NIS LAB3

Prof. Mrudang T. Mehta
Associate Professor
Computer Engineering Department
Faculty of Technology,
Dharmsinh Desai University, Nadiad

- Write a program to implement

1. Playfair cipher
2. Autokey cipher

- Polyalphabetic ciphers
- KEY: MONARCHY (5X5 MATRIX)
- Plain text = givememore= gi ve me mo re
- (u1,v1) = search(g) = (2,2)
- (u2,v2) = search(i) = (2,3)

	0	1	2	3	4
0	M	O	N	A	R
1	C	H	Y	B	D
2	E	F	G	I	K
3	L	P	Q	S	T
4	U	V	W	X	Z

- (0,0), (2,0) (4,1) , (2,0) (4,0), (2,1) (ve)=(UF)

```
If u1 == u2  (same row)
{     s = (v1 +1) mod 5
       t = (v2 +1) mod 5
       k[u1][s], k[u1][t]
}
If v1==v2 (same column)
{    s= (u1 +1) mod 5
       t= (u2 +1) mod 5
       k[s][v1], k[t][v1]
}
Else ( different row, different column)
{      k[u1][v2], k[u2][v1]
}
```

Encryption algorithm

Decryption
Same row
S= (v1-1) mod 5
T= (v2 -1) mod 5
Same column
S= (u1 -1) mod 5
T=(u2 -1) mod 5

(u1,v2) ,(u2,v1)

Autokey cipher

- P =p1 p2 p3.....
- K=(k1, p1, p2, p3,.....)
- C= c1 c2 c3 .....
- C1= (p1 + k1) mod 26
- 12 14 17 22
- 08 12 14 17 22
- 20 0 5 13
- Ci = (pi + ki) mod 26 ki = p(i +1) i >=1
- Pi= (ci – ki) mod 26 ki = p(i -1)