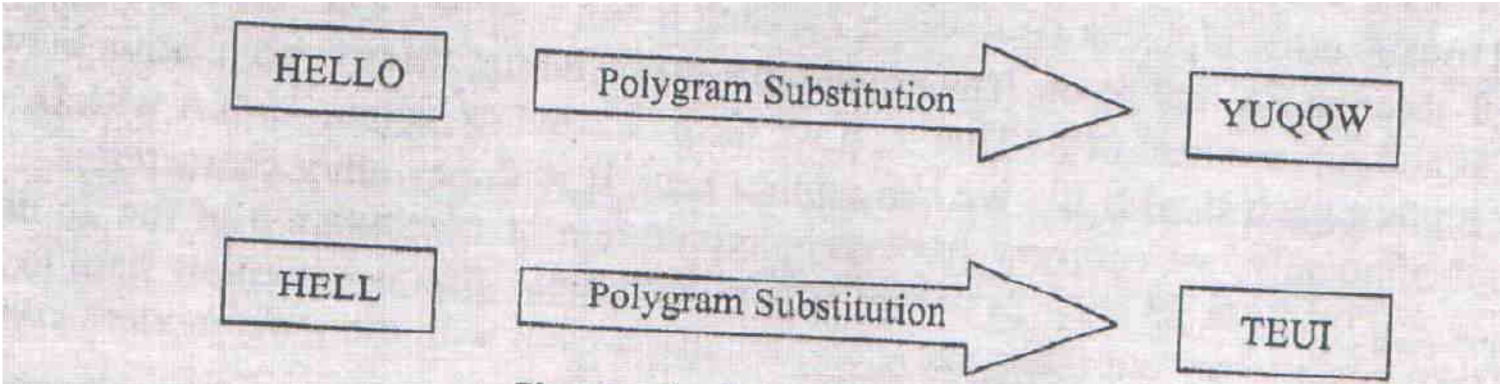


Fig. 2.15 Polygram Substitution

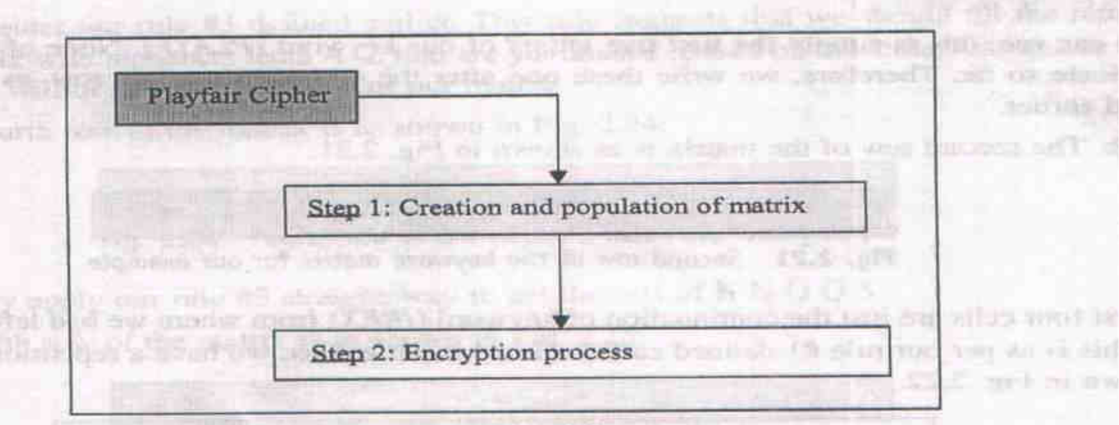
- **Polygram Substitution Cipher**
  - Polygram Substitution Cipher technique replaces one block of plain text with a block of cipher text – it does not work on a character- by – character basis.

Unit -3 Network Security - Cryptography

- **Playfair Cipher**
  - The Playfair Cipher, also called as Playfair Square, is a cryptographic technique that is used for manual encryption of data.
  - This scheme was invented by Charles Wheatstone in 1854.
  - Eventually the scheme came to be known by the name of Lord Playfair, who was Wheatstone’s friend.
  - Playfair mad this scheme popular and hence his name was used.
  - The playfair cipher was used by the **British Army in World War – I and by the Australians in World War – II**
  - Playfair **is fast to use** and does not demand any special equipment to be used.
  - It was used to **protect important but not very critical information.**

Unit -3 Network Security - Cryptography

- **Playfair Cipher**
  - The Playfair encryption **scheme uses two main processes**:



Playfair Cipher

Step 1: Creation and population of matrix

Step 2: Encryption process

Fig. 2.17 Playfair cipher steps

Unit -3 Network Security - Cryptography

- **Playfair Cipher**
- **Step -1 Creation and Population of Matrix**
  - The Playfair cipher makes use of a 5 * 5 matrix,
  - which is used to store a keywod or phrase that becomes the key for encryption and decryption.

Unit -3 Network Security - Cryptography

- **Playfair Cipher**
- **Step -1 Creation and Population of Matrix**
  - The way this is entered into the 5 * 5 matrix is based on some simple rules:

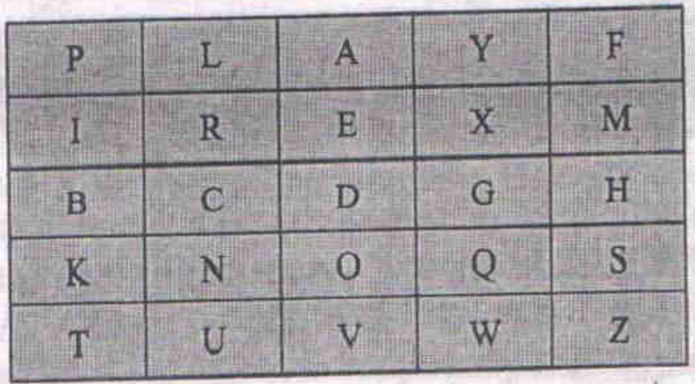
    1. Enter the **keyword in the matrix row-wise: left-to-right and then top-to-bottom.**
    2. **Drop duplicate letters.**
    3. **Fill the remaining spaces in the matrix with the rest of the English alphabets (A – Z) that were not a part of our keyword.**

       While doing so, **combine I and J in the same cell** of the table.

       If I or J is a part of the keyword, disregard both I and J while filling the remaining slots.

Unit -3 Network Security - Cryptography

- **Playfair Cipher**
- **Step -1 Creation and Population of Matrix**
  - i.e – keyword is - “PLAYFAIR EXAMPLE”



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

Fig. 2.19 Keyword matrix for our example

Unit -3 Network Security - Cryptography

- **Playfair Cipher**
- **Step -1 Creation and Population of Matrix**
  - i.e – keyword is - “PLAYFAIR EXAMPLE”
  - Generating 1st Row of 5 * 5 Matrix

P	**L**	**A**	**Y**	**F**

Unit -3 Network Security - Cryptography

- **Playfair Cipher**
- **Step -1 Creation and Population of Matrix**
  - i.e – keyword is - “PLAYFAIR EXAMPLE”
  - Generating 2nd Row of 5 * 5 Matrix

I	**R**	**E**	**X**	**M**

Unit -3 Network Security - Cryptography

- **Playfair Cipher**
- **Step -1 Creation and Population of Matrix**
  - i.e – keyword is - “PLAYFAIR EXAMPLE”
  - Generating 3rd Row of 5 * 5 Matrix

B	**C**	**D**	**G**	**H**

Unit -3 Network Security - Cryptography

- **Playfair Cipher**
- **Step -1 Creation and Population of Matrix**
  - i.e – keyword is - “PLAYFAIR EXAMPLE”
  - Generating 4th Row of 5 * 5 Matrix

K	**N**	**O**	**P**	**Q**

Unit -3 Network Security - Cryptography

- **Playfair Cipher**
- **Step -1 Creation and Population of Matrix**
  - i.e – keyword is - “PLAYFAIR EXAMPLE”
  - Generating 5th Row of 5 * 5 Matrix

T	**U**	**V**	**W**	**Z**

Unit -3 Network Security - Cryptography

- **Playfair Cipher**
- **Step -2 Encryption Process (**It consists of five steps**)**

STEP 1 : Before executing these steps, the plain text message that we want to encrypt needs to be broken down into groups of two alphabets.

Message - “MY NAME IS ATUL”

broken down – MY NA ME IS AT UL

Unit -3 Network Security - Cryptography

- **Playfair Cipher**
- **Step -2 Encryption Process (**It consists of five steps**)**

STEP 2 : If both alphabets are the same (or only one is left) , ad**d an X after the first alphabet.**

Encrypt the new pair and contiue.

- **Playfair Cipher**
- **Step -2 Encryption Process (**It consists of five steps**)**

STEP 3 : If both the alphabets in the pair **appear in the same row of our matrix, replace them with alphabets to their immediate right respectively.**

If the original pair is on the right side of the row, then wrapping around to the left side of the row happens.

Unit -3 Network Security - Cryptography

- **Playfair Cipher**
- **Step -2 Encryption Process (**It consists of five steps**)**

STEP 4 : If both the alphabets in the **pair appear in the same column of our matrix, replace them with alphabets immediately below them respectively.**

If the original pair is on the bottom side of the row, then wrapping around to the top side of the row happens.

Unit -3 Network Security - Cryptography

- **Playfair Cipher**
- **Step -2 Encryption Process (**It consists of five steps**)**

STEP 5 : If both alphabets **are not in the same row or column, replace** then with the **alphabets in the same row respectively, but at the other pair of corner of the rectangle defined by the original pair.**

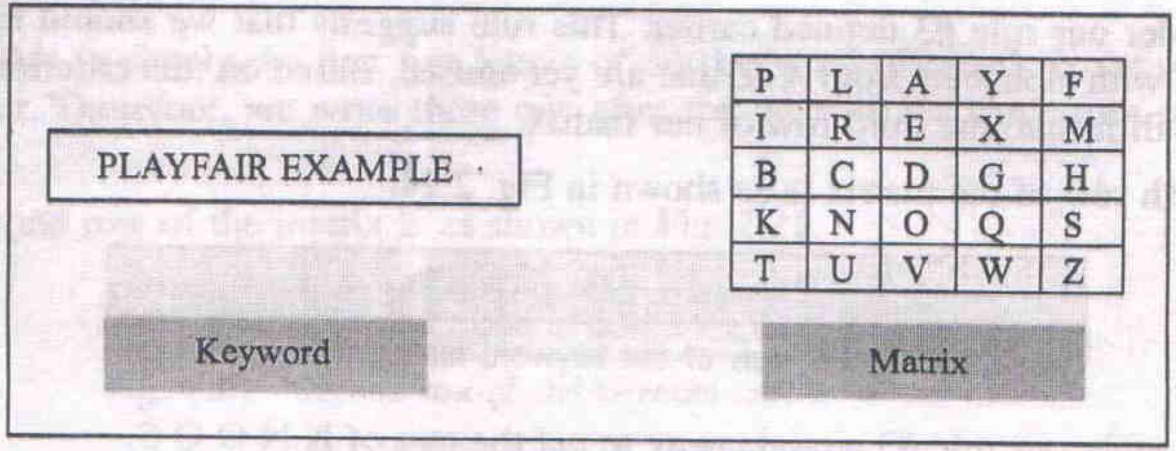
The order is quite significant here. The First encrypted alphabet of the pair is the one that is present on the same row as the first plaintext alphabet.

Unit -3 Network Security - Cryptography

- **Playfair Cipher**
- i.e – Message - “MY NAME IS ATUL”
    - Keyword - “PLAYFAIR EXAMPLE”

Unit -3 Network Security - Cryptography

- **Playfair Cipher**
  - Key Word need to convert in Matrix



PLAYFAIR EXAMPLE

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

Fig. 2.27 Keyword matrix for our example

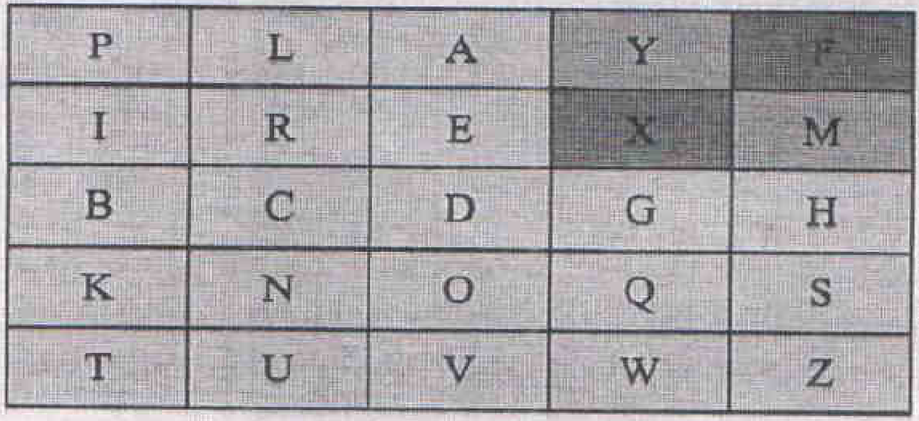
Unit -3 Network Security - Cryptography

- **Playfair Cipher**
  - **Step 1 : Encryption Process**
    - First break the original text into pairs of two alphabets each.
    - So original text would be :

      MY NA ME IS AT UL

Unit -3 Network Security - Cryptography

- **Playfair Cipher**
  - **Step 2 : Encryption Process**
  - **Apply step#5**
  - **MY -> XF**

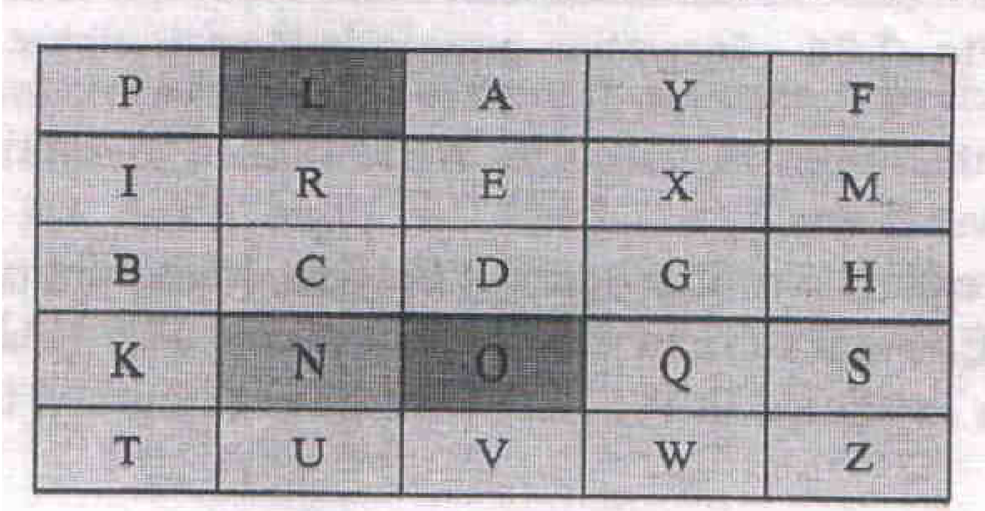


P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

Fig. 2.28 Alphabet pair 1

Unit -3 Network Security - Cryptography

- **Playfair Cipher**
  - **Step 3 : Encryption Process**
  - **Apply step#5**
  - **NA -> OL**

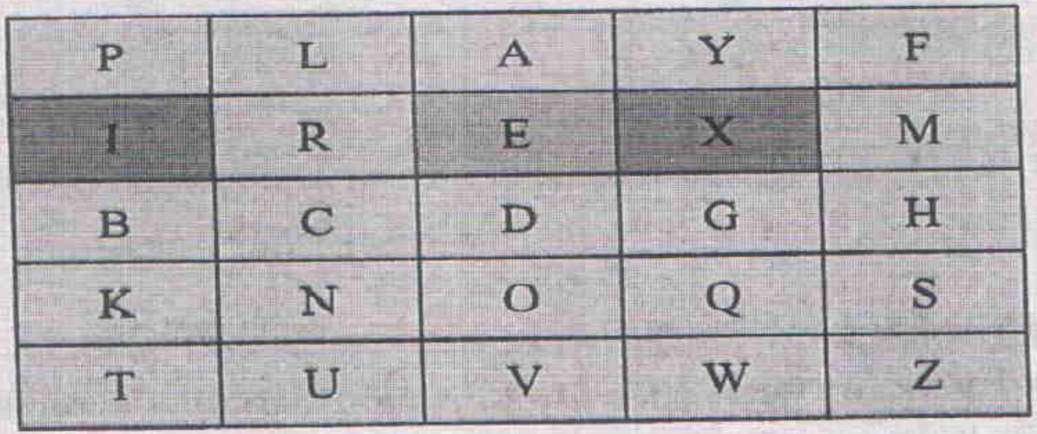


P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

Fig. 2.29 Alphabet pair 2

Unit -3 Network Security - Cryptography

- **Playfair Cipher**
  - **Step 4 : Encryption Process**
  - **Apply step#3**
  - **ME -> IX**

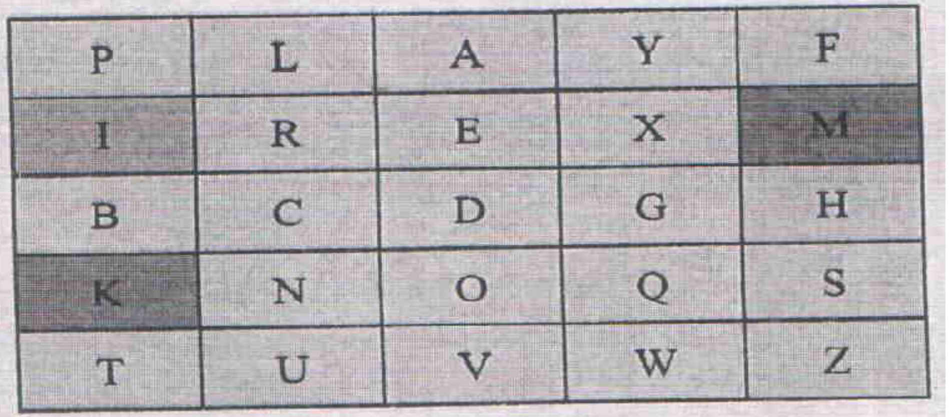


P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

Fig. 2.30 Alphabet pair 3

Unit -3 Network Security - Cryptography

- **Playfair Cipher**
  - **Step 5 : Encryption Process**
  - **Apply step#5**
  - **IS -> MK**

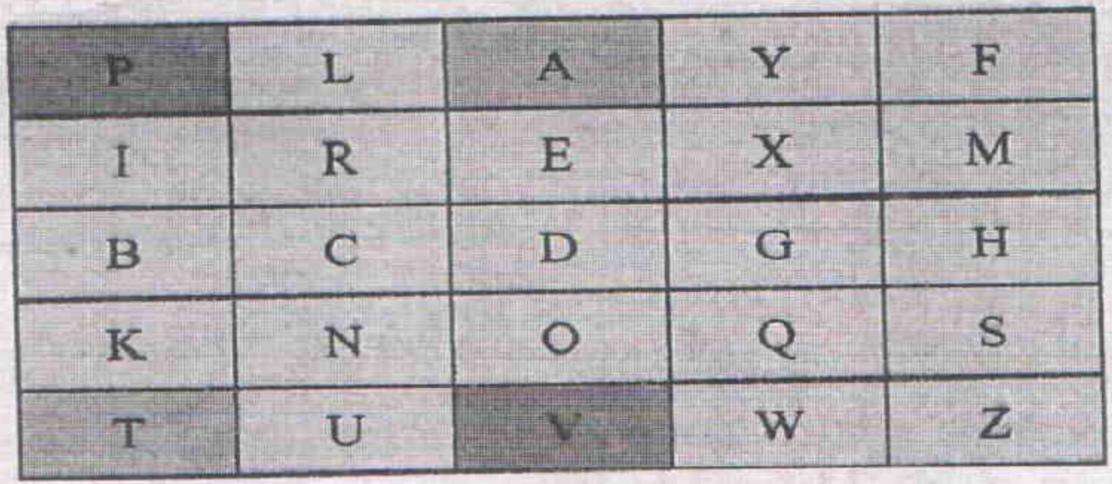


P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

Fig. 2.30 Alphabet pair 4

Unit -3 Network Security - Cryptography

- **Playfair Cipher**
  - **Step 6 : Encryption Process**
  - **Apply step#5**
  - **AT -> PV**

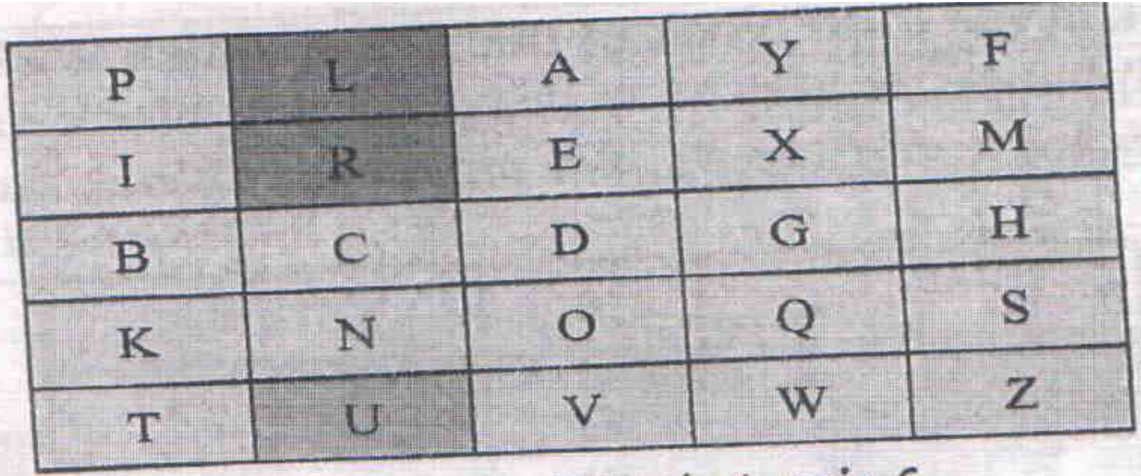


P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

Fig. 2.31 Alphabet pair 5

Unit -3 Network Security - Cryptography

- **Playfair Cipher**
  - **Step 7 : Encryption Process**
  - **Apply step#4**
  - **UL -> LR**



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

Fig. 2.32 Alphabet pair 6

Unit -3 Network Security - Cryptography

- **Playfair Cipher**
- i.e – Message - “MY NAME IS ATUL”
  - Keyword - “PLAYFAIR EXAMPLE”
  - Encrypted Message - “XF OL IX MK PV LR”