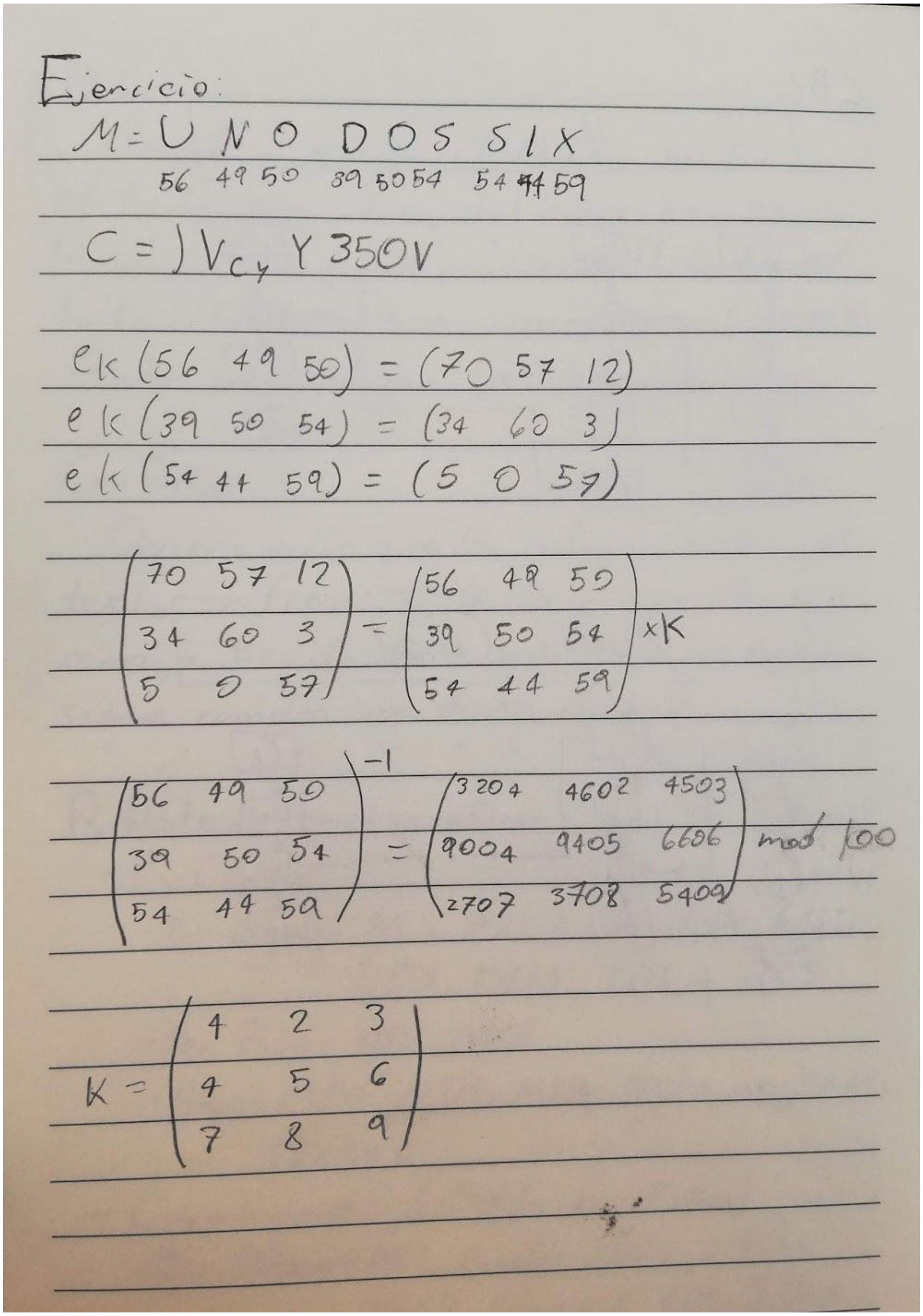


Ejercicio:

M = U N O D O S S I X

56 49 50 39 50 54 54 44 59

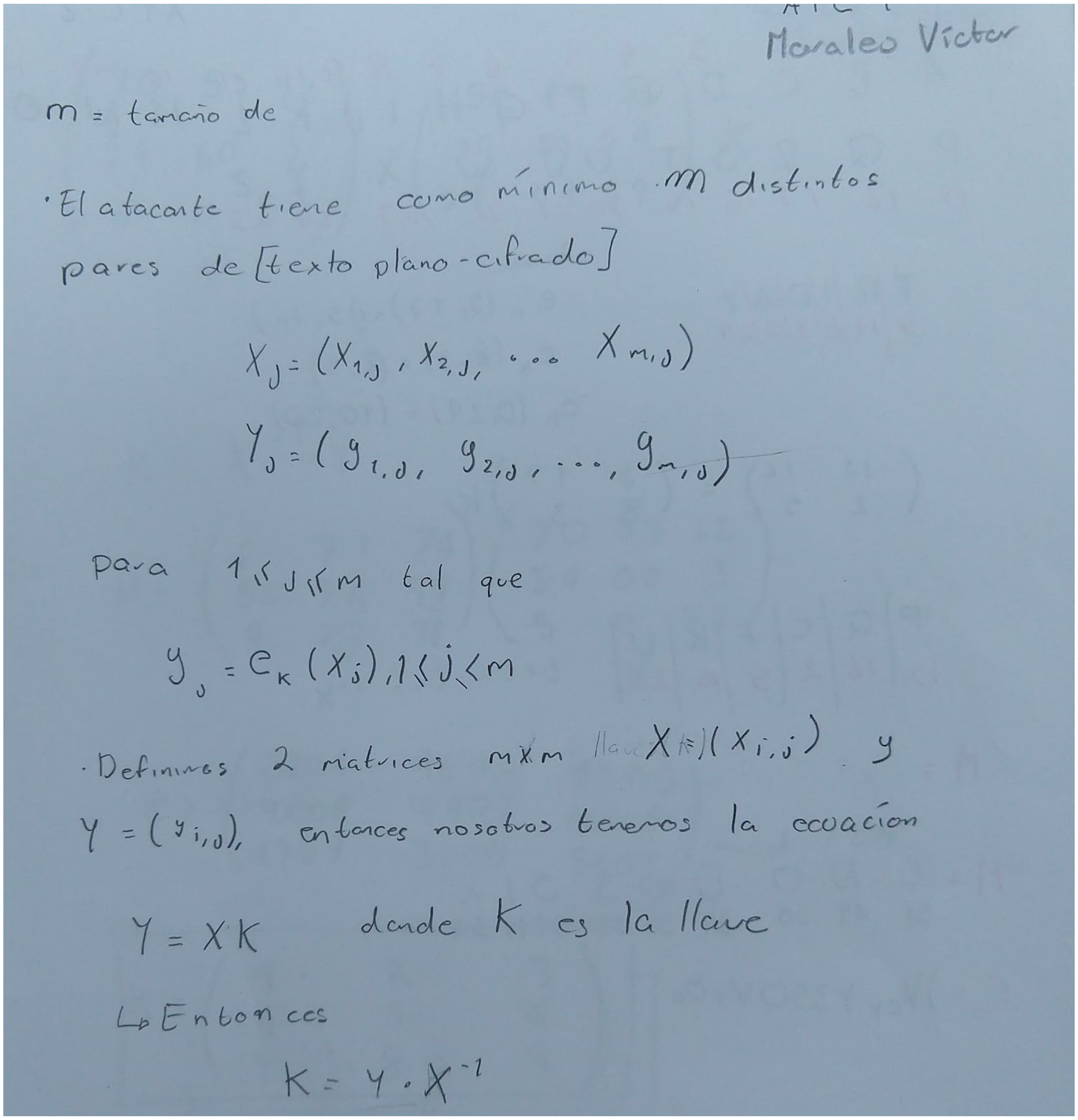
$C =) V_{cy} Y 350V$

$$e_k(56\ 49\ 50) = (70\ 57\ 12)$$
$$e_k(39\ 50\ 54) = (34\ 60\ 3)$$
$$e_k(54\ 44\ 59) = (5\ 0\ 57)$$

$$\begin{pmatrix} 70 & 57 & 12 \\ 34 & 60 & 3 \\ 5 & 0 & 57 \end{pmatrix} = \begin{pmatrix} 56 & 49 & 50 \\ 39 & 50 & 54 \\ 54 & 44 & 59 \end{pmatrix} \times K$$

$$\begin{pmatrix} 56 & 49 & 50 \\ 39 & 50 & 54 \\ 54 & 44 & 59 \end{pmatrix}^{-1} = \begin{pmatrix} 3204 & 4602 & 4503 \\ 9004 & 9405 & 6606 \\ 2707 & 3708 & 5409 \end{pmatrix} \bmod 100$$

$$K = \begin{pmatrix} 4 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$



Moraleo Víctor

m = tamaño de

- El atacante tiene como mínimo m distintos pares de [texto plano - cifrado]

$$X_j = (X_{1,j}, X_{2,j}, \ldots X_{m,j})$$

$$Y_j = (y_{1,j}, y_{2,j}, \ldots, y_{m,j})$$

para $1 \leq j \leq m$ tal que

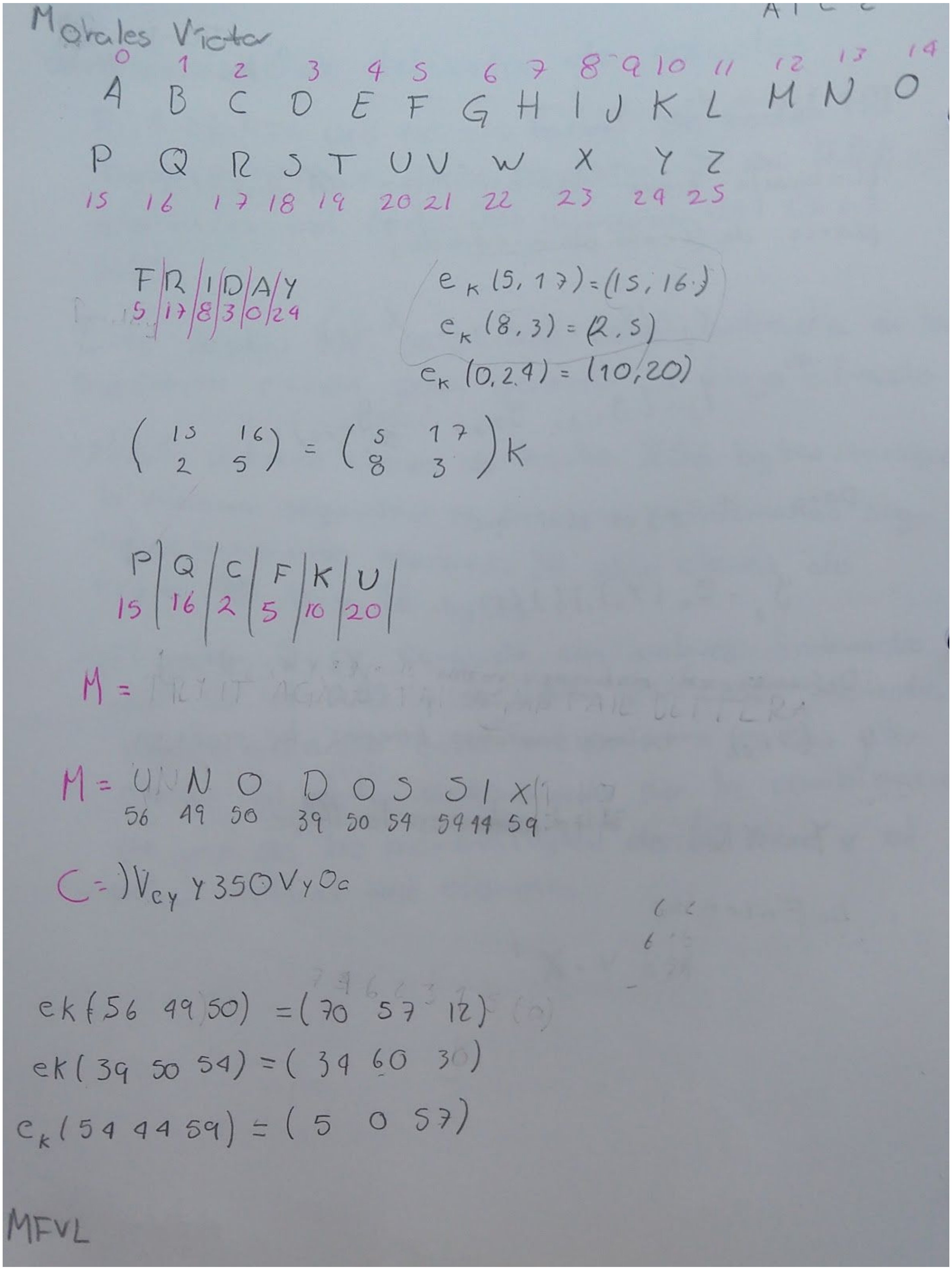
$$y_j = e_K(X_j), 1 \leq j \leq m$$

- Definimos 2 matrices $m \times m$ llave $X =)(x_{i,j})$ y $Y = (y_{i,j})$, entonces nosotros tenemos la ecuación

$$Y = XK$$ donde K es la llave

↳ Entonces

$$K = Y \cdot X^{-1}$$



Morales Victor

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25

F	R	I	D	A	Y
5	17	8	3	0	24

$e_K(5,17)=(15,16)$
$e_K(8,3)=(2,5)$
$e_K(0,24)=(10,20)$

$$\begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix} K$$

P	Q	C	F	K	U
15	16	2	5	10	20

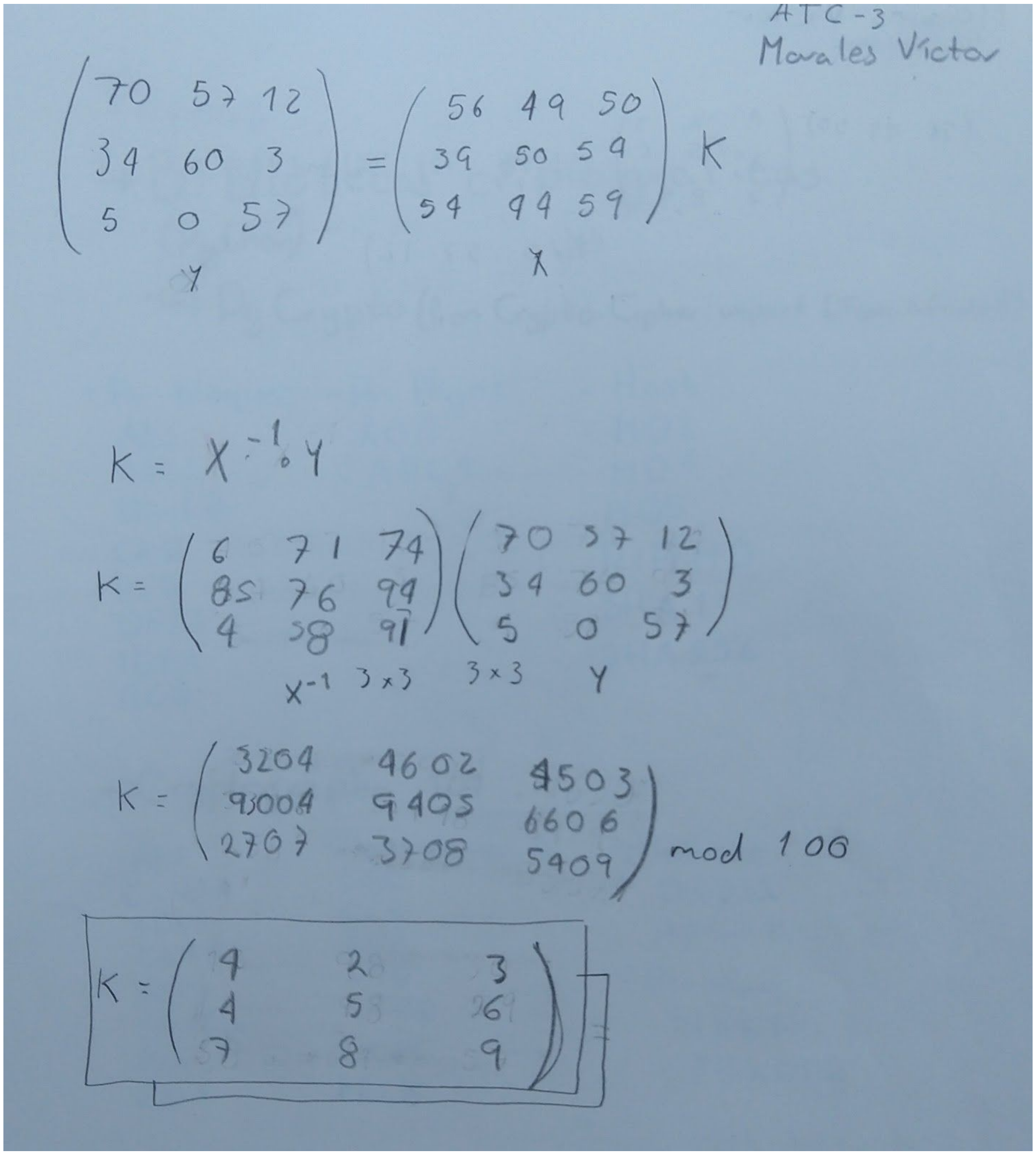
M =

M = UNO DOS SIX
56 49 50 39 50 54 54 44 59

C =)V$_{cy}$ Y 35O V$_{y}$ O$_{c}$

$e_k(56\ 49\ 50) = (70\ 57\ 12)$
$e_k(39\ 50\ 54) = (34\ 60\ 30)$
$e_K(54\ 44\ 59) = (5\ 0\ 57)$

MFVL



ATC-3
Morales Víctor

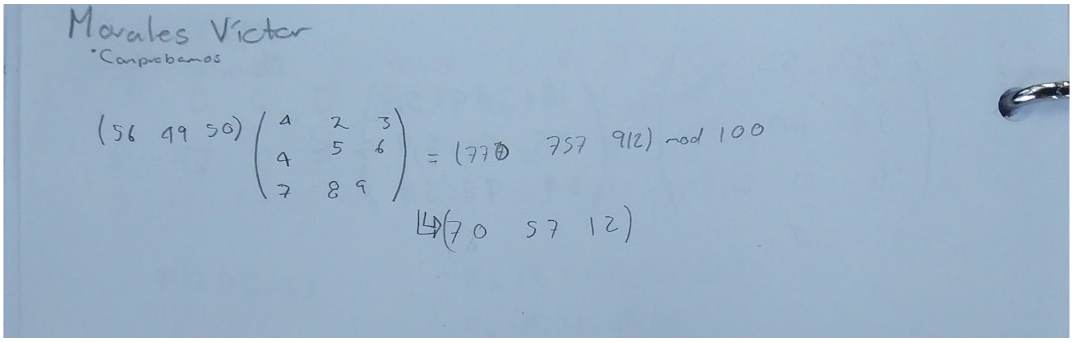
$$\underbrace{\begin{pmatrix} 70 & 57 & 12 \\ 34 & 60 & 3 \\ 5 & 0 & 57 \end{pmatrix}}_{Y} = \underbrace{\begin{pmatrix} 56 & 49 & 50 \\ 39 & 50 & 59 \\ 54 & 44 & 59 \end{pmatrix}}_{X} K$$

$$K = X^{-1} \cdot Y$$

$$K = \underbrace{\begin{pmatrix} 6 & 71 & 74 \\ 85 & 76 & 99 \\ 4 & 58 & 91 \end{pmatrix}}_{X^{-1}\ 3\times 3} \underbrace{\begin{pmatrix} 70 & 57 & 12 \\ 34 & 60 & 3 \\ 5 & 0 & 57 \end{pmatrix}}_{3\times 3\ Y}$$

$$K = \begin{pmatrix} 3204 & 4602 & 4503 \\ 9004 & 9405 & 6606 \\ 2707 & 3708 & 5409 \end{pmatrix} \bmod 100$$

$$\boxed{K = \begin{pmatrix} 4 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}}$$



Morales Víctor
*Comprobamos

$$(56\ 49\ 50)\begin{pmatrix} 4 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} = (770\ \ 757\ \ 912) \bmod 100$$

$$\hookrightarrow (70\ \ 57\ \ 12)$$