

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:

$$Y = \alpha \times + B$$

$$Y = \alpha \times + B$$

$$S1 \times = 191 \times = 21 \Rightarrow$$

$$S2000066 = 210 + B$$

$$1200066 = 190 + B$$

$$210 + 3 - 190 - 8 = (20 - 12)00066$$

$$20 = 800066$$

$$0 = 400033$$

$$0 = 4 + 33k$$

$$CON k = 0 \Rightarrow 0 = 4 SIN EMBARGO MCD (4,66) \neq 1$$

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

 $CON K = 1 \rightarrow Q = 31 / MCD(37,66) = 1$

- 37 Y 66 SON COPRINOS

***UTN** · La Plata

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≡a X+b(mod66) nos sirve para reemplazar y encontrar cual es el valor de b.

$$Y = 0.0066$$
 $12 = 37.19 + BMOD66$
 $-691 = BMOD66 - B = -691 MOD66$
 $-3 B = 35$

En este caso B=35, esto quiere decir que de las siguientes fórmulas candidatas al hacer BMOD(66)=35

$$9784562 \, MoD66 = 62 \neq 35$$

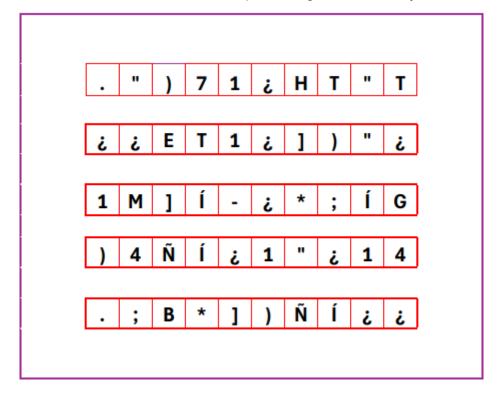
 $30018 \, MoD66 = 54 \neq 35$
 $375839 \, MoD66 = 35$

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

$$\mathbf{Y} = \mathbf{a}.\mathbf{X} + 375839$$

XUTN · La Plata

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



С	L	А	V	Е		Z	U	L	U
					_				
		Q	J	Е		Т	Α	L	
Е	S	Т	0	Y		Р	R	0	В
Α	N	D	0		E	L		E	N
С	R	Ι	Р	Т	Α	D	0		

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

"CLAVE ZULÚ QUE TAL ESTOY PROBANDO EL ENCRIPTADO"