

A 1 2 3 4 5 6 7 8 9
 B C D E F G H I J
 K L M N P Q R S T U V W X Y Z
 Date _____
 Page No. _____

① Encrypt the message "meet me at the
 usual place" using the Hill cipher
 with the key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$

m	e	e	t	m	e	a	t	t	h	e	y
12	4	4	19	12	4	0	19	19	7	4	20
18	9	a	l	p	1	d	c	e			
20	20	0	11	15	11	0	2	9			

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

plain text $(m)(e)(m)(e)(t)(h)(e)(y)(a)(t)(c)(e)$
 $(e)(t)(e)(t)(h)(y)(c)(x)$

step :- 1 $c = pK \bmod 26$ $\begin{pmatrix} m \\ e \end{pmatrix}$

$$= \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 12 \\ 4 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 108 + 16 \\ 60 + 28 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 124 \\ 88 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 20 \\ 10 \end{bmatrix} = \begin{bmatrix} 4 \\ 10 \end{bmatrix}$$

Step 2- $c = PK \bmod 26$ (at t)

$$= \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \text{ mod } \begin{bmatrix} 4 & 1 \\ 19 & 1 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 36 + 76 \\ 20 + 133 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 112 \\ 153 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 8 \\ 23 \end{bmatrix} \rightarrow \begin{bmatrix} I \\ X \end{bmatrix}$$

Step 36- $c = PK \bmod 26$ (on e)

same as step-1 (u/k)

Step 46- $c = PK \bmod 26$ (at)

$$= \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 0 + 76 \\ 0 + 133 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 76 \\ 133 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 24 \\ 3 \end{bmatrix} \rightarrow \begin{bmatrix} 9 \\ 0 \end{bmatrix}$$

Step 5-5 : $C = PK \bmod 26 \quad \binom{t}{h}$

$$= \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \cdot \begin{bmatrix} 19 \\ 7 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 171 + 28 \\ 95 + 49 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 199 \\ 144 \end{bmatrix} \quad \left[\begin{array}{l} 199 \\ 144 \end{array} \right]$$

$$= \begin{bmatrix} 17 \\ 14 \end{bmatrix} \cdot \begin{bmatrix} R \\ 0 \end{bmatrix}$$

Step 6 : $C = PK \bmod 26 \quad \binom{e}{u}$

$$= \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 4 \\ 90 \end{bmatrix}$$

$$= \begin{bmatrix} 9 \times 4 + 4 \times 20 \\ 5 \times 4 + 7 \times 20 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 36 + 80 \\ 20 + 140 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 116 \\ 160 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 12 \\ 4 \end{bmatrix} = \begin{bmatrix} m \\ e \end{bmatrix}$$

Step 7: $c = pK \bmod 26 \quad \begin{pmatrix} s \\ 4 \end{pmatrix}$

$$= \begin{bmatrix} 9 \cdot 4 \\ 57 \end{bmatrix} \begin{bmatrix} 18 \\ 20 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 162 + 80 \\ 90 + 140 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 242 \\ 280 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 8 \\ 22 \end{bmatrix} \div \begin{bmatrix} I \\ w \end{bmatrix}$$

Step 8: $c = pK \bmod 26 \quad \begin{pmatrix} a \\ e \end{pmatrix}$

$$= \begin{bmatrix} 9 \cdot 4 \\ 57 \end{bmatrix} \begin{bmatrix} 0 \\ 11 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 0 + 44 \\ 0 + 77 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 44 \\ 77 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 18 \\ 25 \end{bmatrix} \div \begin{bmatrix} 5 \\ 2 \end{bmatrix}$$

Step :- 9 $c = PK \bmod 26 \quad (P)$

$$= \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 15 \\ 11 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 135 + 44 \\ 75 + 77 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 179 \\ 152 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 23 \\ 22 \end{bmatrix} = \begin{bmatrix} x \\ w \end{bmatrix}$$

Step :- 10 $c = PK \bmod 26 \quad (C)$

$$= \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \end{bmatrix}$$

$$= \begin{bmatrix} 0 + 8 \\ 0 + 14 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 8 \\ 14 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Step :- 11 $c = PK \bmod 26 \quad \begin{bmatrix} e \\ x \end{bmatrix}$

$$= \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 9 \\ 23 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 36 + 92 \\ 20 + 161 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 128 \\ 181 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 24 \\ 25 \end{bmatrix} = \begin{bmatrix} y \\ ? \end{bmatrix}$$

plain-text :- meet me at the 4440 place

ciphertext = UKTXUKYDROMeIWSZXWTOY

- (2) Encrypt the message "Exam" using hill cipher with the key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$.

solution

$$\text{Key matrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$$

$$\text{plain text} = \begin{bmatrix} E \\ x \end{bmatrix} \begin{bmatrix} A \\ m \end{bmatrix} = \begin{bmatrix} 4 \\ 23 \end{bmatrix} \begin{bmatrix} 0 \\ 12 \end{bmatrix}$$

$$\text{Step 2-1 } c = PK \bmod 26$$

$$= \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 4 \\ 23 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 36 + 92 \\ 20 + 161 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 128 \\ 181 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 24 \\ 25 \end{bmatrix} = \begin{bmatrix} y \\ z \end{bmatrix}$$

Step 2 $c = pk \text{ mod } 26$ $\begin{bmatrix} y \\ m \end{bmatrix}$

$$= \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 0 \\ 12 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 0+48 \\ 0+84 \end{bmatrix} \text{ mod } 26$$

$$\begin{bmatrix} 22 \\ 6 \end{bmatrix} = \begin{bmatrix} w \\ v \end{bmatrix}$$

plain text :- Eium

cipher text = yzwvt

- ③ Encrypt the message "REDPEN" using Hill cipher with the key $\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$

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

plain-text :-

$$\begin{bmatrix} R \\ E \\ D \end{bmatrix} \begin{bmatrix} P \\ E \\ N \end{bmatrix}$$

Step 1 :- $c = PK \bmod 26$

$$\begin{bmatrix} R \\ E \\ D \end{bmatrix}$$

$$= \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 17 \\ 4 \\ 3 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 289 + 68 + 15 \\ 357 + 72 + 63 \\ 34 + 8 + 57 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 372 \\ 492 \\ 99 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 8 \\ 24 \\ 21 \end{bmatrix} \cdot \begin{bmatrix} I \\ y \\ v \end{bmatrix}$$

Step 2 :- $c = PK \bmod 26$

$$\begin{bmatrix} P \\ c \\ n \end{bmatrix}$$

$$= \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 15 \\ 4 \\ 13 \end{bmatrix}$$

$$= \begin{bmatrix} 255 + 68 + 65 \\ 315 + 42 + 273 \\ 30 + 8 + 44 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 388 \\ 660 \\ 285 \end{bmatrix} \mod 26$$

$$\therefore = \begin{bmatrix} 24 \\ 10 \\ 25 \end{bmatrix} = \begin{bmatrix} A \\ K \\ Z \end{bmatrix}$$

Plain text: REDPEN

Cipher text: IYVYGKZ

- ① Use Hill cipher to encrypt the text
 PEE. The key to be used is
- $$\begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 8 & 7 \end{bmatrix}$$

Key matrix:

$$\begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 8 & 7 \end{bmatrix}$$

Plain text :-

$$\begin{bmatrix} D \\ E \\ F \end{bmatrix}$$

$$C = P K \mod 26$$

$$= \begin{bmatrix} 2 & 9 & 5 \\ 9 & 2 & 1 \\ 3 & 8 & 7 \end{bmatrix} \begin{bmatrix} 3 \\ 4 \\ 5 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 6 + 16 + 25 \\ 24 + 8 + 5 \\ 9 + 32 + 35 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 47 \\ 40 \\ 76 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 21 \\ 14 \\ 24 \end{bmatrix} = \begin{bmatrix} V \\ O \\ Y \end{bmatrix}$$

plain text : DEF

cipher text : VOY

(5) message "ATTACK IS TONIGHT" using
hill cipher with the key $\begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix}$

SOL:

$$\text{Key} : \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix}$$

$$\text{plain text} : \begin{bmatrix} A \\ T \\ C \end{bmatrix} \begin{bmatrix} A \\ I \\ K \end{bmatrix} \begin{bmatrix} I \\ S \\ T \end{bmatrix} \begin{bmatrix} O \\ N \\ E \end{bmatrix} \begin{bmatrix} G \\ H \\ T \end{bmatrix}$$

Step 1: $c = P K \bmod 26$

\Rightarrow

$$\begin{bmatrix} A \\ T \\ T \end{bmatrix}$$

$$= \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \\ 19 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 0 + 190 + 380 \\ 0 + 171 + 329 \\ 0 + 76 + 329 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 570 \\ 500 \\ 405 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 24 \\ 6 \\ 15 \end{bmatrix} = \begin{bmatrix} q \\ r \\ p \end{bmatrix}$$

Step 2: $c = P K \bmod 26$

$$\begin{bmatrix} A \\ c \\ K \end{bmatrix}$$

$$= \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 10 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 0 + 20 + 200 \\ 0 + 18 + 170 \\ 0 + 8 + 170 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 220 \\ 188 \\ 178 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 12 \\ 6 \\ 22 \end{bmatrix} \cdot \begin{bmatrix} m \\ q \\ w \end{bmatrix}$$

Step 3: $c = p \cdot k \text{ mod } 26$ $\begin{bmatrix} 1 \\ 5 \\ 7 \end{bmatrix}$

$$= \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 29 & 4 & 17 \end{bmatrix} \begin{bmatrix} 8 \\ 18 \\ 19 \end{bmatrix} \text{ mod. } 26$$

$$= \begin{bmatrix} 24 + 180 + 380 \\ 160 + 162 + 323 \\ 72 + 76 + 323 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 584 \\ 645 \\ 471 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 12 \\ 21 \\ 3 \end{bmatrix} = \begin{bmatrix} m \\ v \\ o \end{bmatrix}$$

Step 4: $c \cdot p \cdot k \text{ mod } 26$ $\begin{bmatrix} 0 \\ N \\ 1 \end{bmatrix}$

$$= \begin{bmatrix} 3 & 10 & 26 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix} \begin{bmatrix} 14 \\ 13 \\ 8 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 42 + 130 + 160 \\ 280 + 117 + 186 \\ 126 + 52 + 136 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 332 \\ 533 \\ 814 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 20 \\ 13 \\ 2 \end{bmatrix} = \begin{bmatrix} U \\ N \\ C \end{bmatrix}$$

Step 5: $C = P K \mod 26$ $\begin{bmatrix} G \\ H \\ T \end{bmatrix}$

$$= \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix} \cdot \begin{bmatrix} 6 \\ 7 \\ 19 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 18 + 70 + 380 \\ 120 + 63 + 323 \\ 54 + 28 + 323 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 468 \\ 506 \\ 405 \end{bmatrix} \mod 26 \Rightarrow \begin{bmatrix} 0 \\ 12 \\ 15 \end{bmatrix} = \begin{bmatrix} A \\ m \\ p \end{bmatrix}$$

plain text: ATTACK IS TONIGHT
 cipher text \Rightarrow yipmaw ~~MPDUNCAMP~~

Final pt "Theory" using Hill cipher with key

$$\begin{bmatrix} 7 & 5 \\ 18 & 17 \end{bmatrix}$$

$$\text{plain + cat} = \begin{bmatrix} T \\ h \end{bmatrix} \begin{bmatrix} e \\ 0 \end{bmatrix} \begin{bmatrix} y \\ g \end{bmatrix}$$

$$\text{Step :- 1 } C = PK \bmod 26 \quad \begin{bmatrix} T \\ h \end{bmatrix}$$

$$= \begin{bmatrix} 7 & 5 \\ 18 & 17 \end{bmatrix} \begin{bmatrix} 19 \\ 7 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 168 \\ 461 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 12 \\ 19 \end{bmatrix} = \begin{bmatrix} m \\ T \end{bmatrix}$$

$$\text{Step :- 2 } C = PK \bmod 26 \quad \begin{bmatrix} e \\ 0 \end{bmatrix}$$

$$= \begin{bmatrix} 7 & 5 \\ 18 & 17 \end{bmatrix} \begin{bmatrix} 4 \\ 14 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 98 \\ 310 \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 20 \\ 24 \end{bmatrix} = \begin{bmatrix} u \\ y \end{bmatrix}$$

$$\text{Step :- 3 } C = PK \bmod 26 \quad \begin{bmatrix} u \\ y \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 7 & 5 \\ 18 & 17 \end{bmatrix} \begin{bmatrix} 17 \\ 24 \end{bmatrix} \bmod 26$$

$$\Rightarrow \begin{bmatrix} 19 & 120 \\ 306 & 408 \end{bmatrix} \bmod 26$$

Hill cipher

Date			
Page			

$$\Rightarrow \begin{bmatrix} 23 & 9 \\ 7 & 14 \end{bmatrix} \text{ mod } 25$$

$$= \begin{bmatrix} 5 \\ 12 \end{bmatrix} = \begin{bmatrix} F \\ m \end{bmatrix}$$

Plain text :- Theory

Cipher text :- MIUJFm

- (6) Encrypt "pay more money" using Hill cipher with the key $\begin{bmatrix} 17 & 5 & 7 \\ 18 & 9 & 1 \\ 2 & 2 & 19 \end{bmatrix}$

$$\text{Plain text: - } \begin{bmatrix} p \\ q \\ r \end{bmatrix} \begin{bmatrix} m \\ o \\ r \end{bmatrix} \begin{bmatrix} e \\ m \\ o \end{bmatrix} \begin{bmatrix} n \\ e \\ g \end{bmatrix}$$

$$\text{Step 1: - } c = pK \text{ mod } 26 \quad \begin{bmatrix} p \\ q \\ r \end{bmatrix}$$

$$= \begin{bmatrix} 17 & 17 & 5 \\ 18 & 8 & 1 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 5 \\ 1 \\ 24 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 255 + 0 + 120 \\ 315 + 0 + 504 \\ 30 + 0 + 456 \end{bmatrix}$$

$$= \begin{bmatrix} 375 \\ 819 \\ 486 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 11 \\ 13 \\ 18 \end{bmatrix} = \begin{bmatrix} L \\ N \\ S \end{bmatrix}$$

Step :- 2 $C = PK \bmod 26$ $\begin{bmatrix} m \\ 0 \\ e \end{bmatrix}$

$$\Rightarrow \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 12 \\ 14 \\ 17 \end{bmatrix} \bmod 26$$

$$\Rightarrow \begin{bmatrix} 204 + 288 + 85 \\ 252 + 252 + 357 \\ 24 + 28 + 323 \end{bmatrix} \bmod 26$$

$$\Rightarrow \begin{bmatrix} 527 \\ 861 \\ 375 \end{bmatrix} \bmod 26.$$

$$\Rightarrow \begin{bmatrix} 7 \\ 3 \\ 12 \end{bmatrix} = \begin{bmatrix} H \\ D \\ C \end{bmatrix}$$

Step:-3 $c = PK \bmod 26$ $\begin{bmatrix} e \\ m \\ 16 \end{bmatrix}$

$$= \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 9 \\ 12 \\ 14 \end{bmatrix} \bmod 26$$

$$\text{P} = \begin{bmatrix} 68 + 204 + 70 \\ 84 + 216 + 294 \\ 8 + 24 + 266 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 342 \\ 594 \\ 298 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 4 \\ 22 \\ 12 \end{bmatrix} = \begin{bmatrix} F \\ W \\ m \end{bmatrix}$$

$$\text{Step 4 } C = P \times \begin{bmatrix} n \\ e \\ g \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 13 \\ 9 \\ 24 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 221 + 68 + 120 \\ 273 + 32 + 504 \\ 26 + 8 + 456 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 409 \\ 849 \\ 490 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 19 \\ 17 \\ 22 \end{bmatrix} = \begin{bmatrix} T \\ R \\ W \end{bmatrix}$$

Plaintext is Pay more money
cipher text:- CNS HDL EWM TRW