Name: Sandip Kumar Shah
23081029

Assignment - 1.
Numericals:

Q.no.7 Soln:

Key: KEYWORD
message: WHY DON'T YOU.
diagraph: WH YO ON TY OU
playfair matrix.

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

Now
encoded message: YIEAESVKEZ

Q.no.8 Soln:

plaintext: ABRA KA DABRA

2) ceaser cipher with key = 8

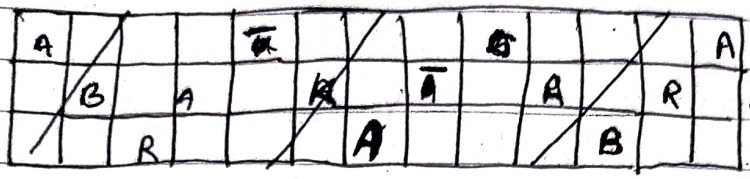
here,

$P_1 = A = 0$; $C_1 = (0+8) \bmod 26 = 8 \Rightarrow I$
$P_2 = B = 1$; $C_2 = (1+8) \bmod 26 = 9 \Rightarrow J$
$P_3 = R = 17$; $C_3 = (17+8) \bmod 26 = 25 \Rightarrow Z$
$P_4 = K = 10$; $C_4 = (10+8) \bmod 26 = 18 \Rightarrow S$
$P_5 = D = 3$; $C_5 = (3+8) \bmod 26 = 11 \Rightarrow L$

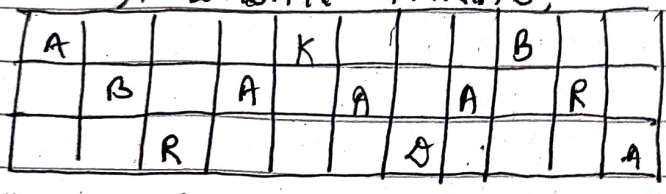
i.e.

ABRA KA DABRA = IJZI SI LIJZI //

b) Raifence cipher with key = 3. (rail)



=> ~~A~~ ~~D~~ABA~~K~~ ~~A~~RR~~A~~B.



=> AKB BAAARR~~D~~A.

Q.no.11 SOLN:

text: ~~D~~AD CAFE ZACH BABE

key: FADE.

newkey = FA~~D~~ EFA~~D~~EFA~~D~~EFA~~D~~

Here analysing the table of vignere cipher we get,

=> iag gffh ifcK ff6h.

Q.no.12 SOLN:

Message: HELP. (P) => $\begin{bmatrix} 7 & 4 \\ 11 & 15 \end{bmatrix}$

key (K) = $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$

Now,

$C = KP \bmod 26$

$= \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 7 & 4 \\ 11 & 15 \end{bmatrix} \bmod 26 = \begin{bmatrix} 54 & 57 \\ 69 & 83 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 2 & 5 \\ 17 & 5 \end{bmatrix} \Rightarrow$ "CFRF"

2×2 ⇒ 2×1.

Q.no. 14

soln:

Message: "MEET ME" ⇒ ME ET ME
12 4 4 19 12 4

key: $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$

Now, for ME: $[12\ 4] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \bmod 26 = \begin{bmatrix} 128 & 76 \end{bmatrix} \bmod 26$

$= [128 \quad 76] \bmod 26$

$= [24 \quad 24] = YY$

Similarly for ET:

$[4\ 19] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \bmod 26 = [131 \quad 149] \bmod 26 = [1 \quad 19]$

⇒ BT.

i.e:

MEET ME = "YY BT YY"

Q.no. 15.

a) ceaser cipher key = 5:

"LOST IN PARADISE" $P_{11} = E = 4$; $C_{11} = (4+5) \bmod 26 = 9 \Rightarrow J$

$P_1 = L = 11$; $C_1 = (11+5) \bmod 26 = 16 \Rightarrow Q$

$P_2 = O = 14$; $C_2 = (14+5) \bmod 26 = 19 \Rightarrow T$

$P_3 = S = 18$; $C_3 = (18+5) \bmod 26 = 23 \Rightarrow X$

$P_4 = T = 19$; $C_4 = (19+5) \bmod 26 = 24 \Rightarrow Y$

$P_5 = I = 8$; $C_5 = (8+5) \bmod 26 = 13 \Rightarrow N$

$P_6 = N = 13$; $C_6 = (13+5) \bmod 26 = 18 \Rightarrow S$

$P_7 = P = 15$; $C_7 = (15+5) \bmod 26 = 20 \Rightarrow U$

$P_8 = A = 0$; $C_8 = (0+5) \bmod 26 = 5 \Rightarrow F$

$P_9 = R = 17$; $C_9 = (17+5) \bmod 26 = 22 \Rightarrow W$

$P_{10} = S = 18$; $C_{10} = (13+5) \bmod 26 = 8 \Rightarrow I$

i.e.

encoded: QTXY NS UF WFIJXJ

6. Raifence cipher with rails = 4.

L						P						S	
	O				N		A				I		E
		S		I				R		O			
			T						A				

encoded : L PSONAIESIROTA.

Q.no.16

soln:

playfair matrix:

"HIDE THE GOLD"

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

NOW

encoded message: IKLMQNLOUGBM

Q.no.18.

soln:

"RUN AWAY".

Key : CRYPTO

playfair matrix:

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

encoded message: CVMBVBPW