

# **Laboratorio de Criptografía**

**Comunicación de Datos**

**Año 2025**

**Comisión: S31**

**Integrantes:**

**Joaquin Montes - 33459**

**Máximo Carpignano - 32971**

**Ulises Moran - 33339**

## Determinamos la función de encriptado

De la información capturada, se sabe que dada :

- El símbolo **U** (valor 21) fue encriptado como **S** (valor 19).
- El símbolo **T** (valor 20) fue encriptado como **M** (valor 12).

Por lo que dadas las fórmulas detectadas para encriptar encontramos la semilla tal que:

$$Y = aX_0 + B$$

$$Y = aX_1 + B$$

$$\text{Si } X_1 = 19 \wedge X_0 = 21 \rightarrow$$

$$\begin{cases} 20 \text{ MOD } 66 = 21a + B \\ 12 \text{ MOD } 66 = 19a + B \end{cases}$$

$$21a + B - 19a - B = (20 - 12) \text{ MOD } 66$$

$$2a = 8 \text{ MOD } 66$$

$$a = 4 \text{ MOD } 33$$

$$a = 4 + 33k$$

$$\text{CON } k=0 \rightarrow a=4 \text{ SIN EMBARGO } \text{MCD}(4,66) \neq 1$$

$$\text{CON } k=1 \rightarrow a=37 / \text{MCD}(37,66) = 1$$

$$\rightarrow 37 \text{ Y } 66 \text{ SON COPRIMOS}$$

En este caso la semilla  $a$  es 37, ya que para el valor 4 el  $\text{MCD}(4,66)$  es distinto de 1 y por lo tanto no son coprimos, utilizamos  $k = 1$  y ahora  $a=37$  tal que el  $\text{MCD}(37,66) = 1$  y por lo tanto son coprimos.

Ahora nos queda ver cuales de las siguientes fórmulas de encriptación candidatas es la que el **sumergible U-573** estaba utilizando para encriptar su mensaje, por lo que la fórmula con sus valores genéricos  $Y \equiv aX + b \pmod{66}$  nos sirve para reemplazar y encontrar cual es el valor de b.

$$\begin{aligned} Y &= aX + B \pmod{66} \\ 12 &= 37 \cdot 19 + B \pmod{66} \\ -691 &= B \pmod{66} \rightarrow B = -691 \pmod{66} \\ \rightarrow B &= 35 \end{aligned}$$

En este caso  $B=35$ , esto quiere decir que de las siguientes fórmulas candidatas al hacer  $B \pmod{66} = 35$

$$9784562 \pmod{66} = 62 \neq 35$$

$$30018 \pmod{66} = 54 \neq 35$$

$$375839 \pmod{66} = 35$$

Por lo que la fórmula de encriptación utilizada por el **sumergible U-573** es

$$Y = a.X + 375839$$

En base a esta fórmula vamos a descriptar el siguiente mensaje:

.	"	)	7	1	¿	H	T	"	T
¿	¿	E	T	1	¿	]	)	"	¿
1	M	]	Í	-	¿	*	;	Í	G
)	4	Ñ	Í	¿	1	"	¿	1	4
.	;	B	*	]	)	Ñ	Í	¿	¿

C	L	A	V	E		Z	U	L	U
		Q	U	E		T	A	L	
E	S	T	O	Y		P	R	O	B
A	N	D	O		E	L		E	N
C	R	I	P	T	A	D	O		

**Tal que el mensaje de emergencia en limpio es el siguiente:**

“CLAVE ZULÚ QUE TAL ESTOY PROBANDO EL ENCRIPTADO”