¿Qué es la criptografía?

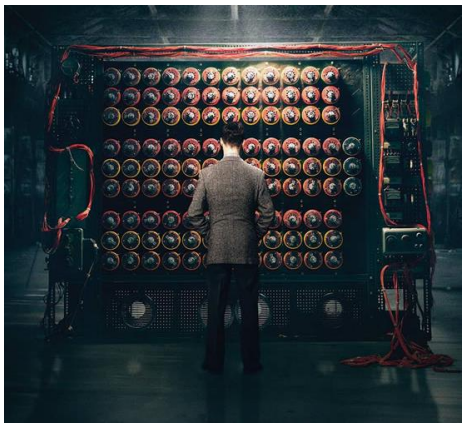
Según la RAE:

Criptografía: Arte de escribir con clave secreta o de un modo enigmático.

La criptografía es la creación de técnicas para el cifrado de datos.

Teniendo como objetivo conseguir la confidencialidad de los mensajes. Si la criptografía es la creación de mecanismos para cifrar datos, el ***criptoanálisis*** son los métodos para "romper" estos mecanismos y obtener la información. Una vez que nuestros datos han pasado un proceso criptográfico decimos que la información se encuentra ***cifrada***.

Los primeros sistemas de cifrado estuvieron ligados a campañas militares, dada la necesidad de evitar que el enemigo obtuviese los movimientos de las tropas al interceptar mensajes.



Enigma era el nombre de una máquina de rotores que permitía usarla tanto para cifrar como para descifrar mensajes.

Criptex es un artilugio de forma cilíndrica, usado para ocultar secretos en su interior.

¿Por qué es necesaria la criptografía?

¿Por qué se hizo necesaria para el resto de la gente?

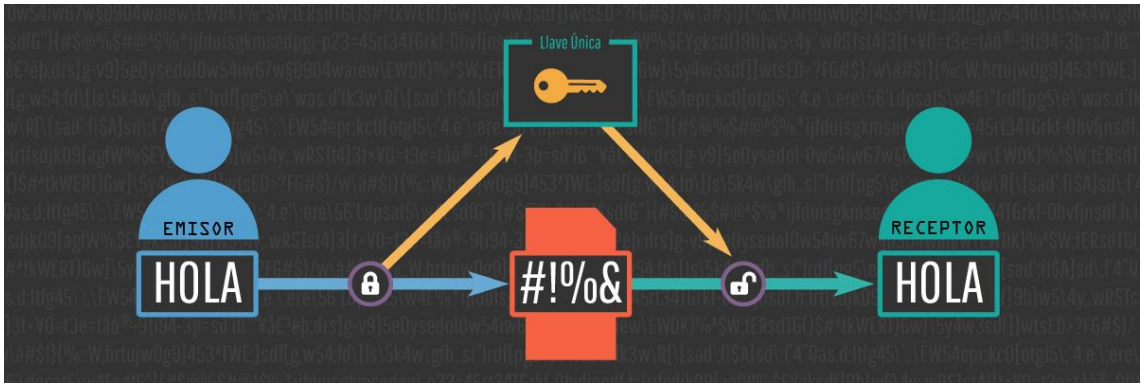
Aunque el uso de comunicaciones seguras ha sido siempre una prioridad militar, la privacidad es requerida en otros sectores. Las empresas necesitan mantener unas comunicaciones seguras para proteger su información.

Aparte de a las empresas, se hace necesario otorgar al ciudadano de privacidad y seguridad. Con el nacimiento de internet y la progresiva oferta de servicios telemáticos como acceso al banco, citas médicas y un sinfín de posibilidades se tiene que ofrecer confidencialidad y seguridad a estos servicios.

Por estas razones es necesaria la criptografía. Para otorgar privacidad, confidencialidad y seguridad a nuestras transacciones telemáticas.

Encriptación o Cifrado de Datos:

Es un procedimiento mediante el cual los archivos, o cualquier tipo de documento, se vuelven completamente ilegibles gracias a un algoritmo que desordena sus componentes. Así, cualquier persona que no disponga de las claves correctas no podrá acceder a la información que contiene.



De esta forma, según la "password", encontramos dos tipos de encriptación de archivos:

- Simétrico: Es aquel que utiliza una misma clave para cifrar y descifrar.
- Asimétrico: En este se usan diferentes claves, una clave pública para cifrar y una de carácter privado para descifrar, de forma que sea imposible deducir la contraseña privada a través de la pública.

Por ejemplo, si queremos que tres compañeros/as nos manden un archivo cifrado, debemos de mandarles nuestra clave pública (que está vinculada a la privada) y nos podrán mandar, de forma confidencial, ese archivo que solo nosotros podremos descifrar con la clave privada.

Aunque pueda parecer que la clave privada pudiese ser descubierta gracias a la pública, no es así. Se utilizan complejos algoritmos para generar las claves, que son muy resistentes a los ataques de los ciberdelincuentes.

Ventajas y desventajas de estos dos tipos de cifrado :

Velocidad:

→ La principal ventaja del cifrado simétrico es que es mucho más rápido y ágil. De modo que, si quieres cifrar una gran cantidad de información, ahorrarás tiempo con este tipo.

→ Por el contrario, el cifrado asimétrico es mucho más lento. Si el rendimiento es un factor clave a tener en cuenta, no es la mejor opción.

Seguridad:

- → El cifrado simétrico no es tan seguro, ya que el hecho de comunicar la clave supone una gran vulnerabilidad. Es muy importante buscar medios seguros para comunicarla.
- → La ventaja del cifrado asimétrico es el hecho de que puede comunicar, de forma segura, claves públicas a terceros. Este tipo, tiene la libertad de entregar la clave pública, mientras la clave privada permanece con el usuario.

Número de claves:

- → La administración de claves también es un beneficio al usar el cifrado asimétrico. Sólo necesitas un par de claves, por usuario, para cada uno, para poder cifrar mensajes para todos los demás usuarios.
- → Con el cifrado simétrico, a medida que aumenta el número de usuarios, aumenta el número de claves.

Usos de la criptografía

La criptografía cuenta con 3 usos: cifrar, autenticar y firmar.

Cifrar:

Siempre hay cierta información que no queremos que sea conocida más que por las personas que nosotros queramos. En esto nos ayuda el cifrado. Cifrando un mensaje hacemos que este no pueda ser leído por terceras personas consiguiendo así la tan deseada privacidad.

Autenticación:

Otra de las necesidades que surgen con la aparición de internet es la necesidad de demostrar que somos nosotros y que el emisor es quien dice ser. Un método de autenticación puede ser el propio cifrado. Si ciframos un mensaje con una clave solo conocida por nosotros, demostrando que somos quien decimos ser, el receptor podrá constatar nuestra identidad descifrándolo. Esto se puede conseguir mediante clave simétrica (el receptor tiene que estar en posesión de la clave empleada) o usando clave asimétrica en su modo de autenticación.

Firmar:

Dados los trámites que podemos realizar hoy en día a través de internet se hace necesaria la aparición de la firma digital. Igual que firmamos un documento, la firma digital nos ofrece la posibilidad de asociar una identidad a un mensaje.

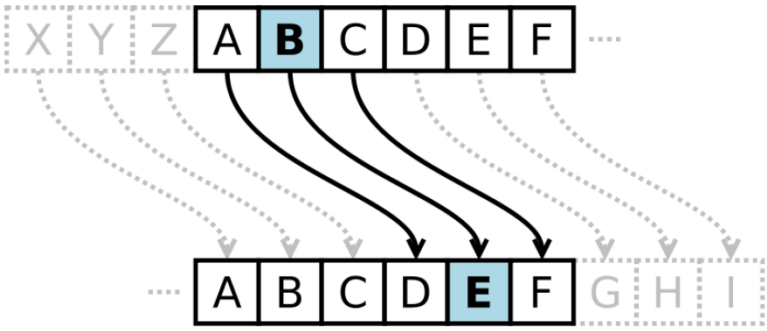
Para la firma digital se utiliza clave asimétrica (dos claves una privada y otra pública). Lo que se cifra con la clave privada (que solo nosotros conocemos) sólo se puede descifrar con la pública. De esta forma al cifrar con nuestra clave privada demostramos que somos nosotros.

La firma digital tiene un problema. ¿Cómo sabe el receptor que la clave corresponde realmente con la persona o entidad que dice poseerla? De este modo surgen las entidades de certificación. Organismos de confianza que actúan como notarios.

Otro sistema existente, es la red de confianza. En esta red los usuarios certifican si los demás son quienes dicen ser. De este modo podría decirse que cada usuario se constituye como entidad certificadora.

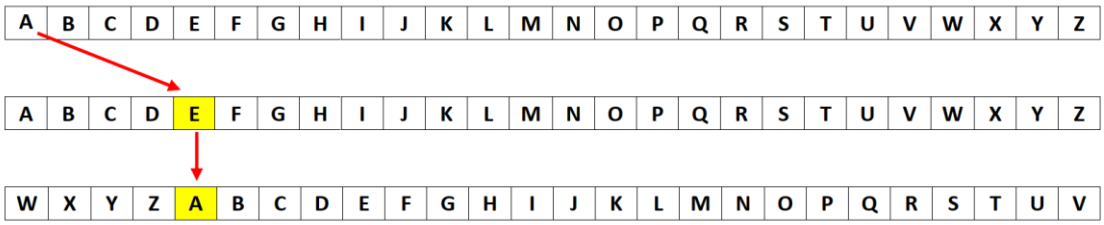
Cifrado César (Cifrado por Desplazamiento):

Es una de las técnicas de cifrado más simples y más usadas. Es un tipo de cifrado por sustitución monoalfabética en el que una letra en el texto original es reemplazada por otra letra que se encuentra en un número fijo de posiciones más adelante en el alfabeto. Al desplazar el alfabeto una cantidad determinada de posiciones y alinearlo con el alfabeto sin desplazar, se obtiene una relación entre las letras.



Por ejemplo, con un desplazamiento de 3, la A sería sustituida por la D (situada 3 lugares a la derecha de la A), la B sería reemplazada por la E, y así sucesivamente. Este método debe su nombre a Julio César, que lo usaba para comunicarse con sus generales.

Este cifrado contiene un ***"Mensaje Original"***, ***"Posición"*** (derecha o izquierda) y un ***"Número de Desplazamiento"*** que se utiliza tanto para el cifrado como el descifrado.



Consigna en Clase: Resolver el siguiente ejercicio, mediante el cifrado de César.

- Mensaje Original → Hola, buenos días
- Numero de Desplazamiento → 4
- Posición → Derecha

Mensaje Original

H	O	L	A	,		B	U	E	N	O	S		D	I	A	S

Mensaje Cifrado

L	S	P	E	,		F	Y	I	R	S	W		H	M	E	W

Cifrado Vigenère:

Es un cifrado basado en diferentes series de caracteres o letras del cifrado César formando estos caracteres una tabla, llamada *"Tabla de Vigenère",* que se usa como clave. El cifrado Vigenère se ha reinventado muchas veces. El método original fue descrito por Giovan Battista Belasso en su libro de 1553 La cifra del Sig. Giovan Battista Belasso. Sin embargo, fue incorrectamente atribuido más tarde a Blaise de Vigenère, concretamente en el siglo XIX, y por ello aún se le conoce como el "cifrado Vigenère". Este cifrado es conocido porque es fácil de entender e implementar, además parece irresoluble; esto le hizo ganar el apodo de *"El Código Indescifrable".* Este cifrado contiene un ***"Mensaje Original"*** y una ***"Clave"*** que se utiliza tanto para el cifrado como el descifrado.

Mensaje

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

Consigna en Clase: Resolver el siguiente ejercicio, mediante el cifrado de Vigenère.

Mensaje Original → Fotosíntesis

Clave → Contraseña

Mensaje Original

F	O	T	O	S	I	N	T	E	S	I	S

Clave

C	O	N	T	R	A	S	E	Ñ	A	C	O

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

Mensaje Original

F	O	T	O	S	I	N	T	E	S	I	S

Clave

C	O	N	T	R	A	S	E	Ñ	A	C	O

Mensaje Cifrado

H	C	G	H	J	I	F	X	R	S	K	G