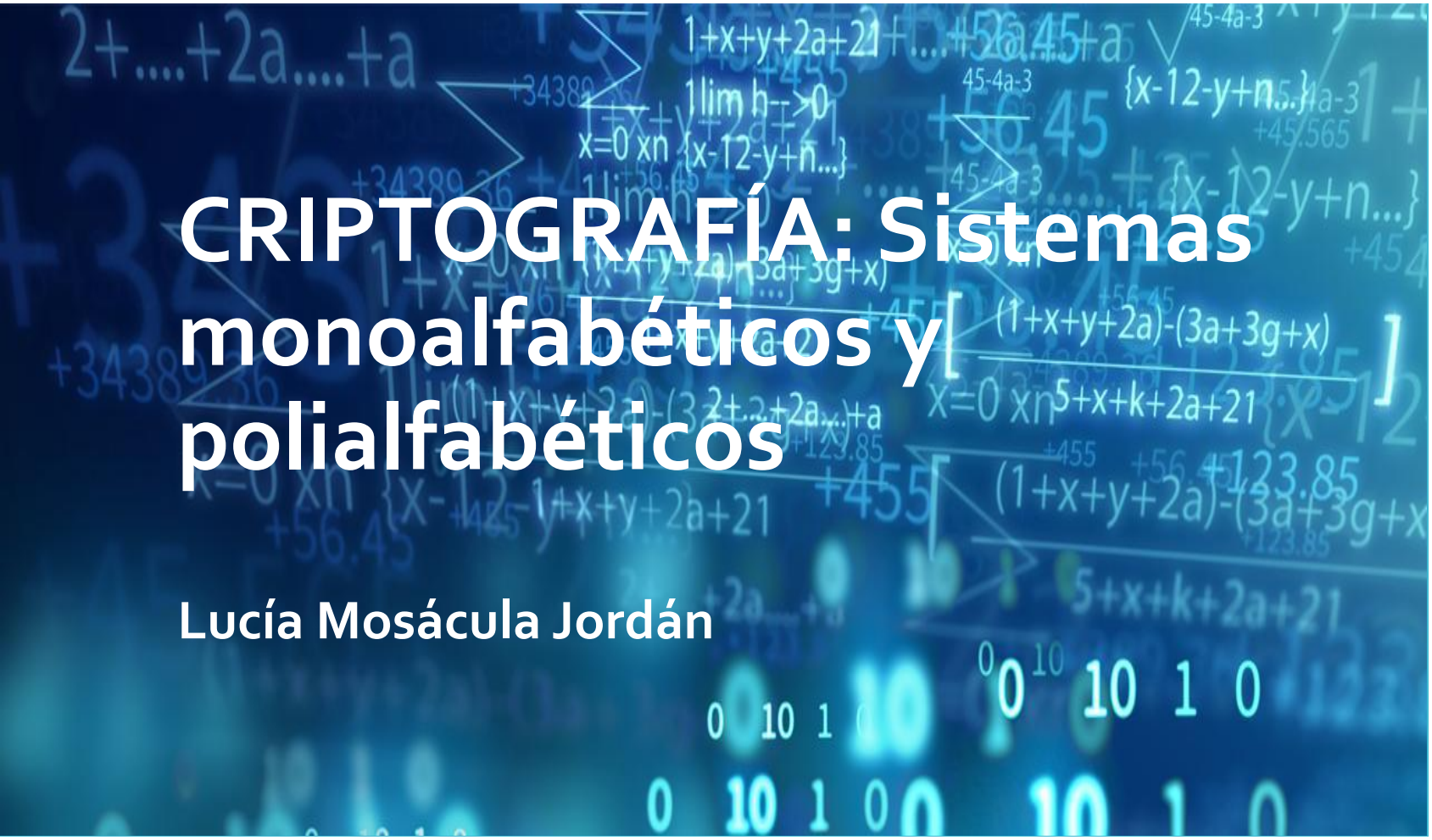


CRIPTOGRAFÍA: Sistemas monoalfabéticos y polialfabéticos

Lucía Mosácula Jordán

Junta de Castilla y León

Universidad de Valladolid

IES Andrés Laguna

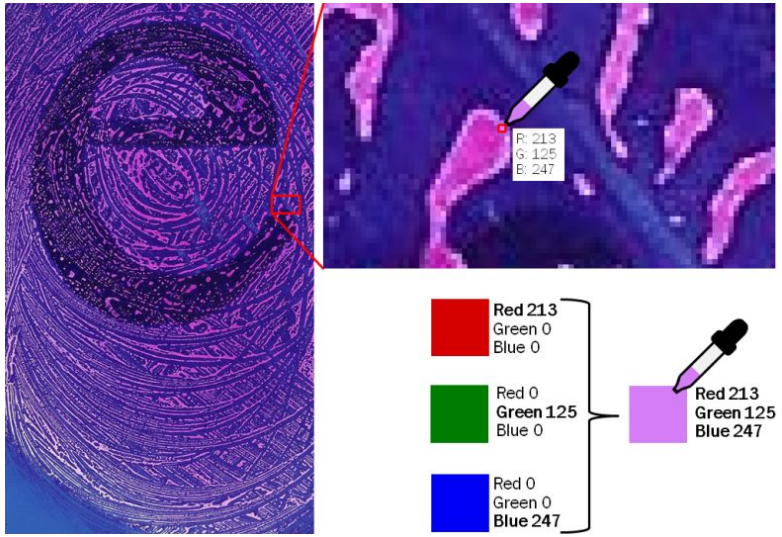
Índice

Conceptos básicos

- **Esteganografía:** Es el arte o la técnica de ocultar mensajes dentro de otros o de objetos sin cifrarles.

- **Criptografía:** Es la técnica de ocultar información para conseguir la confidencialidad cifrando el mensaje.

- **Clave:** Secuencia de números o letras que especifica la transformación del texto plano en texto cifrado, o viceversa.

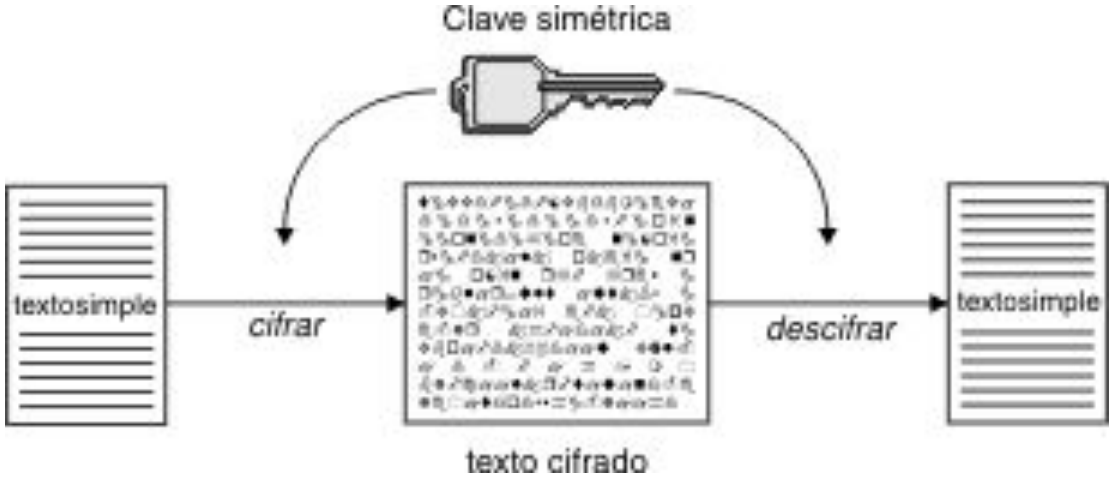


PCQ VMJiPD LhiK LiSe KhahJaWaV haV ZCJPe EiPD KhahJiUaJ LhJee KCPK. CP Lhe LhCMKaPV aPV liJKL PiDhL, QheP Khe haV ePVeV Lhe LaRe CI Sa'aJMI, Khe JCKe aPV EiKKev Lhe DJCMPV ZelCJe hiS, KaUiPD: 'DJeaL EiPD, ICJ a LhCMKaPV aPV CPe PiDhLK i haNe ZeeP JeACMPLiPD LC UCM Lhe laZReK CI FaKL aDeK aPV Lhe ReDePVK CI aPAiePL EiPDK. SaU i SaEe KC ZCRV aK LC AJaNe a IaNCMJ CI UCMJ SaGeKLU?'

eFiRCDMe, LaReK IJCS Lhe LhCMKaPV aPV CPe PiDhLK

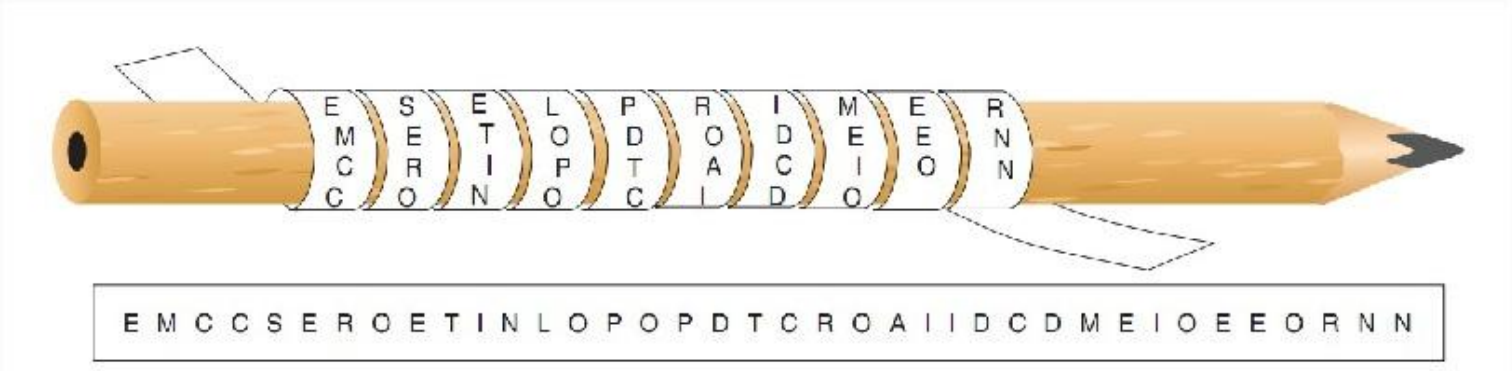
Conceptos básicos

- **Criptoanálisis:** Se encarga de descifrar mensajes sin conocer la clave pero si el método de cifrado.
- **Fuerza bruta:** Método básico de criptoanálisis que descifra un texto probando todas la claves posibles del método con el que se cifró.
- **Análisis de frecuencia:** Método de criptoanálisis que utiliza la frecuencia de las letras del idioma para descifrar un mensaje.



Sistemas cifrados por permutación

- Consiste en intercambiar el orden de las letras de un mensaje según un esquema definido.
- ESCÍTALA
- La clave es el diámetro del tubo.



Pasos para descifrar un mensaje por el Escítala:

- Se va a utilizar el ataque por fuerza bruta colocando las letras en una tabla según la fórmula: $n = q \times c - r$

  "n" el número de letras del mensaje

  "q" el número de filas de la tabla = diámetro de la vara,

  "c" el número de columnas de la tabla = vueltas que da la cinta alrededor de la vara

  "r" el número de casillas de la tabla que sobran.

- El mensaje cifrado es: AVANEDAERVNIIMD

- Se prueba con c=3

  $15 = q \times 3 - r$

  q=5 y r=0

A	D	N
V	A	I
A	E	I
N	R	M
E	V	D

- Se prueba con c=4

  $15 = q \times 4 - r$

  q=4 y r=1

A	E	R	I
V	D	V	M
A	A	N	D
N	E	I	

- Se prueba con c=5

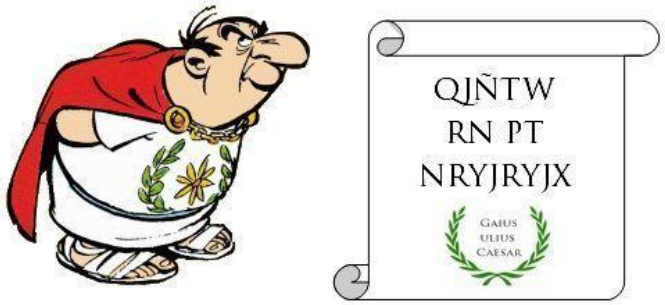
  $15 = q \times 5 - r$

  q=3 y r=0

A	N	A	V	I
V	E	E	N	M
A	D	R	I	D

Sistemas de cifrado por sustitución monoalfabética

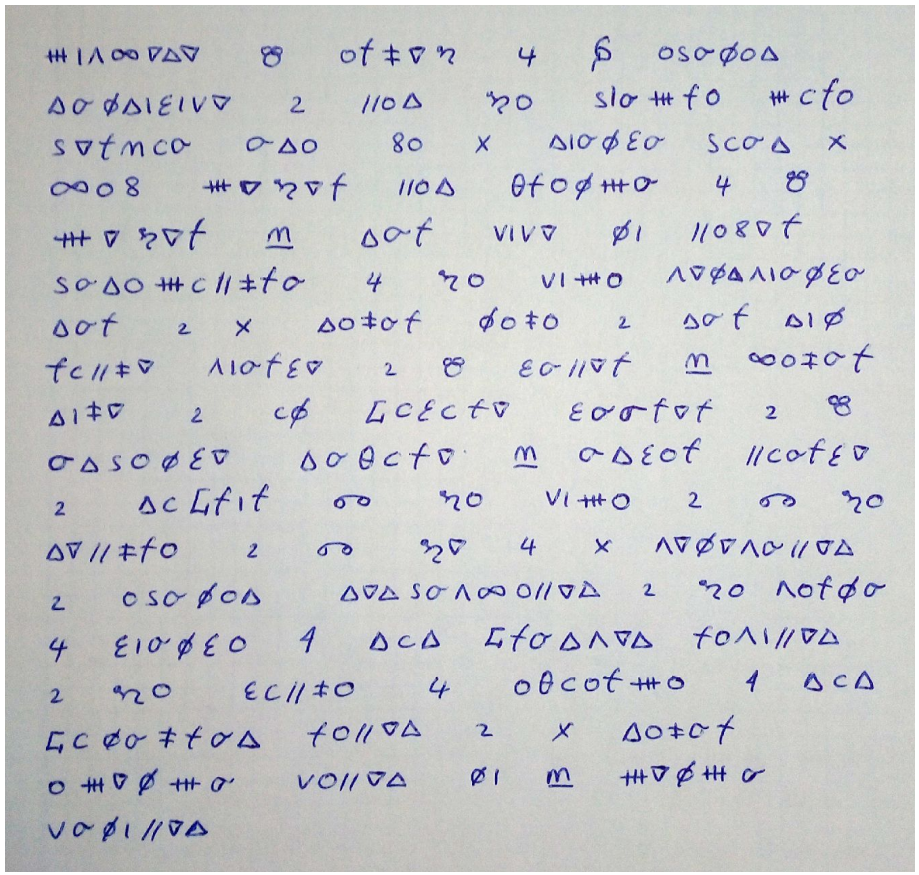
- Consiste en reemplazar cada letra del mensaje por otra letra, número o símbolo siguiendo una clave determinada y siempre de la misma forma.



	A	D	F	G	V	X
A	O	1	S	E	G	F
D	2	0	H	A	Y	D
F	R	B	Z	P	4	N
G	Q	9	8	C	T	K
V	3	X	I	7	5	W
X	J	U	6	M	V	L

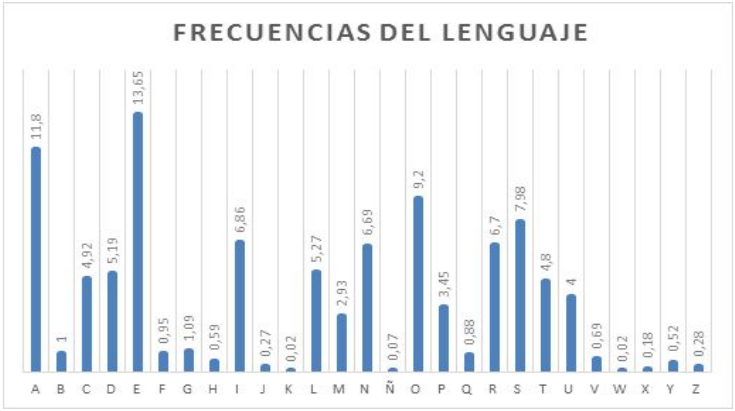
Cifrado de María Estuardo

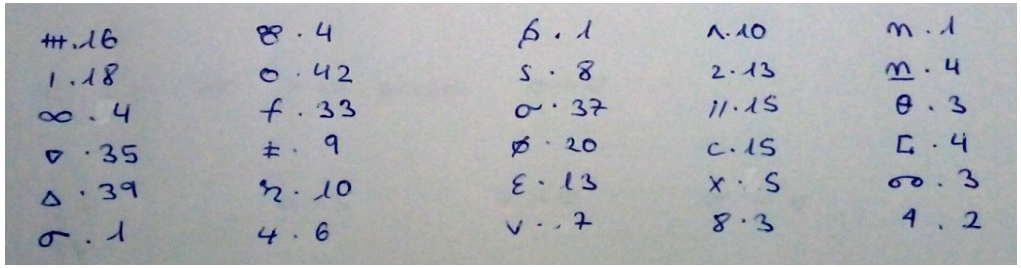
- María Estuardo, reina de Escocia de 1542 a 1567.
- Fue producto de una conspiración entre Babington y María para asesinar a su prima Isabel I, liberar a María de la prisión y conseguir el trono británico.
- Gracias al trabajo de criptoanalistas detuvieron el complot y María Estuardo terminó ejecutada.
- La clave es:



Pasos para descifrar un texto de cifrado monoalfabético:

- Contar las repeticiones de cada símbolo.
- Seguir el análisis de frecuencia.
- Tener cuidado con los símbolos que cifran una palabra.





Sistemas de cifrado por sustitución polialfabética

- Consiste en reemplazar una letra del mensaje por otra del alfabeto que no siempre es la misma.
- El primer sistema polialfabético es el cifrado de Alberti.
- La máquina Enigma permite cifrar mensajes por sustitución polialfabética mediante la mecanización. Gracias a Alan Turing se permitió descifrar los mensajes alemanes y poner fin a la Segunda Guerra Mundial.

Cifrado de Vigenère

- Ha evolucionado de la tabla de Trithemius y es anterior a Enigma. De 1553.
- La clave es una palabra que indica el alfabeto con el que se cifra cada letra del mensaje.
- Para desencriptarle se utiliza el análisis de frecuencia con modificaciones.

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

Pasos para descifrar un texto de cifrado polialfabético:

- Buscar grupos de 3 letras que se repitan y calcular el número de posiciones de diferencia.

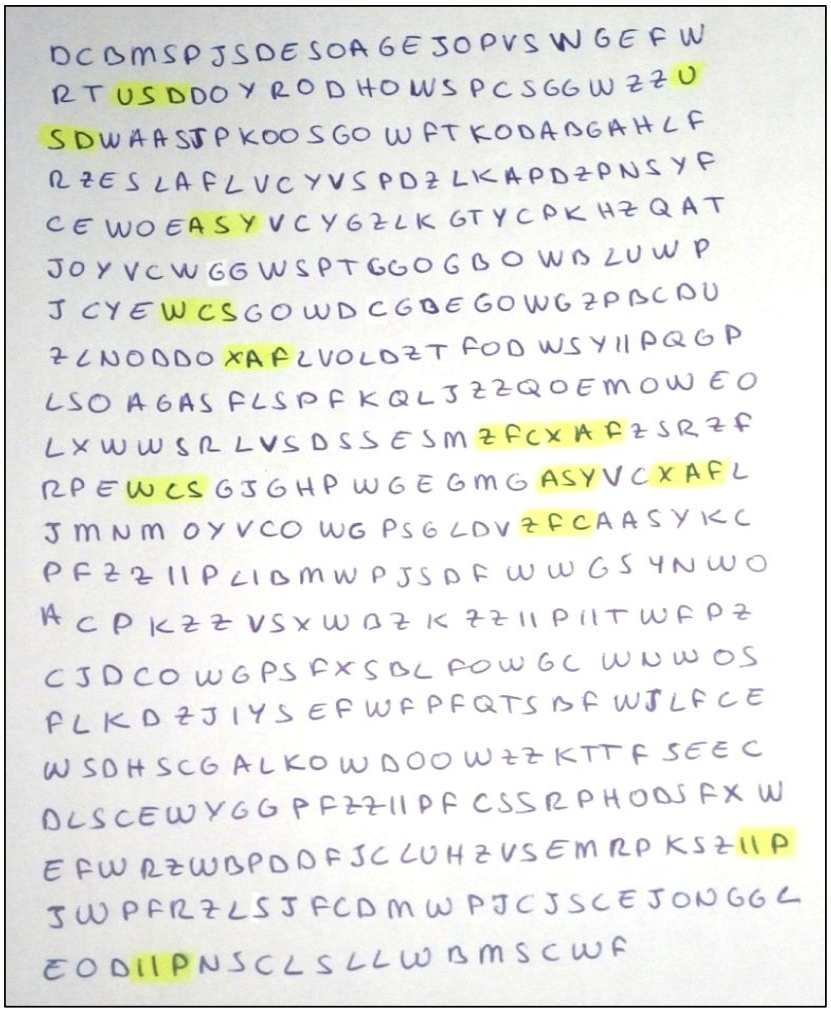
  USD: 21 ASY: 168 WCS: 105

- Calcular el MCD para averiguar la longitud de la clave.

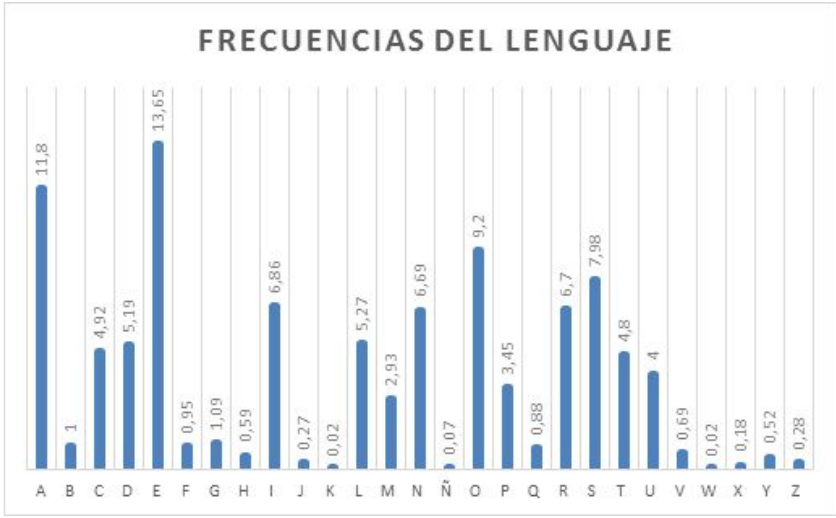
  21 = 3x7 168 = 2^3x3x7 105 = 3x5x7

- Como la longitud de la clave es de 3 letras, calcular la repetición de cada letra según dicho intervalo.

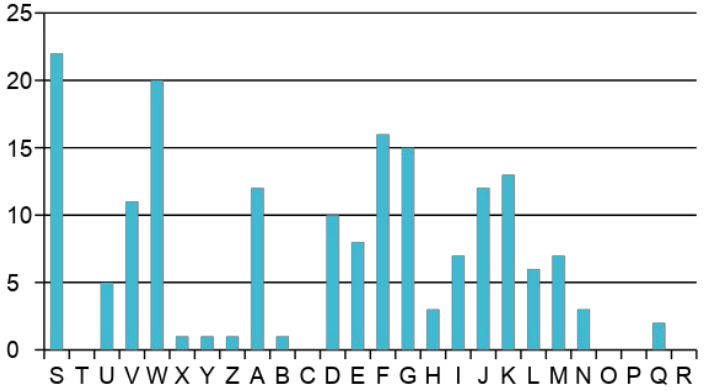
  Clave: L1-L2-L3



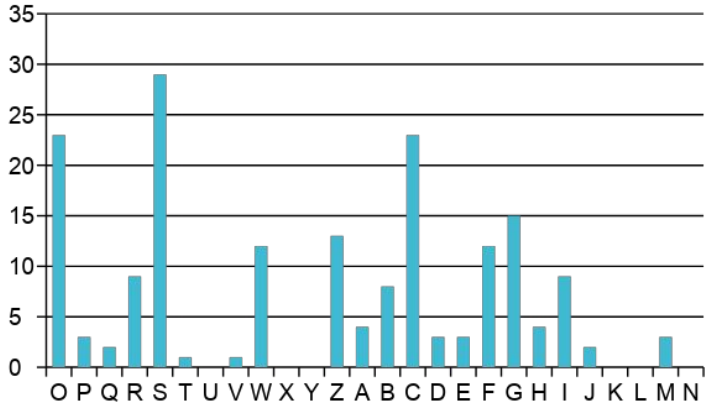
- Comparar gráficamente los datos obtenidos con una gráfica de frecuencias para averiguar la clave.
- Invertir el cifrado de Vigenère según la clave obtenida.



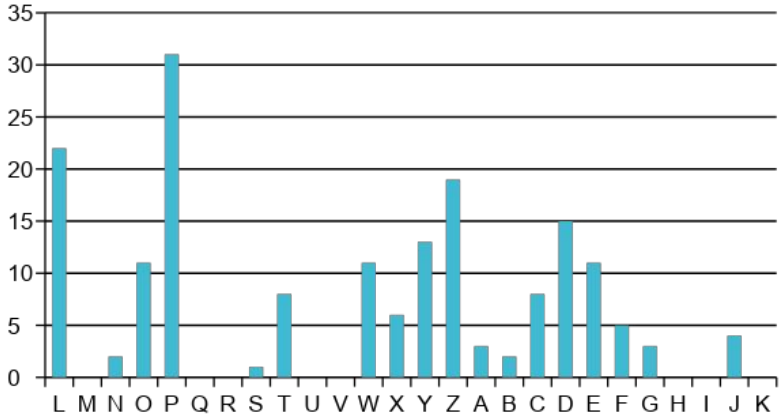
L1 = S



L2 = O



L3 = L



Sistemas de cifrado en la actualidad

- Gracias a la aparición de la informática, los sistemas de cifrado han evolucionado y son más seguros gracias a la utilización de funciones matemáticas y algoritmos.
- Destacan el DES (Data Encryption Standard), el AES (Advanced Encryption Standard) y el RSA (Rivest, Shamir y Adleman).

Conclusión

- La criptografía ha evolucionado a lo largo de la historia gracias a la necesidad del ser humano de proteger su información.
- Los métodos de cifrado han ido variando y haciéndose más seguros según se iban desvelando las debilidades de los métodos anteriores.
- En la actualidad, gracias a los ordenadores se pueden conseguir nuevos sistemas de cifrado basados en funciones matemáticas.

Agradecimientos

- Ángela Isabel Barbero Díez
- Gema Galbarte Hernández

Junta de Castilla y León

Universidad de Valladolid

IES Andrés Laguna