Criptografía Clásica

Ismael Macareno Chouikh

2024-10-14

Índice

1. Instrucciones

1. Busca información sobre el cifrado de **Polybios** y el cifrado de **César**. Mira enlace a criptografía clásica
2. El compañero que te corrija deberá poder descifrar el mensaje cifrado mediante el **cifrado de Polybios**. El mensaje deberá incluir una pregunta que el compañero deberá contestarle. Así podréis comprobar si el proceso ha funcionado correctamente.
3. Cifra mediante el cifrado de **César** el siguiente mensaje: "Los alumnos de ASIR2 saben cifrar información". Recuerda dar una pista con el nº de movimientos
4. Cifra mediante Vigenére el mensaje: ."Esto se va a encriptar". **No olvides dar la CLAVE** (o una pista)

NOTA: Indica en la documentación de la práctica a que compañero le has enviado el mensaje y que compañero te ha enviado el mensaje a ti.

Recuerda que puedesa usar las páginas de:

- Cyberchef
- Dcode
- EduScapeRoom
- Cryptii

2. Información sobre el cifrado Polybios y el cifrado César

2.1. Polybios

Es un sistema el cuál coloca las letras del alfabeto en una red cuadrada de 5x5. El sistema de cifrado consistía en hacer corresponder a cada letra del alfabeto un par de letras que indicaban la fila y la columna, en la cual aquella se encontraba.

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	I, J	K
C	L	M	N, Ñ	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

Tablero de Polibio

Si en el tablero de Polybios, introduciomos números, resulta una variante sumamente interesante:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I, J	K
3	L	M	N, Ñ	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

2.2. César

Es uno de los algoritmos criptrográficos más simples. Es un algoritmo de sustitución, su cifrado consistía simplemente en sustituir una letra por la situada tres lugares más allá en el alfabeto esto es la A se transformaba en D, la B en E y así sucesivamente hasta que la Z se convertía en C.

Alfabeto original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto cifrado	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

3. Mensaje cifrado mediante Polybios

El mensaje cifrado mediante Polybios es **AEDCCEAACCBDDDAA**.

La pista que porporciono está en nuestro **país**.

4. Mensaje cifrado mediante César

El mensaje a cifrar es **Los alumnos de ASIR2 saben cifrar información**.

El cifrado es: Svz hsbtuvz kl HZPY2 zhilu jpmyhy pumvythjpóu

La pista del número de salto es mi nombre+1.

5. Cifrado mediante *Vigenére*

El mensaje a cifrar es **Esto se va a encriptar**.

El mensaje cifrado es: Ekbf sw dr a wvtraxkaj

La *key* es **asir**