Hill Cipher

Another interesting multiletter cipher is the Hill cipher, developed by the mathematician Lester Hill in 1929.

the Hill cipher is apolygraphic substitution cipher based on linear algebra. developed by the mathematician Lester S. Hill. It was the first polygraphic cipher in which it was practical to operate on more than three symbols at once.

Encryption:

C = K P mod 26

Decryption:

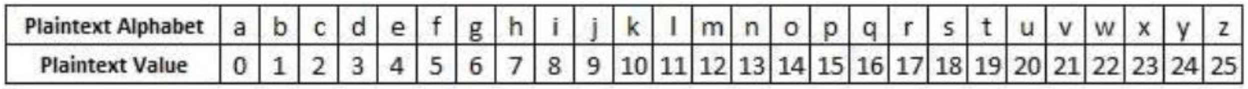
P = K^{-1}C mod 26

To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an

Invertible n*n matrix, against modulus 26.

To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption. The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible(modulo26).

The cipher can, of course, be adapted to an alphabet with any number of letters; all arithmetic just needs to be done modulo the number of letters instead ofmodulo26.



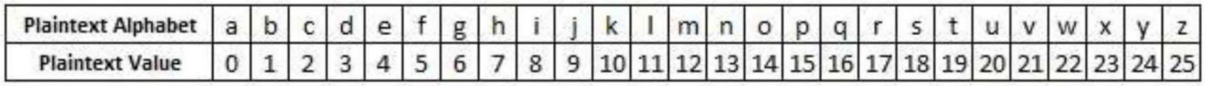
Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Example: Encrypt the plaintext “attack”, using Hill cipher for the given key = $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$.

Ans. :

Since the key is a 2x2 Matrix, plaintext should be converted into vectors of length 2. So, $\begin{bmatrix} a \\ t \end{bmatrix}_{2x1} \begin{bmatrix} t \\ a \end{bmatrix}_{2x1} \begin{bmatrix} c \\ k \end{bmatrix}_{2x1}$

Encryption:



Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

1) **1st Vector** $\begin{bmatrix} a \\ t \end{bmatrix}_{2x1} = \begin{bmatrix} 0 \\ 19 \end{bmatrix}$, **key =** $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$,

$$\mathbf{C = K\ P\ mod\ 26} = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 2(0) + 3\,(19) \\ 3(0) + 6\,(19) \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 57 \\ 114 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 5 \\ 10 \end{bmatrix} = \begin{bmatrix} F \\ K \end{bmatrix}$$

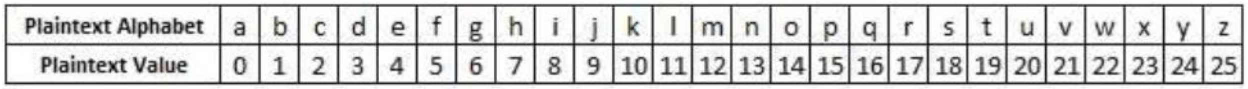
2) **2nd Vector** $\begin{bmatrix} t \\ a \end{bmatrix}_{2x1} = \begin{bmatrix} 19 \\ 0 \end{bmatrix}$

$$\mathbf{C = K\ P\ mod\ 26} = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 19 \\ 0 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 2(19) + 3\,(0) \\ 3(19) + 6\,(0) \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 38 \\ 57 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 12 \\ 5 \end{bmatrix} = \begin{bmatrix} M \\ F \end{bmatrix}$$

3) **3rd Vector** $\begin{bmatrix} c \\ k \end{bmatrix}_{2x1} = \begin{bmatrix} 2 \\ 10 \end{bmatrix}$

$$\mathbf{C = K\ P\ mod\ 26} = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 2 \\ 10 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 2(2) + 3\,(10) \\ 3(2) + 6\,(10) \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 34 \\ 66 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 8 \\ 14 \end{bmatrix} = \begin{bmatrix} I \\ O \end{bmatrix}$$

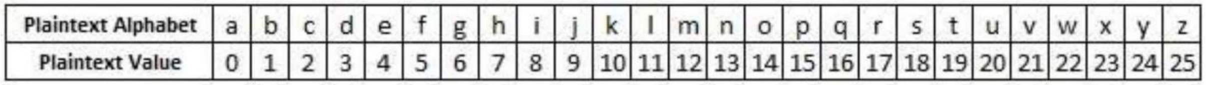
Ciphertext: “FKMFIO”.



Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Example: Decrypt the ciphertext**"FKMFIO"**, using Hill cipher for the given key = $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$.

Ans. :



Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

P = $\mathbf{K^{-1}}$ C mod 26

$$\textbf{Inverse of Key Matrix } \mathbf{K^{-1}} = \frac{\mathbf{1}}{|\mathbf{K}|} \textbf{ adj (K)} = \mathbf{K^{-1}} \textbf{ adj (K)} = \frac{\mathbf{1}}{|\mathbf{D}|} \textbf{ adj (K)} = \mathbf{D^{-1}} \textbf{ adj (K)}$$

$$\textbf{determinant of Matrix } \mathbf{D} = \begin{vmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{vmatrix} = |\mathbf{ad} - \mathbf{bc}|, \textbf{ where } \mathbf{D} \neq \mathbf{0}$$

$$\mathbf{D} = \begin{vmatrix} \mathbf{2} & \mathbf{3} \\ \mathbf{3} & \mathbf{6} \end{vmatrix} = |\mathbf{12} - \mathbf{9}| = \mathbf{3}$$

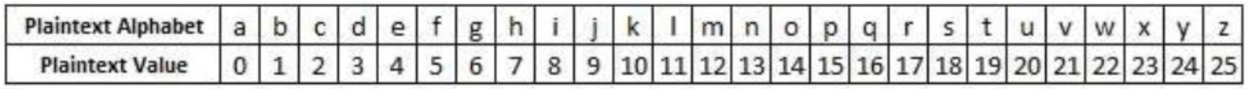
Now, find multiplicative inverse of determinant $\mathbf{D\,D^{-1} = 1 \text{ mod } 26}$

Using hit and trial method 3 $\mathbf{D^{-1}} \equiv \mathbf{1} \; \boldsymbol{mod} \; \mathbf{26}$ = 3 $\mathbf{D^{-1}}$mod 26 = 1

$\mathbf{3 \times 9 \text{ mod } 26 = 27 \text{ mod } 26 = 1}$, $\mathbf{D^{-1}}$= 9.

To find the adjoint of the Matrix A $= \begin{bmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{bmatrix}$, adj (A) = $\begin{bmatrix} \mathbf{d} & -\mathbf{b} \\ -\mathbf{c} & \mathbf{a} \end{bmatrix}$

Here, K $= \begin{bmatrix} \mathbf{2} & \mathbf{3} \\ \mathbf{3} & \mathbf{6} \end{bmatrix}$, adj (K) = $\begin{bmatrix} \mathbf{6} & -\mathbf{3} \\ -\mathbf{3} & \mathbf{2} \end{bmatrix}$ = $\begin{bmatrix} \mathbf{6} & \mathbf{23} \\ \mathbf{23} & \mathbf{2} \end{bmatrix}$



Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Inverse of Key Matrix $K^{-1} = \frac{1}{|K|}\ \text{adj}\ (K) = K^{-1}\ \text{adj}\ (K) = \frac{1}{|D|}\ \text{adj}\ (K) = D^{-1}\ \text{adj}\ (K)$

$$K^{-1} = 9\begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 54 & 207 \\ 207 & 18 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}$$

Now, we will decrypt the cipher: FK MF IO

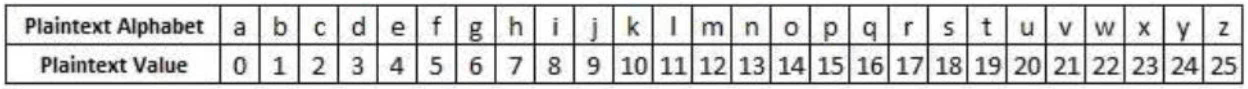
$$C = \begin{bmatrix} F \\ K \end{bmatrix}_{2x1} = \begin{bmatrix} 5 \\ 10 \end{bmatrix}, C = \begin{bmatrix} M \\ F \end{bmatrix}_{2x1} = \begin{bmatrix} 12 \\ 5 \end{bmatrix}, C = \begin{bmatrix} I \\ O \end{bmatrix}_{2x1} = \begin{bmatrix} 8 \\ 14 \end{bmatrix}$$

$$P = K^{-1}\ C \text{ mod } 26 = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}\begin{bmatrix} 5 \\ 10 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 2(5) + 25\ (10) \\ 25(5) + 18\ (10) \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 260 \\ 305 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 0 \\ 19 \end{bmatrix} = \begin{bmatrix} a \\ t \end{bmatrix}$$

$$P = K^{-1}\ C \text{ mod } 26 = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}\begin{bmatrix} 12 \\ 5 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 2(12) + 25\ (5) \\ 25(12) + 18\ (5) \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 149 \\ 390 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 19 \\ 0 \end{bmatrix} = \begin{bmatrix} t \\ a \end{bmatrix}$$

$$P = K^{-1}\ C \text{ mod } 26 = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}\begin{bmatrix} 8 \\ 14 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 2(8) + 25\ (14) \\ 25(8) + 18\ (14) \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 366 \\ 452 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 2 \\ 10 \end{bmatrix} = \begin{bmatrix} c \\ k \end{bmatrix}$$

Plaintext: “attack”



Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Example: Encrypt the plaintext “safe messages”, using Hill cipher for the given key: **“ciphering”.**

Ans. :

Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Since key is a 3 × 3 Matrix, plaintext should be converted into column vectors of length 3. i.e.

(n × 1) ≡ (3 × 1) matrices. So, we get: saf, eme, ssa, ges.

$$\begin{bmatrix} s \\ a \\ f \end{bmatrix} = \begin{bmatrix} 18 \\ 0 \\ 5 \end{bmatrix}, \begin{bmatrix} e \\ m \\ e \end{bmatrix} = \begin{bmatrix} 4 \\ 12 \\ 4 \end{bmatrix}, \begin{bmatrix} s \\ s \\ a \end{bmatrix} = \begin{bmatrix} 18 \\ 18 \\ 0 \end{bmatrix}, \begin{bmatrix} g \\ e \\ s \end{bmatrix} = \begin{bmatrix} 6 \\ 4 \\ 18 \end{bmatrix}.$$

$$\textbf{Key} = \textbf{ciphering} = \begin{bmatrix} c & i & p \\ h & e & r \\ i & n & g \end{bmatrix} = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}.$$

$$\mathbf{C = K\,P \bmod 26} = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \begin{bmatrix} 18 \\ 0 \\ 5 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2(18) + 8(0) + 15(5) \\ 7(18) + 4(0) + 17(5) \\ 8(18) + 13(0) + 6(5) \end{bmatrix} \bmod 26 = \begin{bmatrix} 111 \\ 211 \\ 174 \end{bmatrix} \bmod 26 = \begin{bmatrix} 7 \\ 3 \\ 18 \end{bmatrix} = \begin{bmatrix} H \\ D \\ S \end{bmatrix}.$$

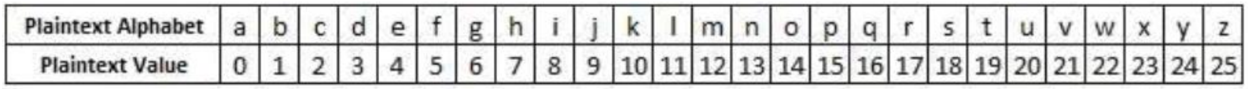
Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

$$\mathbf{C = K\,P \bmod 26 = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \begin{bmatrix} 4 \\ 12 \\ 4 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2(4)+8(12)+15(4) \\ 7(4)+4(12)+17(4) \\ 8(4)+13(12)+6(4) \end{bmatrix} \bmod 26 = \begin{bmatrix} 164 \\ 144 \\ 212 \end{bmatrix} \bmod 26 = \begin{bmatrix} 8 \\ 14 \\ 4 \end{bmatrix} = \begin{bmatrix} I \\ O \\ E \end{bmatrix}}.$$

$$\mathbf{C = K\,P \bmod 26 = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \begin{bmatrix} 18 \\ 18 \\ 0 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2(18)+8(18)+15(0) \\ 7(18)+4(18)+17(0) \\ 8(18)+13(18)+6(0) \end{bmatrix} \bmod 26 = \begin{bmatrix} 180 \\ 198 \\ 378 \end{bmatrix} \bmod 26 = \begin{bmatrix} 24 \\ 16 \\ 14 \end{bmatrix} = \begin{bmatrix} Y \\ Q \\ O \end{bmatrix}}.$$

$$\mathbf{C = K\,P \bmod 26 = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \begin{bmatrix} 6 \\ 4 \\ 18 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2(6)+8(4)+15(18) \\ 7(6)+4(4)+17(18) \\ 8(6)+13(4)+6(18) \end{bmatrix} \bmod 26 = \begin{bmatrix} 314 \\ 364 \\ 208 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} C \\ A \\ A \end{bmatrix}}.$$

Ciphertext: “HDSIOEYQOCAA”

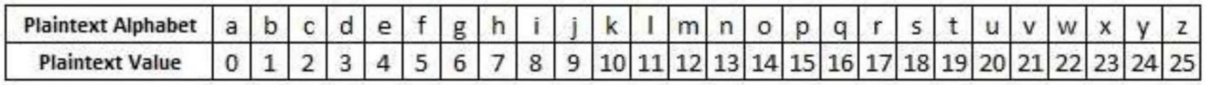


Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Example: Decrypt the plaintext **“HDSIOEYQOCAA”**, using Hill cipher for the given key: **“ciphering”.**

Ans. :

$$\begin{bmatrix} H \\ D \\ S \end{bmatrix} = \begin{bmatrix} 7 \\ 3 \\ 18 \end{bmatrix}, \begin{bmatrix} I \\ O \\ E \end{bmatrix} = \begin{bmatrix} 8 \\ 14 \\ 4 \end{bmatrix}, \begin{bmatrix} Y \\ Q \\ O \end{bmatrix} = \begin{bmatrix} 24 \\ 16 \\ 14 \end{bmatrix}, \begin{bmatrix} C \\ A \\ A \end{bmatrix} = \begin{bmatrix} 2 \\ 0 \\ 0 \end{bmatrix}.$$



Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

$$P = K^{-1}\ C \bmod 26$$

$$\textbf{Inverse of Key Matrix } K^{-1} = \frac{1}{|K|}\ \text{adj}\ (K) = K^{-1}\ \text{adj}\ (K) = \frac{1}{|D|}\ \text{adj}\ (K) = D^{-1}\ \text{adj}\ (K)$$

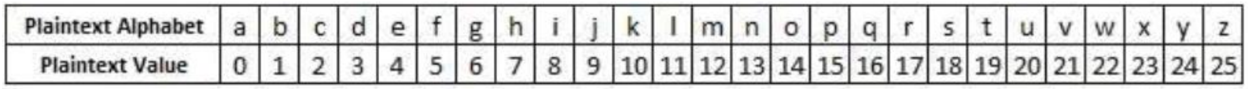
$$\det = \begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = a \begin{vmatrix} e & f \\ h & i \end{vmatrix} - b \begin{vmatrix} d & f \\ g & i \end{vmatrix} + c \begin{vmatrix} d & e \\ g & h \end{vmatrix} = a\,(ei - fh) - b\,(di - fg) + c\,(dh - eg)$$

$$D = \begin{vmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{vmatrix} = 2 \begin{vmatrix} 4 & 17 \\ 13 & 6 \end{vmatrix} - 8 \begin{vmatrix} 7 & 17 \\ 8 & 6 \end{vmatrix} + 15 \begin{vmatrix} 7 & 4 \\ 8 & 13 \end{vmatrix} = 2\,(24 - 221) - 8\,(28 - 136) + 15(91 - 32) = 1243$$

$$D\,D^{-1} \equiv 1 \bmod 26 = 1243\ .\ D^{-1} \equiv 1 \bmod 26 = 1243\ \times 5 \bmod 26 = 6215 \bmod 26 = 1$$

,

$$D^{-1} = 5$$



Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

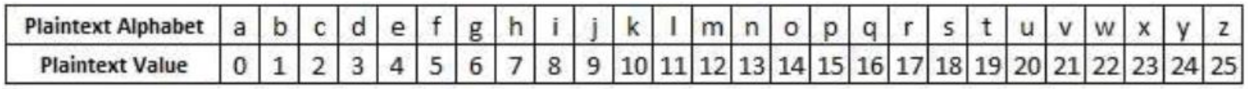
Now, we will find the inverse of (K).

$$K^{-1} = \frac{1}{|D|}\,\text{adj (K)} = D^{-1}\,\text{adj (K)} = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}^{-1} = \frac{1}{|D|}\begin{bmatrix} +(ei-fh) & -(di-fg) & +(dh-eg) \\ -(bi-ch) & +(ai-cg) & -(ah-bg) \\ +(bf-ce) & -(af-cd) & +(ae-bd) \end{bmatrix}^{T}$$

$$K^{-1} = \frac{1}{|D|}\,\text{adj (K)} = D^{-1}\,\text{adj (K)} = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}^{-1} = 5\begin{bmatrix} +(24-221) & -(42-136) & +(91-32) \\ -(48-195) & +(12-120) & -(26-64) \\ +(136-60) & -(34-105) & +(8-56) \end{bmatrix}^{T}$$

$$K^{-1} = 5\begin{bmatrix} +(-197) & -(-94) & +(59) \\ -(-147) & +(-108) & -(-38) \\ +(76) & -(-71) & +(-48) \end{bmatrix}^{T} = 5\begin{bmatrix} -197 & 94 & 59 \\ 147 & -108 & 38 \\ 76 & 71 & -48 \end{bmatrix}^{T} = 5\begin{bmatrix} -197 & 147 & 76 \\ 94 & -108 & 71 \\ 59 & 38 & -48 \end{bmatrix}$$

$$K^{-1} = \begin{bmatrix} -985 & 735 & 380 \\ 470 & -540 & 355 \\ 295 & 190 & -240 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix}, K^{-1} = \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix}$$



Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Example: Encrypt the plaintext “safe messages”, using Hill cipher for the given key: **“ciphering”.**

Ans. :

Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Since key is a 3 × 3 Matrix, plaintext should be converted into column vectors of length 3. i.e. (n × 1) ≡ (3 × 1) matrices. So, we get: saf, eme, ssa, ges.

$$\begin{bmatrix} \mathrm{s} \\ \mathrm{a} \\ \mathrm{f} \end{bmatrix} = \begin{bmatrix} 18 \\ 0 \\ 5 \end{bmatrix}, \begin{bmatrix} \mathrm{e} \\ \mathrm{m} \\ \mathrm{e} \end{bmatrix} = \begin{bmatrix} 4 \\ 12 \\ 4 \end{bmatrix}, \begin{bmatrix} \mathrm{s} \\ \mathrm{s} \\ \mathrm{a} \end{bmatrix} = \begin{bmatrix} 18 \\ 18 \\ 0 \end{bmatrix}, \begin{bmatrix} \mathrm{g} \\ \mathrm{e} \\ \mathrm{s} \end{bmatrix} = \begin{bmatrix} 6 \\ 4 \\ 18 \end{bmatrix}.$$

$$\mathbf{Key} = \mathbf{ciphering} = \begin{bmatrix} c & i & p \\ h & e & r \\ i & n & g \end{bmatrix} = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}.$$

$$\mathbf{C = K\,P \bmod 26} = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \begin{bmatrix} 18 \\ 0 \\ 5 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2(18) + 8(0) + 15(5) \\ 7(18) + 4(0) + 17(5) \\ 8(18) + 13(0) + 6(5) \end{bmatrix} \bmod 26 = \begin{bmatrix} 111 \\ 211 \\ 174 \end{bmatrix} \bmod 26 = \begin{bmatrix} 7 \\ 3 \\ 18 \end{bmatrix} = \begin{bmatrix} \mathrm{H} \\ \mathrm{D} \\ \mathrm{S} \end{bmatrix}.$$

Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25