

Cryptography



Prof. Claudia Ximena Muñoz Ausecha

INTRODUCCION

La **criptografía** es la ciencia que se encarga de proteger la información mediante técnicas que la transforman, de modo que solo las personas autorizadas puedan entenderla. Se utiliza desde hace siglos, pero hoy en día es fundamental para la seguridad en el mundo digital.

La criptografía **convierte información entendible (texto plano)** en un formato **ilegible (texto cifrado)** mediante procesos matemáticos, y solo quien tenga la **clave correcta** puede volverla a entender.

EJEMPLO

Imagina que quieres decirle a un amigo "TE VEO A LAS 7", pero no quieres que nadie más lo entienda. Entonces cambias las letras con una regla secreta (como mover cada letra 3 lugares en el alfabeto). El mensaje se vuelve incomprendible para quien no sepa la regla.

CRIPTOGRAFÌA

La criptología (del griego krypto y logos, estudio de lo oculto, lo escondido): Ciencia que trata los problemas teóricos relacionados con la seguridad en el intercambio de mensajes en clave entre un emisor y un receptor a través de un canal de comunicaciones.

Criptografía:

Esta también ocupa del cifrado de mensajes en clave y del diseño de criptosistemas.

Criptoanálisis: Trata de descifrar los mensajes en clave, rompiendo así el criptosistema.

Objetivos principales de la criptografía

Confidencialidad: Solo quien debe ver el mensaje puede entenderlo.

Integridad: Asegura que el mensaje no ha sido alterado.

Autenticación: Verifica quién envió el mensaje.

No repudio: El emisor no puede negar que envió el mensaje.

Temas generales de la criptografía

Texto plano (plaintext): Es el mensaje original que quieres proteger.

Cifrado (encryption): Es el proceso de transformar ese mensaje en algo ilegible.

Texto cifrado (ciphertext): Es el resultado ilegible del cifrado.

Descifrado (decryption): Es el proceso inverso: volver el texto cifrado a su forma original.

Clave (key): Es un valor secreto que se usa para cifrar o descifrar el mensaje.

Tipos de criptografía

Criptografía simétrica

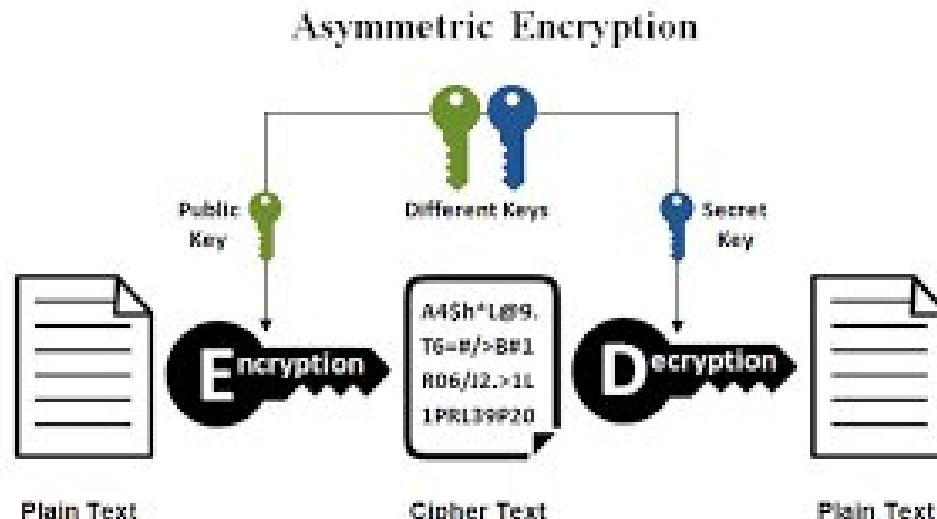
- Usa la misma clave para cifrar y descifrar.
- Ejemplo: AES (Advanced Encryption Standard)



Tipos de criptografía

Criptografía asimétrica

- Usa **una clave pública** para cifrar y **una privada** para descifrar.
- Ejemplo: **RSA**
- Muy usada en sitios web (HTTPS) y firmas digitales.



Uso de la criptografía

- Proteger contraseñas y datos personales
- Garantizar la confidencialidad en mensajes
- Firmar documentos digitalmente
- Hacer transacciones seguras (banca, criptomonedas)

Algoritmo RSA

El algoritmo **RSA** es un sistema de cifrado de clave pública muy utilizado en la seguridad informática, especialmente para proteger datos confidenciales cuando se transmiten por internet.

Algoritmo RSA

RSA son las iniciales de los apellidos de sus inventores: **Rivest, Shamir y Adleman**, quienes lo desarrollaron en 1977.

Dónde se usa RSA

HTTPS (seguridad en sitios web)

Firmas digitales

VPNs

Correos electrónicos cifrados

Autenticación en sistemas seguros

Función hash

Una función hash es un algoritmo que **toma una entrada (un dato cualquiera)** y la convierte en una **salida de longitud fija**, normalmente representada como una cadena de caracteres o un número.

Ejemplo

Entrada: "Hola mundo" Hash SHA-256:
a830d7beb04eb7549ce990fb7dc962e499
a27230e9fe22d5faffb3e0c8c... (etc.)

CRIPTOGRAFIA

Del griego Kryptos (oculto) y graphein (escribir) Es el arte o ciencia de cifrar y descifrar información utilizando técnicas que hagan posible el intercambio de mensajes de manera segura que sólo puedan ser leídos por las personas a quienes van dirigidos.



Sus técnicas complementarias:

EL CRIPTOANÁLISIS

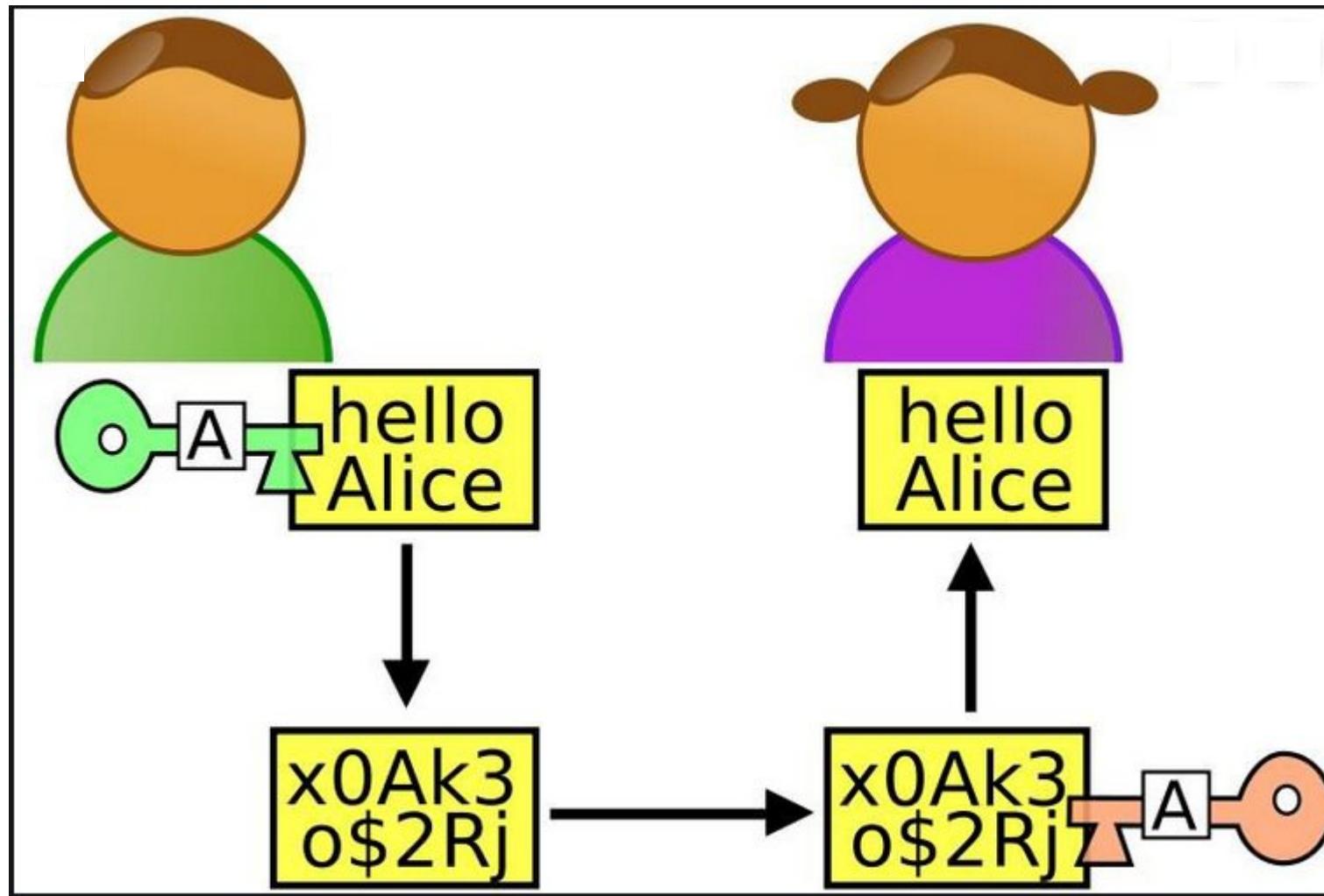
Del griego cryptos (oculto) y analyein (desatar) que estudia los métodos que se utilizan para romper textos cifrados con objeto de recuperar la información original en ausencia de las claves.

La Criptografía es un arte antigua que surge, prácticamente, como un escrito y dará diferentes tipos de cifrado :

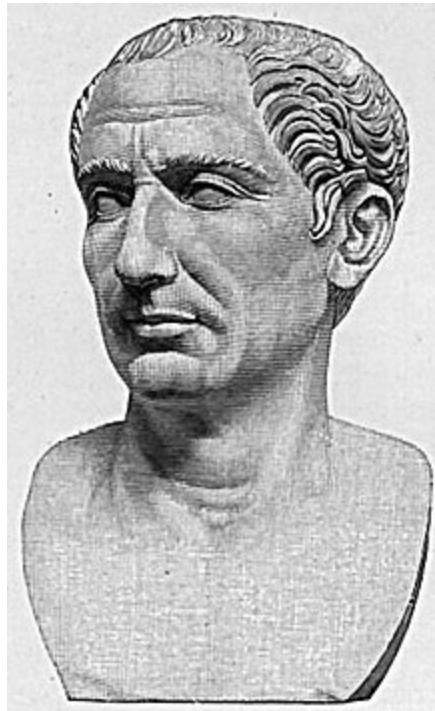
- CRIPTOSISTEMAS
- Confidencialidad
- Integridad
- No repudio



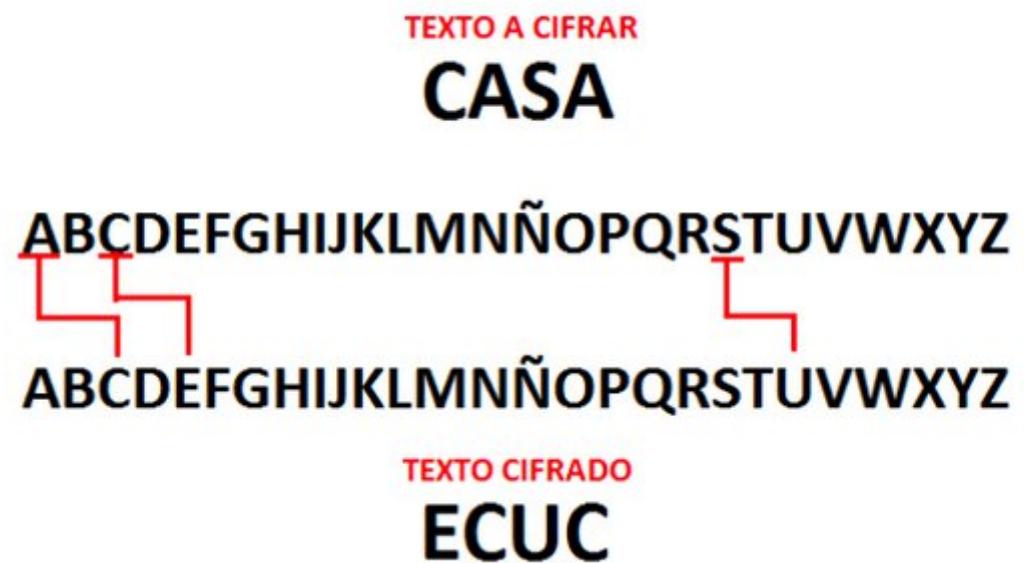
CRIPTOGRAFIA



K-1 (sistema de César 3):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 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 K-2 (sistema de César 17):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 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-3 (sistema de César 8):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 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



En criptografía, el cifrado **César**, también conocido como **cifrado por desplazamiento**, **código de César** o **desplazamiento de César**, es una de las técnicas de cifrado más simples y más usadas. Es un tipo de cifrado por sustitución en el que una letra en el texto original es reemplazada por otra letra que se encuentra un número fijo de posiciones más adelante en el alfabeto.



Método de Julio César

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Letra
original



Desplazamiento



$$D(x) = (x+k) \bmod N$$



MÉTODO DE JULIO CESAR

Desplazamiento de 3 letras

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

Ejemplo

La transformación se puede representar alineando dos alfabetos; el alfabeto cifrado es un alfabeto normal que está desplazado un número determinado de posiciones hacia la izquierda o la derecha.

Para codificar un mensaje, simplemente se debe buscar cada letra de la línea del texto original y escribir la letra correspondiente en la línea codificada. Para decodificarlo se debe hacer lo contrario.

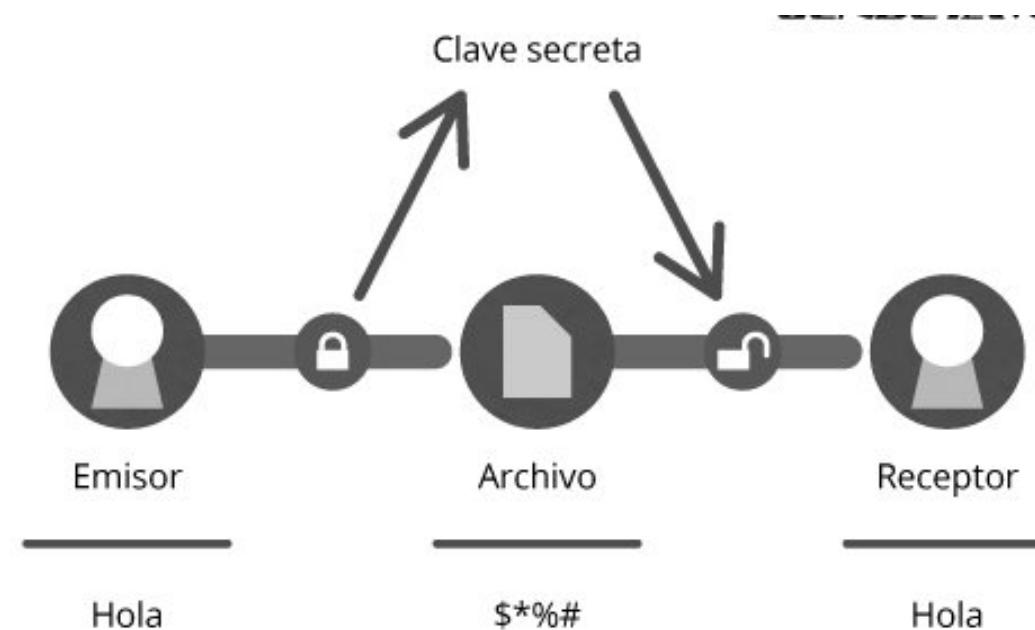
Texto original: TECNOLOGIA EN SISTEMAS

Texto codificado: WHFPRÑRJLD HP VLVWHODV



Criptografía simétrica

La **criptografía simétrica** es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma.



El 50% de las contraseñas son inferiores a 8 caracteres o (las típicas: 123456, password, qwerty...) y realmente una contraseña de 6 dígitos puede ser fácil de resolver por un hacker con un equipo básico en un par de semanas o en una ínfima fracción de segundo por un equipo de profesionales con un supercomputador.

Tiempo estimado de poder vulnerar una clave cifrada es de 3 meses. (símbolos, letras, etc)



Fortaleza de claves de acceso

¿Cómo creo una contraseña segura?

«123456» es una de las contraseñas más utilizadas por los usuarios, pero aunque resulte fácil de recordar, no es una clave fuerte, las recomendaciones al crear la contraseña.

Un mínimo de 6 caracteres. Cuantos más tenga, mejor.

Combinar distintos caracteres: números, mayúsculas y minúsculas. Usar otros caracteres, como los símbolos, aporta un nivel de seguridad adicional a nuestra clave, pero puede dificultar su recuerdo y ser incompatible con algunos sistemas. Para ayudar a crear una contraseña segura, incluyen un indicador visual de fortaleza que nos guiará paso a paso en su creación:

Cambiar contraseña :

Muy buena 

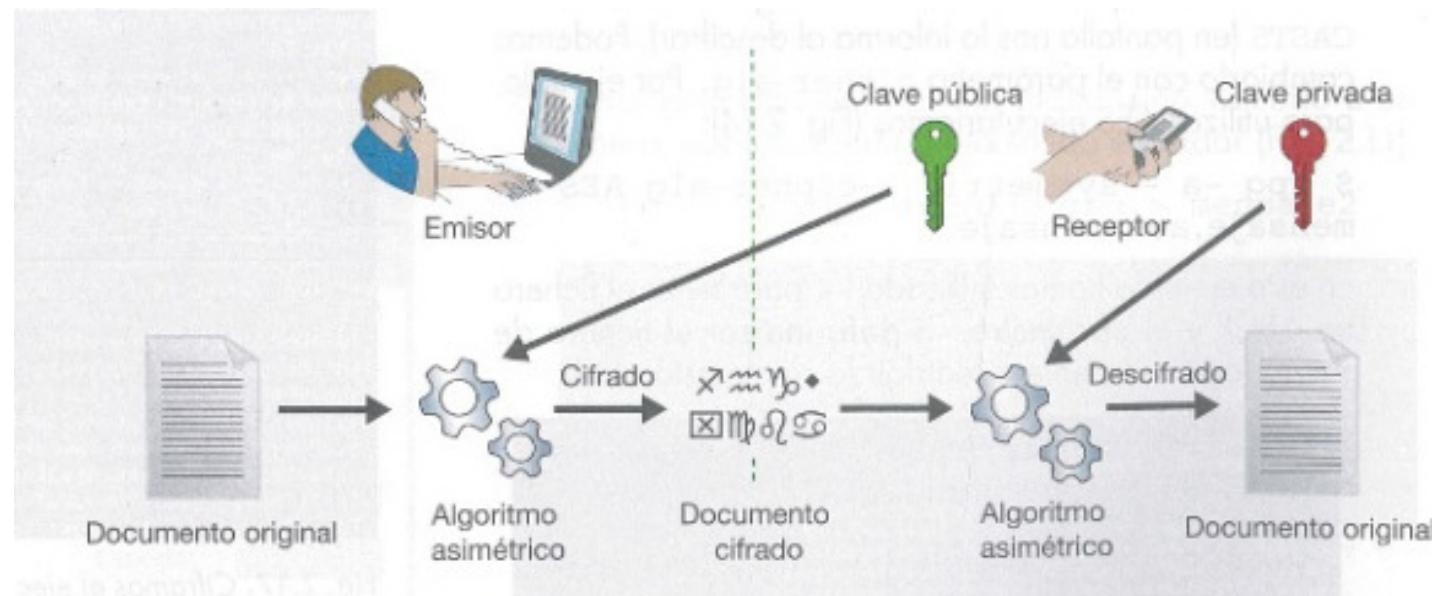
La contraseña debe contener:

- ✓ Entre 6 y 12 caracteres
- ✓ Al menos una letra minúscula
- ✓ Al menos una letra mayúscula
- ✓ Al menos un número
- ✓ No se permiten otros caracteres

<https://passwordsgenerator.net/es/>

Criptografía asimétrica.

- La criptografía asimétrica se basa en el uso de **dos claves**: **la pública** (que se podrá difundir sin ningún problema a todas las personas que necesiten mandarte algo cifrado) y **la privada** (que no debe de ser revelada nunca).



Cifrado de Vigenère

El **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 de Vigenère es un cifrado de sustitución simple polialfabético.

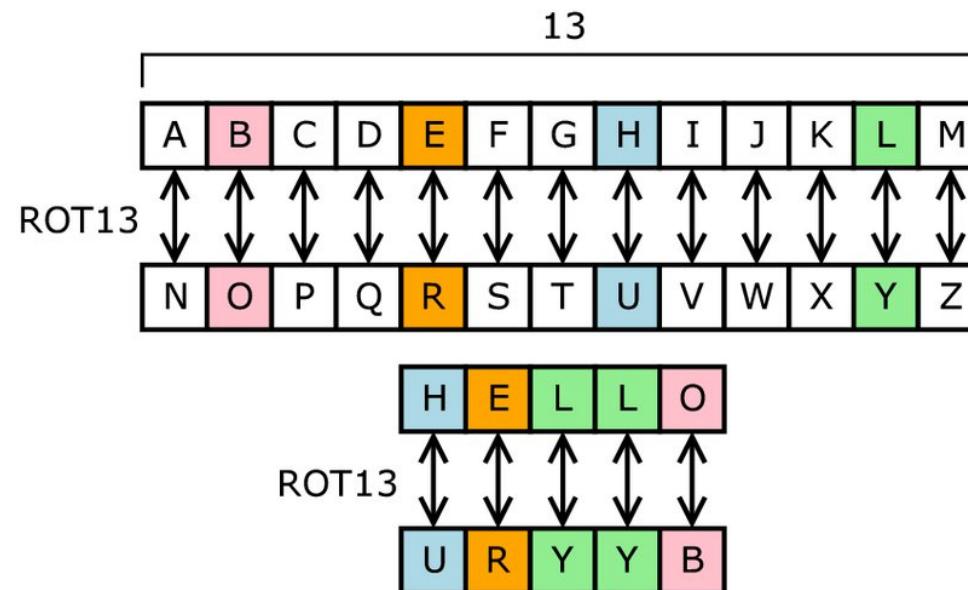
El método original fue descrito por Giovan Battista Belasso en su libro de 1553 *La cifra del Sig. Giovan Battista Belasso*. Sin embargo, fue incorrectamente atribuido más tarde a Blaise de Vigenère, concretamente en el siglo XIX, y por ello aún se le conoce como el "cifrado Vigenère".

Blaise de Vigenère



SISTEMAS DE SUBSTITUCIÓN POLIALFABÉTICA

Los sistemas de substitución simple y de permutación son mucho fáciles de ser quebrados. La tentativa de colocar más dificultades no proceso tentativo - intención de sistema poli alfabetico. Este sistema, son reemplazados de un único alfabeto de sustitución, son utilizados varios alfabetos permutados, trocados periódicamente una señal de mensaje. Un objetivo principal de que va tentar desvendar o código é descubrir o período de clave y, después, los códigos usados. Por ejemplo, una clave poli alfabética de período tres va ha modificar las posiciones cero, tres, seis, etc, de mensajes de acuerdo con el primer código, las posiciones en, cuatro, siete, etc, con un segundo código y las posiciones dos, cinco, ocho, etc con un tercero. Tómese una clave $K=\{3,17,8\}$, tenemos:



Entrada texto plano texto a cifrar

Entrada Clave o palabra 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

https://cic.unb.br/~rezende/segdados_files/Sharky%27s%20Vigenere%20Cipher.html

<https://www.dcode.fr/cifrado-vigenere>

LOS TIPOS DE CLASES DE HACKERS

- 1. WHITE - HATS = Profesional ético” protección”
 2. BLACK - HATS = No son éticos “Crímenes”
 3. GRAY - HATS = Ambas actividades “éticos y no éticos”



Taller en clase.

Cifrar con método de Julio Cesar y Vigenére las siguientes frases.

- Cien años de soledad
- Nació una flor a orillas de una fuente.
- “La tecnología por sí sola no basta. También tenemos que poner el corazón” – *Jane Goodall*
- ‘Un mal PROGRAMADOR puede crear fácilmente dos nuevos empleos al año’ – *David Parnas*
- NO POR MUCHO MADRUGAR AMANECE MAS TEMPRANO

Tu tiempo es limitado, de modo que no lo malgastes viviendo la vida de alguien distinto. No quedes atrapado en el dogma, que es vivir como otros piensan que deberías vivir. No dejes que los ruidos de las opiniones de los demás acallen tu propia voz interior. Y, lo que es más importante, ten el coraje para hacer lo que te dice tu corazón y tu intuición.

El recordar que estaré muerto pronto es la herramienta más importante que he encontrado para ayudarme a tomar las grandes decisiones en la vida. Porque casi todo —todas las expectativas externas, todo el orgullo, todo temor a la vergüenza o al fracaso— todas estas cosas simplemente desaparecen al enfrentar la muerte, dejando sólo lo que es verdaderamente importante. Recordar que uno va a morir es la mejor manera que conozco para evitar la trampa de pensar que hay algo por perder. Ya se está indefenso. No hay razón alguna para no seguir los consejos del corazón.

Steve Jobs

¡Preguntas!