U20CS005

PAGE NO.
DATE / /

Tutorial-5

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

$$K = \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$$

→

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

w(22)e(4) l(11)i(8) v(21)e(4) i(8)n(13) a(0)n(13) i(8)n(13)
s(18)e(4) c(2)u(20) r(17)e(4) w(22)o(14) r(17)l(11) d(3)z(25)
↳ bogus letter.

$$\begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}\begin{bmatrix} 22 \\ 4 \end{bmatrix} \bmod 26 = \begin{bmatrix} 74 \\ 138 \end{bmatrix} \bmod 26 = \begin{bmatrix} 22 \\ 8 \end{bmatrix} = wi$$

$$\begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}\begin{bmatrix} 11 \\ 8 \end{bmatrix} \bmod 26 = \begin{bmatrix} 49 \\ 111 \end{bmatrix} \bmod 26 = \begin{bmatrix} 23 \\ 7 \end{bmatrix} = xh$$

$$\begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}\begin{bmatrix} 21 \\ 4 \end{bmatrix} \bmod 26 = \begin{bmatrix} 71 \\ 133 \end{bmatrix} \bmod 26 = \begin{bmatrix} 19 \\ 3 \end{bmatrix} = td$$

$$\begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}\begin{bmatrix} 8 \\ 13 \end{bmatrix} \bmod 26 = \begin{bmatrix} 50 \\ 131 \end{bmatrix} \bmod 26 = \begin{bmatrix} 24 \\ 1 \end{bmatrix} = yb$$

$$\begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}\begin{bmatrix} 0 \\ 13 \end{bmatrix} \bmod 26 = \begin{bmatrix} 26 \\ 91 \end{bmatrix} \bmod 26 = \begin{bmatrix} 0 \\ 13 \end{bmatrix} = an$$

$$\begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}\begin{bmatrix} 8 \\ 13 \end{bmatrix} \bmod 26 = \begin{bmatrix} 50 \\ 131 \end{bmatrix} \bmod 26 = \begin{bmatrix} 24 \\ 1 \end{bmatrix} = yb$$

$$\begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}\begin{bmatrix} 18 \\ 4 \end{bmatrix} \bmod 26 = \begin{bmatrix} 62 \\ 118 \end{bmatrix} \bmod 26 = \begin{bmatrix} 10 \\ 14 \end{bmatrix} = ko$$

$$\begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}\begin{bmatrix} 2 \\ 20 \end{bmatrix} \bmod 26 = \begin{bmatrix} 46 \\ 150 \end{bmatrix} \bmod 26 = \begin{bmatrix} 20 \\ 20 \end{bmatrix} = uu$$

$$\begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}\begin{bmatrix} 17 \\ 4 \end{bmatrix} \bmod 26 = \begin{bmatrix} 59 \\ 113 \end{bmatrix} \bmod 26 = \begin{bmatrix} 7 \\ 9 \end{bmatrix} = hj$$

$$\begin{bmatrix}3 & 2\\ 5 & 7\end{bmatrix}\begin{bmatrix}22\\ 14\end{bmatrix} \bmod 26 = \begin{bmatrix}94\\ 208\end{bmatrix} \bmod 26 = \begin{bmatrix}16\\ 0\end{bmatrix} = qa$$

$$\begin{bmatrix}3 & 2\\ 5 & 7\end{bmatrix}\begin{bmatrix}17\\ 11\end{bmatrix} \bmod 26 = \begin{bmatrix}73\\ 162\end{bmatrix} \bmod 26 = \begin{bmatrix}21\\ 6\end{bmatrix} = vg$$

$$\begin{bmatrix}3 & 2\\ 5 & 7\end{bmatrix}\begin{bmatrix}3\\ 25\end{bmatrix} \bmod 26 = \begin{bmatrix}59\\ 190\end{bmatrix} \bmod 26 = \begin{bmatrix}7\\ 8\end{bmatrix} = hi$$

⇒ Encrypted message is,
wi xh td yb an yb ko uu hj qa vg hi

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

$$\begin{pmatrix}17 & 17 & 5\\ 21 & 18 & 21\\ 2 & 2 & 19\end{pmatrix}$$

→ ~~P(15)a(0)y(24)m(12)o(14)r(17)e(4)m(12)o(14)n(13)e(4)y(24)~~

p(15)a(0)y(24) m(12)o(14)r(17) e(4)m(12)o(14) n(13)e(4)y(24)

$$\begin{pmatrix}17 & 17 & 5\\ 21 & 18 & 21\\ 2 & 2 & 19\end{pmatrix}\begin{pmatrix}15\\ 0\\ 24\end{pmatrix} \bmod 26 = \begin{pmatrix}375\\ 819\\ 486\end{pmatrix} \bmod 26 = \begin{pmatrix}11\\ 13\\ 18\end{pmatrix} = lns$$

$$\begin{pmatrix}17 & 17 & 5\\ 21 & 18 & 21\\ 2 & 2 & 19\end{pmatrix}\begin{pmatrix}12\\ 14\\ 17\end{pmatrix} \bmod 26 = \begin{pmatrix}527\\ 861\\ 375\end{pmatrix} \bmod 26 = \begin{pmatrix}7\\ 3\\ 11\end{pmatrix} = hdl$$

$$\begin{pmatrix}17 & 17 & 5\\ 21 & 18 & 21\\ 2 & 2 & 19\end{pmatrix}\begin{pmatrix}4\\ 12\\ 14\end{pmatrix} \bmod 26 = \begin{pmatrix}342\\ 594\\ 198\end{pmatrix} \bmod 26 = \begin{pmatrix}4\\ 22\\ 12\end{pmatrix} = ewon$$

$$\begin{pmatrix}17 & 17 & 5\\ 21 & 18 & 21\\ 2 & 2 & 19\end{pmatrix}\begin{pmatrix}13\\ 4\\ 24\end{pmatrix} \bmod 26 = \begin{pmatrix}359\\ 849\\ 490\end{pmatrix} \bmod 26 = \begin{pmatrix}21\\ 17\\ 22\end{pmatrix} = vrw$$

⇒ Encrypted message is
~~lns hdl ewon vrw~~ lns hdl ewon vrw

PAGE NO.
DATE / /

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

→ Key Matrix is,

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

Plain text is :
SW AR AJ XI SX MY XB IR TH XR IG HT.

⇒ Cipher Text is,
QX RM BS AS XA NC AI KA PD ZA KI DP.

5. Discuss the properties that are satisfied by groups, Rings and fields

→ -Properties satisfied by groups:
1) Closure : $a, b \in G$, then $(a \cdot b) \in G$.
2) Associative : $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in G$
3) Identity Element : $(a \cdot a') = (a' \cdot a) = a \quad \forall a, a' \in G$
4) Inverse Element : $(a \cdot a') = (a' \cdot a) = e \quad \forall a, a' \in G$.

- Properties satisfied by rings:
- It should satisfy all 4 properties of groups ~~at~~along with,
5) commutative : $(a \cdot b) = (b \cdot a) \quad \forall a, b \in R$
6) Closure under Multiplication : if $a, b \in R$ then $ab \in R$.
7) Associativity of Multiplication : $a(bc) = (ab)c \quad \forall a, b, c \in R$
8) Distributive law : $a(b+c) = ab + ac \quad \forall a, b, c \in R$.
$(a+b)c = ac + bc \quad \forall a, b, c \in R$.

- Properties satisfied by ~~rin~~fields :
- All of the above listed properties should be satisfied by field along with,

9) Commutative of multiplication: $ab = ba \quad \forall a, b \in F$.
10) Multiplicative identity: There is an element $1 \in R$ such that $a1 = 1a = a \quad \forall a \in RF$
11) No zero divisors: If $a, b \in F$ th and $ab = 0$, then either $a = 0$ or $b = 0$.
12) Multiplicative invers: For each a in F, except 0, there is an element a^{-1} in F such that $aa^{-1} = (a^{-1})a = 1$

6. Compare substitution and transposition techniques.

→

Substitution Technique	Transposition Technique
- In substitution cipher technique, plain text characters are replaced with other characters, numbers and symbols.	- In transposition cipher technique, plain text characters are rearranged with respect to the position
- Substitution cipher's form are: Monoalphabetic supstitution cipher and poly-alphabetic substitution cipher	- Transposition cipher's form are: Key less transposition cipher & keyed transposition cipher
- In substitution cipher technique, character's identity is changed while its position remain unchanged	- In transposition cipher technique, the position of character is changed but character's identity does not.
- In substitution cipher technique, the letter with low frequency can detect plain text	- In Transposition cipher technique, the key which are nearer to correct key can disclose plain texts.
- Eg Caesar cipher	Eg Rail fence cipher

PAGE NO.
DATE / /

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

→ Plaintext: LETUSMEETNOW

11 4 19 20 18 12 4 4 19 13 14 22

Ciphertext: HBCDFNOPIKLB

7 1 2 3 5 13 14 15 8 10 11 1.

- Since we don't know the size of key matrix, possible size of key matrix can be 2x2, 3x3, 4x4, 12x12, 6x6 as factor of (12 are, 2, 3, 4, 12, 6)

Let's start with 2x2 matrix;

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 11 \\ 4 \end{bmatrix} \bmod 26 = \begin{bmatrix} 7 \\ 1 \end{bmatrix} \quad ; \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 19 \\ 20 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2 \\ 3 \end{bmatrix}$$

$\Rightarrow (11a+4b) \bmod 26 = 7 \quad ; (19a+20b) \bmod 26 = 2$

$(11c+4d) \bmod 26 = 1 \quad ; (19c+20d) \bmod 26 = 3.$

Since $C = KP \pmod{26}$.

we can say $K = C * P^{-1} \pmod{26}$.

$$\Rightarrow \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 7 \\ 2 \end{pmatrix}\begin{pmatrix} 11 & 4 \\ 19 & 20 \end{pmatrix}^{-1} \bmod 26.$$

$\Rightarrow D = 144$ whose inverse under mod 26 is not possible $\Rightarrow$ Size of matrix is not 2x2

- Let's check for 3x3.

$$\begin{pmatrix} 7 \\ 2 \\ 5 \end{pmatrix}\begin{pmatrix} 11 & 4 & 19 \\ 20 & 18 & 12 \\ 4 & 4 & 19 \end{pmatrix}^{-1}$$

$D = 11(342-48) - 4(380-48) + 19(80-72)$

$= 11(294) - 4(332) + 19(8)$

$= 3234 - 1328 + 152$

$\Rightarrow D = 2058$ whose inverse under mod 26 is not possible

$\Rightarrow$ Size of matrix is not 3x3

- Similarly we can prove for 4x4, 12x12, 6x6, inverse doesn't exist for all case.

$\Rightarrow$ Key matrix is not possible for given text pair