Tutorial 5

Q1 Use a hill cipher to encipher the message "we live in an insecure world". Use the following key

$$K = \begin{bmatrix} 03 & 02 \\ 05 & 07 \end{bmatrix}$$

$$\text{messages} = \begin{bmatrix} we \\ li \\ ve \\ in \\ an \\ in \\ se \\ cu \\ re \\ wo \\ rl \\ dz \end{bmatrix} = \begin{bmatrix} 22, 4 \\ 11, 8 \\ 21, 4 \\ 8, 13 \\ 0, 13 \\ 8, 13 \\ 18, 4 \\ 2, 20 \\ 17, 4 \\ 22, 14 \\ 17, 11 \\ 4, 25 \end{bmatrix}$$

cipher = K x message, vector

$$= \begin{bmatrix} 74, 138 \\ 49, 111 \\ 71, 133 \\ 50, 131 \\ 26, 91 \\ 50, 131 \\ 62, 118 \\ 46, 150 \\ 59, 113 \\ 94, 208 \\ 63, 162 \\ 62, 195 \end{bmatrix} \quad \text{mod } 26$$

$$\equiv \begin{bmatrix} 22, 8 \\ 23, 7 \\ 19, 3 \\ 24, 1 \\ 0, 13 \\ 24, 1 \\ 10, 14 \\ 20, 20 \\ 7, 9 \\ 16, 0 \\ 11, 6 \\ 10, 13 \end{bmatrix} = \begin{bmatrix} wi \\ xh \\ td \\ yb \\ an \\ yb \\ ko \\ uu \\ hj \\ qa \\ lg \\ kn \end{bmatrix}$$

$\Rightarrow$ cipher = wixhtdybanybkouuhjqalgkn

Q2 The plaintext "letusmeetnow" and the corresponding ciphertext "HBCDFNIOPIKLB" are given. You know that the algorithm is a Hill cipher, but you don't know the size of the key. Find the key matrix.

$P = [11, 4, 19, 20, 18, 12, 18, 22, 14, 22, 23]$

$C = [7, 1, 2, 3, 5, 13, 15, 10, 8, 11, 1]$

Key matrix, $K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$\because \quad C = K \times P \bmod 26$

$$\begin{bmatrix} 7 \\ 1 \\ 2 \\ 3 \\ 5 \\ 13 \\ 15 \\ 10 \\ 8 \\ 11 \\ 1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \times \begin{bmatrix} 11 \\ 4 \\ 19 \\ 20 \\ 18 \\ 12 \\ 18 \\ 22 \\ 14 \\ 22 \\ 23 \end{bmatrix} \bmod 26$$

$11a + 4b \equiv 7 \bmod 26$
$19a + 20b \equiv 1 \bmod 26$
$18a + 12b \equiv 2 \bmod 26$
$18c + 22d \equiv 3 \bmod 26$
$14a + 22b \equiv 5 \bmod 26$
$23c \equiv 1 \bmod 26$
$11c + 22d \equiv 13 \bmod 26$
$4c + 19d \equiv 15 \bmod 26$
$20c + 18d \equiv 10 \bmod 26$
$18c + 14d \equiv 8 \bmod 26$
$12c + 22d \equiv 11 \bmod 26$

$a = 3$
$b = 4$ $\quad \therefore \quad K = \begin{bmatrix} 3 & 4 \\ 1 & 3 \end{bmatrix}$
$c = 1$
$d = 3$

Q 3 Using hill cipher technique, encrypt the text "Paymoremoney" using the following key

$$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} = K$$

$$\begin{array}{|ccc|ccc|ccc|ccc|c} P & A & Y & M & O & R & E & M & O & N & E & Y & D \\ 15 & 0 & 24 & 12 & 14 & 17 & 4 & 12 & 14 & 13 & 4 & 24 & \end{array}$$

V_1 $\quad$ V_2 $\quad$ V_3 $\quad$ V_4

$$C_i = K V_i \mod 26$$

$$C_1 = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \times \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 18 \\ 4 \\ 1 \end{bmatrix} = SEB$$

$$C_2 = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \times \begin{bmatrix} 12 \\ 14 \\ 17 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 4 \\ 0 \\ 20 \end{bmatrix} = EAU$$

$$C_3 = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \times \begin{bmatrix} 4 \\ 12 \\ 14 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 1 \\ 8 \\ 15 \end{bmatrix} = \text{BIP}$$

$$C_4 = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \times \begin{bmatrix} 13 \\ 4 \\ 24 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 1 \\ 24 \\ 5 \end{bmatrix} = \text{BYF}$$

~~∴ C = SEBHXK CVFRCZ~~

∴ C = SEB EAU BIP BYF

Q4 Encrypt the following using playfair cipher using the keyword "MONARCHY" "SWARAJ IS MY BIRTH RIGHT". Use X as blank space.

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

SW AR AJ IS MY BI RT HR IG

IJ RP IK RO QT CT PL GT

HT

SW → QX

AR → RM

AJ → BS

IS → SX

MY → NC

BT → DS

RT → DZ

HR → DO

IG → KI

HT → DP

⇒ Cipher = "QX RMBS SXNCD SDZ DOKIDP"

Page :
Date : / /

Q5 Discuss the properties that are satisfied by Groups, Rings & Fields.

Group
- Closure
- Associativity
- Existence of identity element
- Existence of inverse

Ring
- Abelian group
- Closure under multiplication
- Associativity of multiplication
- Distributive laws

Fields
- integral domain
- multiplicative inverse

Q6 Compare substitution & transportation.

	Substitution	Transportation
i)	Plaintext characters are replaced with other characters.	Plaintext characters are rearranged
ii)	Mono alphabetic & Poly alphabetic	Key less & Keyed transposition ciphers
iii)	Character's identity is changed while its position remains unchanged.	Position is changed but identity remains unchanged.
iv)	The letter with high frequency can detect plaintext.	The keys which are nearer to correct key can disclose plaentext.
v)	Caesar cipher, hill cipher, playfair cipher	Columnar, rail-fence cipher.