te lo cuenta la criptografía

te lo cuenta una espía

Taller manipulativo

Contenidos para el profesorado

te lo cuenta la criptografía

Criptografía

- La ***criptografía*** es la ciencia que estudia las técnicas de cifrado de mensajes con la finalidad de hacerlos solamente comprensibles para los receptores autorizados.
- En contraposición a la criptografía, el ***criptoanálisis***, estudia los cifrados con el objetivo de romper su seguridad y permitir que los mensajes puedan ser descifrados por receptores no autorizados.

te lo cuenta la criptografía

El cifrado del César

- Es uno de los primeros sistemas de cifrado.
- Julio César observaba como sus mensajeros eran interceptados constantemente por sus enemigos y estos podían descubrir las instrucciones militares.
- Decidió enviar sus mensajes cifrados mediante la sustitución de cada letra del mensaje original por la que está situada 3 posiciones después.

te lo cuenta la criptografía

El cifrado del César: ejemplo

S → V

O → R

L → Ñ

D → G

A → D

D → G

O → R

te lo cuenta la criptografía

Clave del César: 3

A	B	C	D	E	F	G	H	I	J	K	L	M	N
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P

Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Patrocina Consello Social Universidade de Vigo
Organiza MaReMa
Con la colaboración de Universidade Vigo

te lo cuenta la criptografía

Descifrado con cifrado César: ejemplo

V → S

R → O

Ñ → L

G → D

D → A

G → D

R → O

te lo cuenta la criptografía

Cifrados de sustitución

Los ***cifrados de sustitución*** son aquellos en los que los mensajes se dividen en unidades más pequeñas, por ejemplo letras. Estas se sustituyen por otras unidades siguiendo un patrón (por ejemplo, una clave) conocido por el emisor y el receptor con las siguientes características:

- Sencillo para poder cifrar y descifrar rápidamente.
- Fácil de transmitir para evitar riesgos.

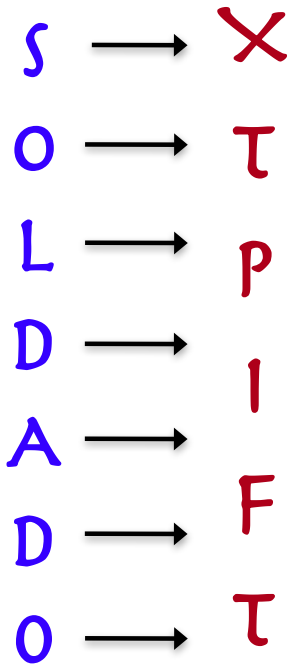
te lo cuenta la criptografía

Claves

- *Una **clave*** es cierta información (puede ser una palabra, un número…), conocida solamente por emisor y receptor, ya que permite cifrar y descifrar cualquier mensaje.
- En el cifrado César la clave es el número 3, el número que indica el desplazamiento del alfabeto utilizado.
- Cambiando la clave 3 otro número del 1 al 26, obtenemos otro cifrado de sustitución distinto.

te lo cuenta la criptografía

Cifrado con clave 5: ejemplo



te lo cuenta la criptografía

Cifrado de sustitución polialfabético

- En un ***cifrado de sustitución polialfabético*** una misma letra en dos posiciones diferentes puede dar lugar a dos letras distintas en el mensaje cifrado.
- Son cifrados que proporcionan una mayor seguridad que el de César.
- Leon Battista Alberti publicó en *De Cifris* (1466) el primer sistema de cifrado de sustitución polialfabético que se conoce.

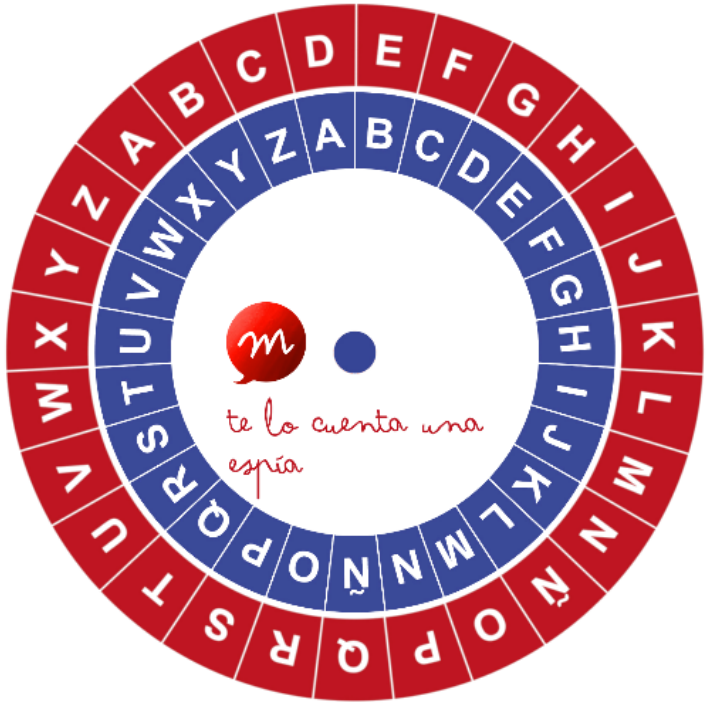
te lo cuenta la criptografía

Disco de Alberti

- Es un artilugio que permite cifrar y descifrar con sustitución polialfabética.
- Consiste en dos discos ensamblados que giran uno sobre otro. Según el cifrado y descifrado propuestos se hacían varios giros en el proceso.

te lo cuenta la criptografía

Máquina de cifrado



Patrocina
Consello Social Universidade de Vigo
Organiza
MaReMa
Con la colaboración de
Universidade Vigo

te lo cuenta la criptografía

Objetivos del taller

Se pretende que el alumnado comprenda la implicación de las matemáticas en el cifrado y descifrado de mensajes, realizando en primera persona dicho cifrado y descifrado y protagonizando personalmente los roles implicados en una comunicación cifrada: emisor, interceptor y receptor.

te lo cuenta la criptografía

Material necesario para el taller

- Material escolar básico: folios, bolígrafos azul y rojo, tijera.
- Material específico


Comunicación cifrada

Cifrando un mensaje para el soldado

Personaje:	César	Clave:
Mensaje original		
Mensaje cifrado		

Descifrando el mensaje interceptado

Personaje:	Guerrera celta	Clave:
Mensaje cifrado		
Mensaje original		

Descifrando el mensaje del César

Personaje:	Soldado	Clave:
Mensaje cifrado		
Mensaje original		

Cifrado/descifrado de un mensaje

Personaje:		Clave:
Mensaje original		
Mensaje cifrado		

Patrocina Consello Social Universidade de Vigo
Organiza MaReMa
Con la colaboración de Universidade Vigo

te lo cuenta la criptografía

Resultados de aprendizaje

- Cifrar y descifrar mensajes con el cifrado César.
- Emplear métodos deductivos para averiguar el sistema de cifrado utilizado en un mensaje.
- Construir una máquina de cifrado y descifrado.
- Identificar los protagonistas de una comunicación cifrada.
- Comprender el papel de la clave en la comunicación cifrada.
- Crear distintos cifrados de sustitución con distintas claves.
- Cifrar y descifrar con distintos sistemas de sustitución.
- Hallar la clave del cifrado de sustitución conociendo parte del mensaje original.
- Comprender la implicación de las matemáticas en comunicaciones secretas.

te lo cuenta la criptografía

Temporalización y secuenciación

- 90 min
- El origen de la clave del César
- Ejemplo de cifrado y descifrado
- Construcción de la máquina de cifrado y juego de roles
- Para profundizar en los cifrados de sustitución
- Reto

te lo cuentan las matemáticas

Patrocina

Consello Social
Universidade de Vigo

Organiza

MaReMa

Con la colaboración de

Universidade Vigo