INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO
Nombre _Edmundo Josue Sanchez Mendez_

Actividad 7.-Modos de Operación

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix}^{-1} mod\ 256 = \begin{pmatrix} 90 & 167 & 1 \\ 74 & 179 & 254 \\ 177 & 81 & 1 \end{pmatrix}$$

Plainimage

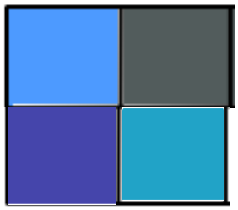
P1			P2		
10	50	9	10	50	9
P3			**P4**		
10	50	9	10	50	9

ECB

C1			C2		
53	95	146	53	95	146
C3			**C4**		
53	95	146	53	95	146

CBC

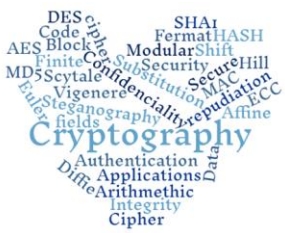
C1			C2		
93	173	255	101	111	111
C3			C4		
69	69	171	33	163	199



Nota: Los procedimientos deben realizarse a mano, debes escanear tus notas y juntarlas con este documento o tomar una foto e incluirla como imagen al final de este archivo.

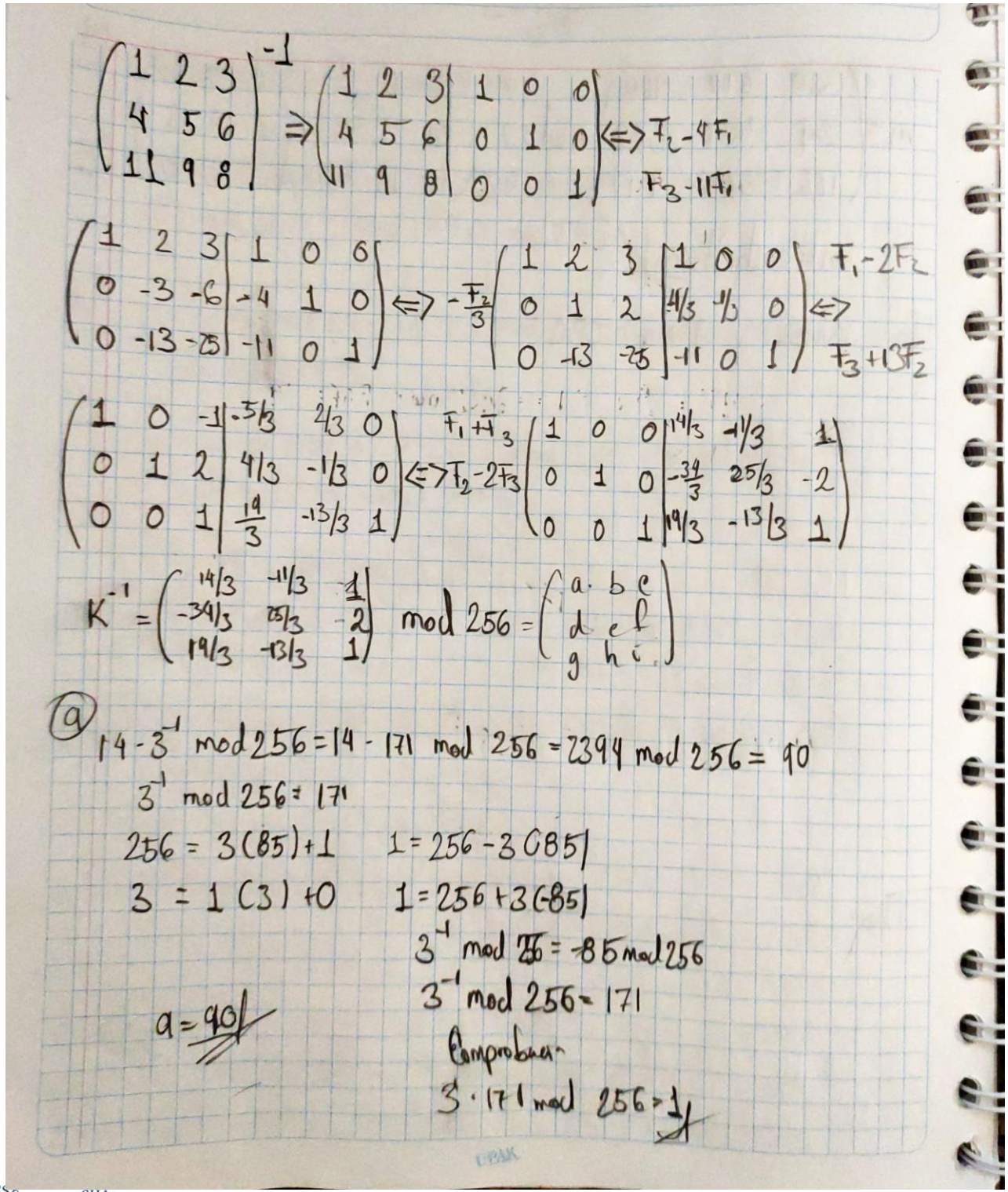
Trabajos sin procedimientos a mano valen 0 puntos.

Al finalizar guarda un sólo archivo como PDF para subirlo a Classroom.



M. en C. Nidia A. Cortez Duarte

Actividad 7.-Modos de Operación



$$\begin{pmatrix}1&2&3\\4&5&6\\11&9&8\end{pmatrix}^{-1} \Rightarrow \left(\begin{array}{ccc|ccc}1&2&3&1&0&0\\4&5&6&0&1&0\\11&9&8&0&0&1\end{array}\right) \Leftrightarrow F_2-4F_1,\ F_3-11F_1$$

$$\left(\begin{array}{ccc|ccc}1&2&3&1&0&0\\0&-3&-6&-4&1&0\\0&-13&-25&-11&0&1\end{array}\right) \Leftrightarrow -\frac{F_2}{3} \left(\begin{array}{ccc|ccc}1&2&3&1&0&0\\0&1&2&4/3&-1/3&0\\0&-13&-25&-11&0&1\end{array}\right) F_1-2F_2 \Leftrightarrow F_3+13F_2$$

$$\left(\begin{array}{ccc|ccc}1&0&-1&-5/3&2/3&0\\0&1&2&4/3&-1/3&0\\0&0&1&\frac{14}{3}&-13/3&1\end{array}\right) F_1+F_3 \Leftrightarrow F_2-2F_3 \left(\begin{array}{ccc|ccc}1&0&0&14/3&-1/3&1\\0&1&0&-34/3&25/3&-2\\0&0&1&14/3&-13/3&1\end{array}\right)$$

$$K^{-1}=\begin{pmatrix}14/3&-11/3&1\\-34/3&25/3&-2\\14/3&-13/3&1\end{pmatrix} \bmod 256 = \begin{pmatrix}a&b&c\\d&e&f\\g&h&i\end{pmatrix}$$

(a) $14 \cdot 3^{-1} \bmod 256 = 14 \cdot 171 \bmod 256 = 2394 \bmod 256 = 90$

$3^{-1} \bmod 256 = 171$

$256 = 3(85)+1 \quad 1 = 256 - 3(85)$

$3 = 1(3)+0 \quad 1 = 256 + 3(-85)$

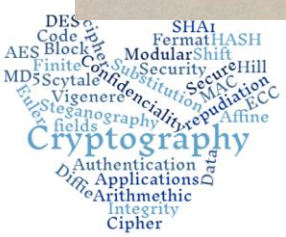
$3^{-1} \bmod 256 = -85 \bmod 256$

$3^{-1} \bmod 256 = 171$

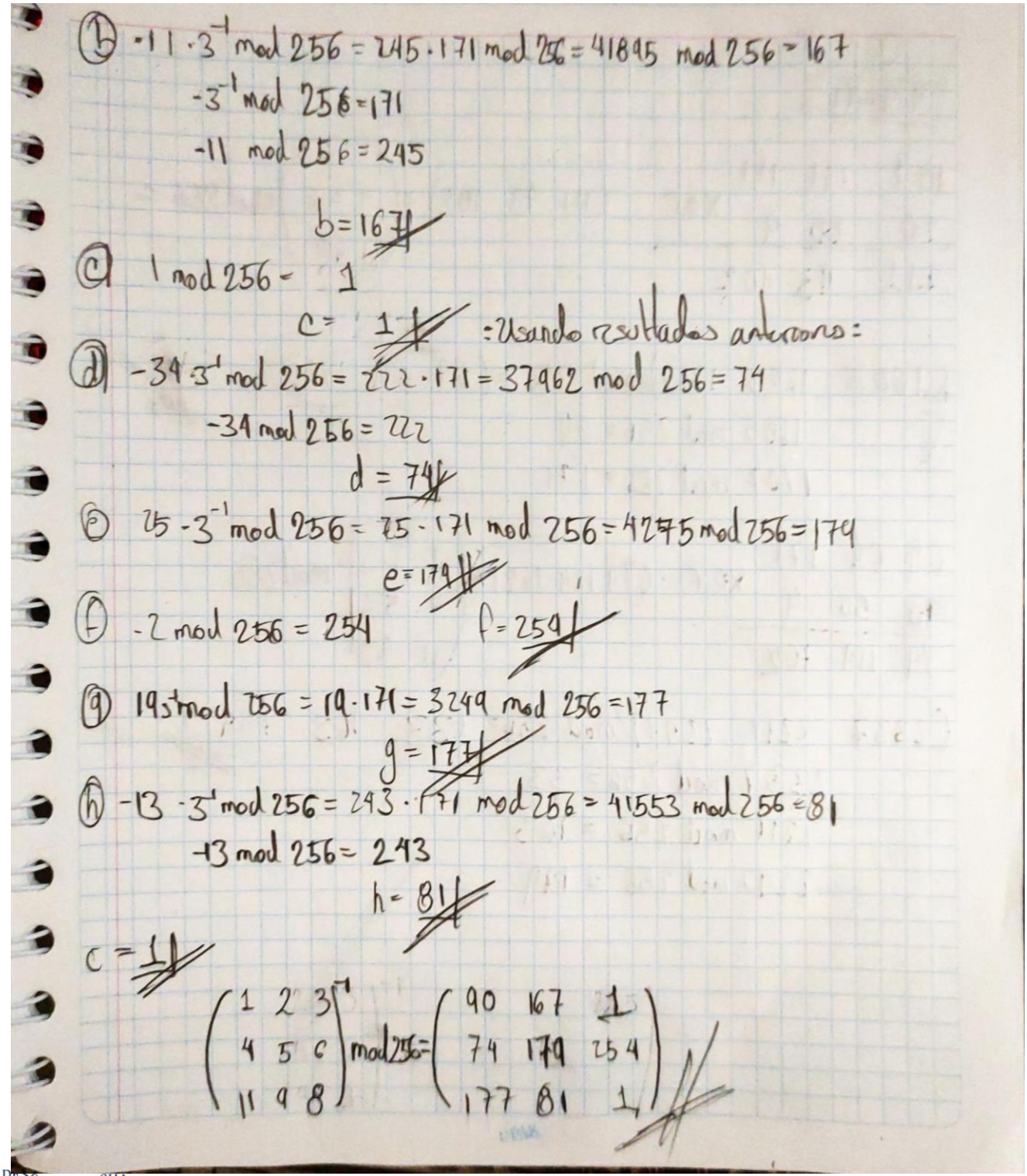
Comprobar

$3 \cdot 171 \bmod 256 = 1$

$a = 90$



Actividad 7.-Modos de Operación



b) $-11 \cdot 3^{-1} \bmod 256 = 245 \cdot 171 \bmod 256 = 41895 \bmod 256 = 167$

$-3^{-1} \bmod 256 = 171$

$-11 \bmod 256 = 245$

$b = 167$

c) $1 \bmod 256 = 1$

$c = 1$: Usando resultados anteriores:

d) $-34 \cdot 3^{-1} \bmod 256 = 222 \cdot 171 = 37962 \bmod 256 = 74$

$-34 \bmod 256 = 222$

$d = 74$

e) $25 \cdot 3^{-1} \bmod 256 = 25 \cdot 171 \bmod 256 = 4275 \bmod 256 = 179$

$e = 179$

f) $-2 \bmod 256 = 254$ $f = 254$

g) $19 \cdot 3^{-1} \bmod 256 = 19 \cdot 171 = 3249 \bmod 256 = 177$

$g = 177$

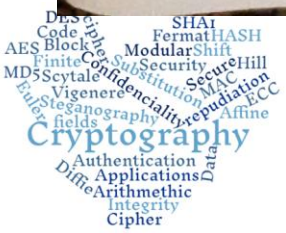
h) $-13 \cdot 3^{-1} \bmod 256 = 243 \cdot 171 \bmod 256 = 41553 \bmod 256 = 81$

$-13 \bmod 256 = 243$

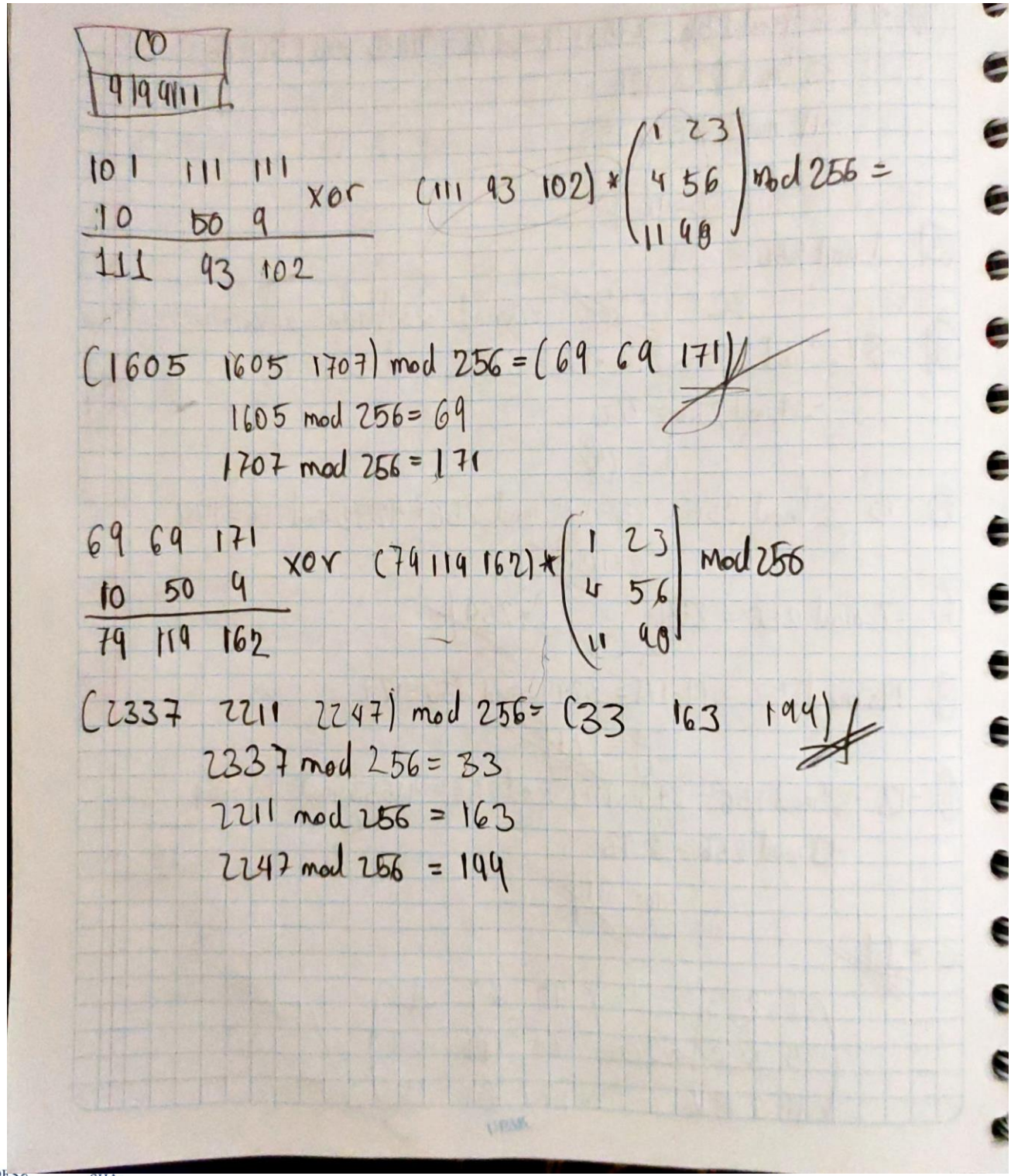
$h = 81$

$c = 1$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix}^{-1} \bmod 256 = \begin{pmatrix} 90 & 167 & 1 \\ 74 & 179 & 254 \\ 177 & 81 & 1 \end{pmatrix}$$



Actividad 7.-Modos de Operación



M. en C. Nidia A. Cortez Duarte