The Islamic University
College of Technical Engineering
Department of Computer Technical Engineering

Fourth Stage

Security

Lecture 6

Asst. Lec. Yousif Samer Mudhafar

Email: yousif.samir19@gmail.com

Lecture objectives

The student will recognize the following objectives

- **Transposition Techniques**
- **Encryption and Decryption using Play fair Cipher.**

Transposition Techniques

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

A transposition cipher does not substitute one symbol for another, instead it changes the location of the symbol, a symbol in the first position of the plaintext ma appear in the tenth position of the Ciphertext a symbol in the eighth position in the plaintext ay appear in the first position of the Ciphertext, in another words, a transposition cipher reorders (transposes) the symbols.

In **substitution** which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and **Transposition** in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost (that is, that all operations are reversible). Most systems, referred to as product systems, involve multiple stages of substitutions and transpositions.

There is technique that depend on Transposition is :

1. Play fair Cipher.

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 Ciphertext diagrams. The Play fair algorithm is based on the use of a $5 * 5$ Matrix of letters constructed using a keyword.

Here is an example :

keyword is monarchy

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

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

Play fair Cipher

In this case, the keyword is 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 alphabetic order.

The letters I and J count as one letter. 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.

Play fair Cipher

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 become BP and ea becomes IM (or JM, as the enciphered wishes).**

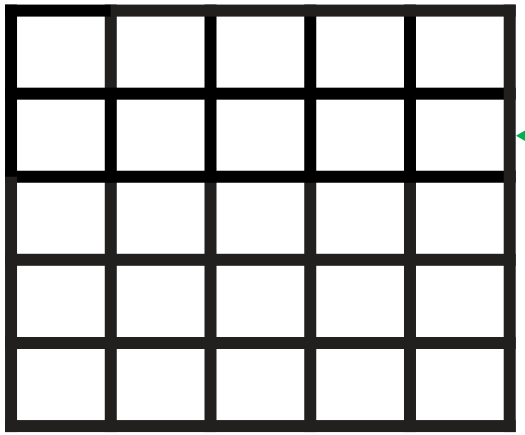
Play fair Cipher

Alice

Sender

Bob

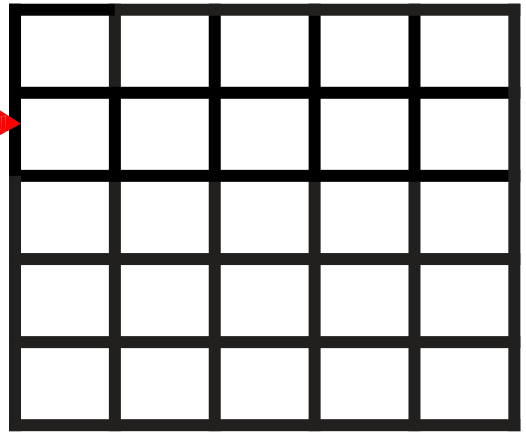
Receiver



Keyword
$5 * 5\ matrix$

Encryption

Keyword
$5 * 5\ matrix$



Decryption

Cipher text

Example

Encrypt and then decrypt the Plaintext “**hello bop**” by using **Play fair Cipher** with the **Keyword** “**teaching**”.

Ans:-

1. Encryption Algorithm

The Play fair algorithm is based on the use of a 5 * 5 Matrix of letters constructed using a keyword.

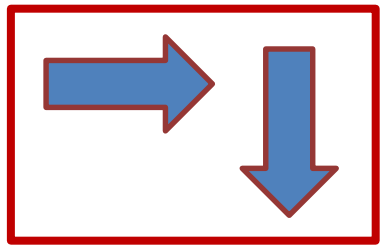
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

5 * 5 si drowyeK Matrix

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

Plaintext : hello bop → **Plaintext : helxlo bopx**

Plaintext → **he** **lx** **lo** **bo** **px**



P_1 P_2 P_3 P_4 P_5

$P_1 = he \rightarrow C_1 = TA$

$P_2 = lx \rightarrow C_2 = RA$

$P_3 = lo \rightarrow C_3 = MF$

$P_4 = bo \rightarrow C_4 = DM$

$P_5 = px \rightarrow C_5 = RV$

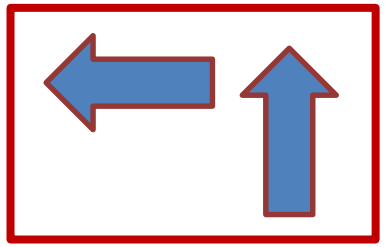
T	E	A	C	H
I/J	N	G	B	D
F	K	L	M	O
P	Q	R	S	U
V	W	X	Y	Z

The **Cipher text** is "**TARAMFDMRV**"

2. Decryption Algorithm

The **Cipher text** is "**TARAMFDMRV**"

Ciphertext → **TA** **RA** **MF** **DM** **RV**



C_1 C_2 C_3 C_4 C_5

$C_1 = TA \rightarrow P_1 = he$

$C_2 = RA \rightarrow P_2 = lx$

$C_3 = MF \rightarrow P_3 = lo$

$C_4 = DM \rightarrow P_4 = bo$

$C_5 = RV \rightarrow P_5 = px$

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

The **Plaintext** is "**helxlobopx**" → The **Plaintext** is "**hello bop**"

Keyword is 5 * 5 Matrix

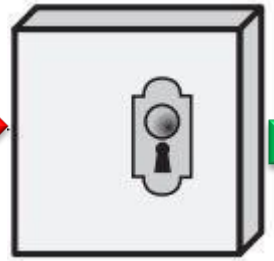
T	E	A	C	H
I/J	N	G	B	D
F	K	L	M	O
P	Q	R	S	U
V	W	X	Y	Z

Keyword is 5 * 5 Matrix

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

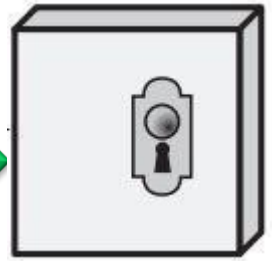
hello bop

(Sender)



Encryption algorithm
By using Play fair
Cipher

TARAMFDMRV



Decryption algorithm
By using Play fair
Cipher

hello bop

(receiver)

Homework

By using Play fair algorithm, encrypt this message "See you" with the Keyword is "tomorrow".