Student Manual/DR. Bashar Al-Esawi

Playfair:

تتلخص قاعدة التشفير في نظام شفرة بلايفير في الآتي:

- إذا وقع الحرفان في الصف نفسه من الجدول، يحل محل كل حرف الحرفُ الذي إلى يمينه.
- إذا وقع الحرفان في العمود نفسه الجدول، يحل محل كل حرف الحرفُ الذي يقع إلى الأسفل منه.
- إذا لم يقع الحرفان في الصف أو العمود نفسه، يحل محل الحرفِ الأول الحرفُ الذي يقع في صف الحرف الأول وعمود الحرف الثاني. ويحل محل الحرف الثاني الحرف الذي يوجد في عمود الحرف الأول وصف الحرف الثاني.

Use Playfair to encrypt "Cybersecurity" using keyword" congradulations"?

Playfair square

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

The Cipher text is : GVEFOFIGTNFAZY

Hill Cipher:

Let Alphabet is:

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	26	27	28

Text or Plain= **information security**

Key = **best hill cipher**

Find key length ==16==4X4

B	e	s	t
	h	i	l
L		c	i
P	h	e	r

Plain

8
13
5
14

Key

1	4	18	19
26	7	8	11
11	26	2	8
15	7	4	17

8*1+13*4+5*18+14*19=416 mod 29=10=**K**

8*26+13*7+5*8+14*11=493 mod 29=0=A

And so on>>>>

Therefore Cipher=?????

Bashar help:

https://www.geeksforgeeks.org/vigenere-cipher/?ref=lbp

Transposition Ciphers:

Rail fence

https://www.dcode.fr/rail-fence-cipher

The main idea depends on the following:

1. The KEY between sender and receiver is Depth.
2. The other is the PROTOCOL of operation this may be (Top-Down OR Bottom-Up).
3. All Plain or Cipher must be rearranged in ZigZag way depends on Depth (KEY).

EXAMPLE:

If the depth=3, decryptes the Plain="**Give me the Password**" using Rail Fence technique? By TD and BU.

ANSWER:

G				_				t				P				w				X
	i		e		m		_		h		_		a		s		o		d	
		v				e				e				s				r		

Therefore, to get Cipher Text read the matrix Row-By-Row:

Ciphertext= "G_tPwXiem_h_asodveesr"

If the direction BU the solution as follow:

		▨				▨				▨				▨				▨		
	▨		▨		▨		▨		▨		▨		▨		▨		▨		▨	
▨				▨				▨				▨				▨				▨

EXAMPLE2:

Q) Decryptes “ERBRUIYSCTCEY” using key=4 by ZigZag method from Bottom-Up?

ANSWER:

			E						**R**			
		B		R				U		I		
	Y				S		C				T	
C						E						Y

CYBERSECURITY

Matrix Transposition (Columnar Transposition):

- **In this method there is a KEY either to be numbers of Keyword,**
- **Build a Matrix with column = to number of char in KEY.**
- **In encryption, put the Plain row-by row.**
- **To find Cipher text, read characters by index of KEY.**
- **To find Plain, divide the total chars of cipher text by length of key= number of char for each column, then read row-by row to find the Plain text (Decryption).**

EXAMPLE:

https://www.boxentriq.com/code-breaking/columnar-transposition-cipher

Let the key =631245, find the cipher text if Plain=”do DoS Attack”?

ANSWER:

6	3	1	2	4	5
D	o	D	o	S	A
t	t	a	c	k	X

Therefore Thé CipherText=”DaocotSkAXDt”

Example2:

If the Key=”Bashar” encrypt using Matrix if the plain=”Infromation$Security”?

ANSWER:

b	a	s	h	a	r
3	1	6	4	2	5
I	n	f	o	r	m
a	t	i	o	n	$
s	e	c	u	r	i
t	y	X	X	X	X

the CipherText=”ntey rnrX Iast oouX m$Ix ficX”