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

ciphertext:

R	U	P	O	T	E	N	T	O	I	F	V
17	20	15	14	19	4	13	19	14	8	5	21

message:

B	R	E	A	T	H	T	A	K	I	N	G
1	17	4	0	19	7	19	0	10	8	13	6

$C_1 = [17, 20, 15]$ $\quad m_1 = [1, 17, 4]$
$C_2 = [14, 19, 4]$ $\quad m_2 = [0, 19, 7]$
$C_3 = [13, 19, 14]$ $\quad m_3 = [19, 0, 10]$
$C_4 = [8, 5, 21]$ $\quad m_4 = [8, 13, 6]$

$$C = \begin{bmatrix} 17 & 14 & 8 \\ 20 & 19 & 5 \\ 15 & 4 & 21 \end{bmatrix} \qquad m = \begin{bmatrix} 1 & 0 & 8 \\ 17 & 19 & 13 \\ 4 & 7 & 6 \end{bmatrix}$$

Sea K la matriz key

$$m \times K = C \quad \therefore \quad K = C \times m^{-1}$$

$$m = \frac{1}{\det(m)} \begin{bmatrix} A & B & C \\ D & E & F \\ G & H & I \end{bmatrix}^T \bmod 26 = \frac{1}{\det(m)} \begin{bmatrix} A & D & G \\ B & E & H \\ C & F & I \end{bmatrix} \bmod 26$$

$$\begin{aligned} \text{Det}(M) &= (1 \times 19 \times 6 + 17 \times 7 \times 8 + 4 \times 0 \times 13) - (4 \times 19 \times 8 + 7 \times 13 \times 1 + 17 \times 0 \times 6) \\ &= 1066 - 699 \\ &= 367 \bmod 26 = 3 \end{aligned}$$

$A = 19 \times 6 - 13 \times 7 = 23$ $\quad D = 8 \times 7 - 0 = 56$ $\quad G = 0 \times 13 - 19 \times 8 = -152$
$B = 4 \times 13 - 17 \times 6 = -50$ $\quad E = 1 \times 6 - 4 \times 8 = -26$ $\quad H = 8 \times 17 - 1 \times 13 = 123$
$C = 17 \times 7 - 4 \times 19 = 43$ $\quad F = 0 \times 4 - 1 \times 7 = -7$ $\quad I = 1 \times 19 - 0 \times 17 = 19$

$$m^{-1} = \frac{1}{3} \begin{bmatrix} 23 & -50 & 43 \\ 56 & -26 & -7 \\ -152 & 123 & 19 \end{bmatrix}^T (\bmod 26) = \frac{1}{3} \begin{bmatrix} 23 & 56 & -152 \\ -50 & -26 & 123 \\ 43 & -7 & 19 \end{bmatrix} (\bmod 26)$$

Inverso multiplicativo de $\frac{1}{3} \bmod 26 \Rightarrow 9 \times 3 \bmod 26 = 1 \quad \therefore 9$

$$m^{-1} = 9 \begin{bmatrix} 23 & 56 & -152 \\ -50 & -26 & 123 \\ 43 & -7 & 19 \end{bmatrix} (\bmod 26) = \begin{bmatrix} 207 & 504 & -1368 \\ -450 & -234 & 1107 \\ 387 & -63 & 171 \end{bmatrix} (\bmod 26)$$

$$m^{-1} = \begin{bmatrix} 25 & 10 & 10 \\ 18 & 0 & 15 \\ 23 & 15 & 15 \end{bmatrix}$$

$$K = C \times m^{-1} = \begin{bmatrix} 17 & 14 & 8 \\ 20 & 19 & 5 \\ 15 & 4 & 21 \end{bmatrix} \times \begin{bmatrix} 25 & 10 & 10 \\ 18 & 0 & 15 \\ 23 & 15 & 15 \end{bmatrix} = \begin{bmatrix} 17 \cdot 25 + 14 \cdot 18 + 8 \cdot 23 & 17 \cdot 10 + 14 \cdot 0 + 8 \cdot 15 & 17 \cdot 10 + 14 \cdot 15 + 8 \cdot 15 \\ 20 \cdot 25 + 19 \cdot 18 + 5 \cdot 23 & 20 \cdot 10 + 19 \cdot 0 + 5 \cdot 15 & 20 \cdot 10 + 19 \cdot 15 + 5 \cdot 15 \\ 15 \cdot 25 + 4 \cdot 18 + 21 \cdot 23 & 15 \cdot 10 + 4 \cdot 0 + 21 \cdot 15 & 15 \cdot 10 + 4 \cdot 15 + 21 \cdot 15 \end{bmatrix}$$

$$K = \begin{bmatrix} 861 & 290 & 500 \\ 957 & 275 & 560 \\ 930 & 465 & 525 \end{bmatrix} (\bmod 26) = \begin{bmatrix} 3 & 4 & 6 \\ 21 & 15 & 14 \\ 20 & 23 & 5 \end{bmatrix}$$