INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE CÓMPUTO

Nombre __Sanchez Mendez Edmundo Josue_____

Actividad 2.-Inverso multiplicativo

Considera el alfabeto en Inglés (26 caracteres)

Ejercicio 2

Encontrar todos los inversos multiplicativos por fuerza bruta.

α	{1	3	5	7	9	11	15	17	19	21	23	25}
α^{-1}	{1	9	21	15	3	19	7	23	11	5	17	25}

Ejercicio 2

Let Encryption function C=7p+5 mod 26

Find the decryption function _____p = 15(C +21) mod 26_____

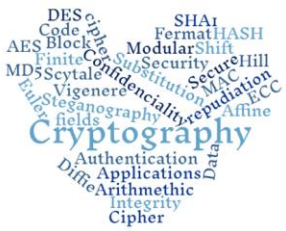
Find the plaintext

Ciphertext	**L**	**F**	**I**	**C**	**H**	**L**	**F**	**I**	**J**	**T**	**B**	**I**	**J**	**L**	**H**
plaintext	**M**	**A**	**T**	**H**	**E**	**M**	**A**	**T**	**I**	**C**	**S**	**T**	**I**	**M**	**E**

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.

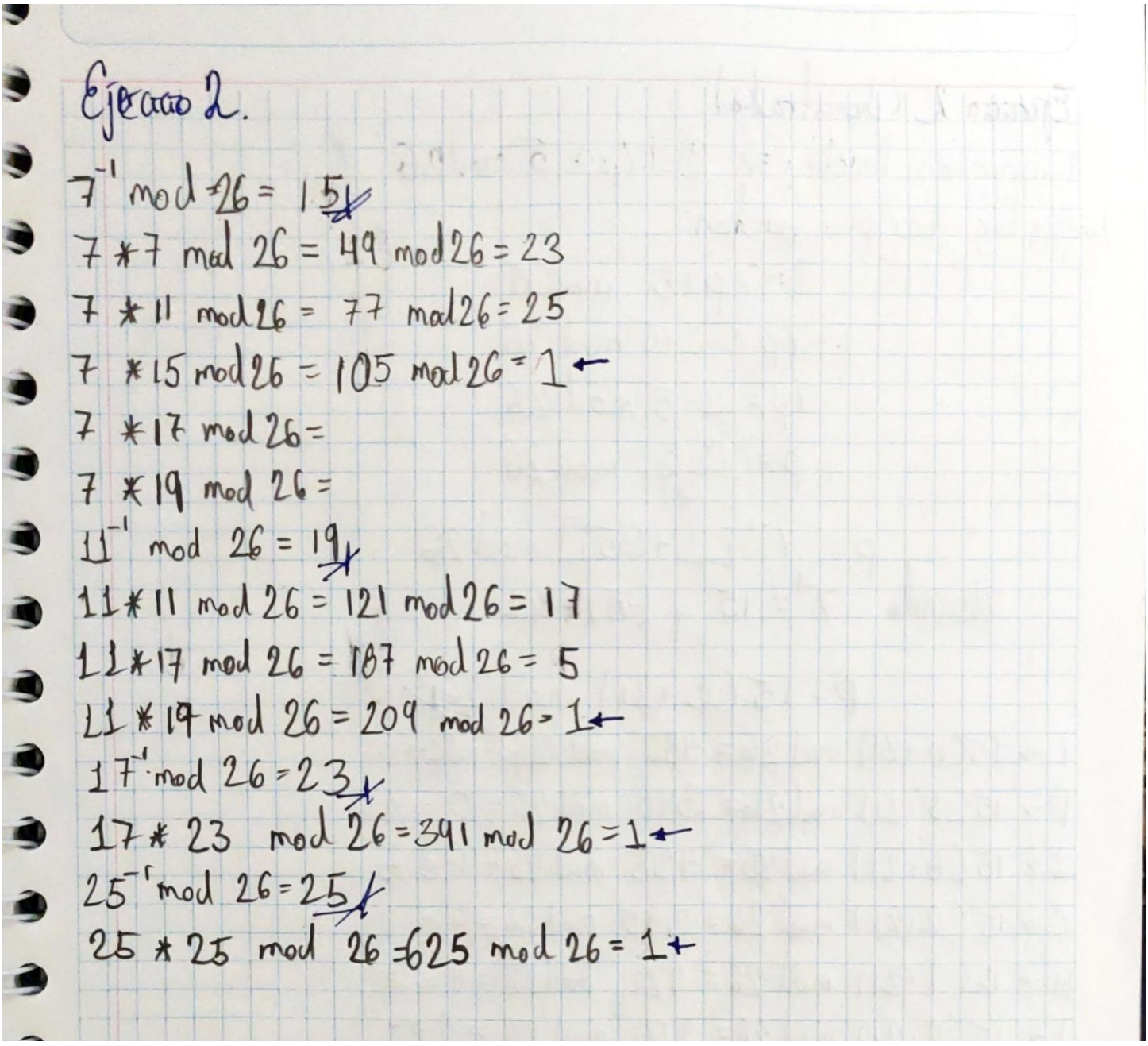
Trabajos sin procedimientos a mano valen 0 puntos.

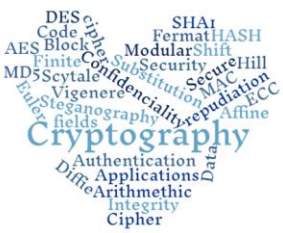
Al finalizar guarda un sólo archivo como PDF para subirlo a Classroom.



M. en C. Nidia A. Cortez Duarte

Actividad 2.-Inverso multiplicativo





M. en C. Nidia A. Cortez Duarte

Actividad 2.-Inverso multiplicativo

Ejercicio 2 (duocatrado)

Encryption function => $C = (7p + 5) \bmod 26$

Looking for decryption function:

$$C = 7p + 5 \bmod 26$$
$$-(-7p = -C + 5) \bmod 26$$
$$7p = C - 5 \bmod 26$$
$$p = \frac{C-5}{7} \bmod 26$$
$$p = 7^{-1}[C + (-5)] \bmod 26$$

Usando $7^{-1} = 15$ y $(-5) = 21$

$$p = 15(C + 21) \bmod 26$$

L → $15(11+21) \bmod 26 = 480 \bmod 26 = 12 \rightarrow m$

F → $15(5+21) \bmod 26 = 340 \bmod 26 = 0 \rightarrow a$

I → $15(8+21) \bmod 26 = 435 \bmod 26 = 19 \rightarrow t$

C → $15(2+21) \bmod 26 = 345 \bmod 26 = 7 \rightarrow H$

H → $15(7+21) \bmod 26 = 420 \bmod 26 = 4 \rightarrow E$

J → $15(9+21) \bmod 26 = 450 \bmod 26 = 8 \rightarrow I$

T → $15(19+21) \bmod 26 = 600 \bmod 26 = 2 \rightarrow c$

B → $15(1+21) \bmod 26 = 330 \bmod 26 = 18 \rightarrow S$