CC3078 Cifrado de Información
Sección 11
Erick Stiv Junior Guerra Muñoz - 21781

Ejercicio de Criptografía

Repositorio de GitHub: erickguerra22/Cifrados_2025.git

Parte 1:

Cifrado Vigenère

La relevancia del cifrado Vigenère radica en que marcó un hito en la evolución de las técnicas criptográficas al introducir el uso de múltiples alfabetos sustitutivos como base para el cifrado y descifrado de textos. Este avance inauguró la era de los cifrados polialfabéticos, revolucionando la seguridad de la información en su tiempo.

La primera referencia teórica a este enfoque se encuentra en el libro *"Tractate on Ciphers"*, escrito en 1467 por Leon Battista Alberti, quien es considerado uno de los pioneros de la criptografía. Sin embargo, el cifrado Vigenère toma su nombre del diplomático francés Blaise de Vigenère, del siglo XVI, quien presentó sus ideas al rey Enrique III. No obstante, la historia de este cifrado es más compleja y cuenta con la participación de otros personajes destacados, como el criptógrafo italiano Giovan Battista Bellaso, quien describió técnicas similares en su obra *"La Cifra del Sig. Giovan Battista Bellaso"*.

Aunque Blaise de Vigenère no fue el creador original del cifrado, sus aportaciones, incluidas en su tratado *"Traicté des Chiffres"* publicado en el siglo XVI, enriquecieron significativamente la criptografía de su tiempo. Desde el siglo XIX, el cifrado lleva exclusivamente su apellido, probablemente debido a la influencia de los historiadores franceses, quienes destacaron las contribuciones de Vigenère basándose en su obra. (Marvin the Robot, 2015)

Aplicación destacada:

Durante la guerra civil estadounidense, el cifrado Vigenère era utilizado para enviar mensajes entre los soldados, esto mediante un dispositivo compuesto de dos discos, en donde el interno puede girar hasta la posición deseada y así simplificar el método de cifrado y descifrado. (Población, 2018)

Ejemplo: Cifrar la palabra CRIPTOGRAFIA.

Este tipo de cifrado toma como base al cifrado César, de manera que se obtiene una tabla con diferentes alfabetos sustitutivos en ciclos:

	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

Ahora, para cifrar el texto deseado, especificamos una palabra clave, por ejemplo, LLAVE.

Teniendo la clave utilizar, repetimos sus caracteres hasta alcanzar la longitud de la palabra original:

Texto	C	R	I	P	T	O	G	R	A	F	I	A
Clave	L	L	A	V	E	L	L	A	V	E	L	L

Por último, cada carácter del texto cifrado será la conjunción entre la fila del carácter correspondiente en la clave, junto con la columna del carácter correspondiente en el texto original. Por ejemplo, para el primer caso, se buscaría en la fila L y la columna C, que según la tabla a utilizar, corresponde a la letra N, y así con todo el texto.

Texto	C	R	I	P	T	O	G	R	A	F	I	A
Clave	L	L	A	V	E	L	L	A	V	E	L	L
Cifrado	N	C	I	K	X	Z	R	R	V	J	T	L

Por lo tanto, nuestro resultado sería: NCIKXZRRVJTL.

Para realizar el descifrado del texto se realizaría el proceso inverso: Se buscan las filas que corresponden a las letras de nuestra clave, buscamos cada carácter del texto cifrado, y se toma

la letra que indica la columna de la matriz. Por ejemplo, para descifrar la N; buscamos la fila L, buscamos la N y vemos que se encuentra bajo la columna C. Por lo tanto, el primer carácter de nuestro texto descifrado es la C, que concuerda con la palabra original, CRIPTOGRAFIA.

Ventajas:

- Al ser un cifrado polialfabético; su robustez es bastante confiable, puesto que descifrar un carácter no proporciona automáticamente la clave para descifrar el texto completo.

- Una misma letra de la palabra cifrada puede corresponder a diferentes letras de la palabra original, puesto que podría estar encriptada con diferentes alfabetos al mismo tiempo.

- Utiliza un sistema de claves para realizar el encriptado y descifrado del texto, por lo que es necesario conocer la palabra clave utilizada para poder obtener el texto original.

Vulnerabilidades:

- La vulnerabilidad más grave, descubierta por el oficial Friedrich Kasiski en el siglo XIX, destaca el hecho de que la clave utilizada debe ser repetida varias veces para poder alcanzar la longitud del texto a cifrar, por lo que descubriendo dicha longitud, cada carácter puede ser tratado como un cifrado César independiente, el cual puede ser más fácil de corromper. Sabiendo esto, incluso sin conocer exactamente cuál es la clave utilizada, descubrir la longitud de la misma nos facilitaría la tarea de romper el sistema de ecnriptación. (Población, 2018)

Bibliografía

Marvin the Robot. (2015). *Cómo un cifrado del siglo XVII se convirtió en la base de un cifrado irrompible del siglo XX*. Obtenido de https://www.kaspersky.es/blog/vigenere-cipher-history/6804/

Población, A. (2018). *La cifra Vigenère: el misterioso código que se tardó tres siglos en descifrar.* Obtenido de https://www.abc.es/ciencia/abci-cifra-vigenere-misterioso-codigo-tardo-tres-siglos-descifrar-201811192150_noticia.html?ref=https%3A%2F%2Fwww.abc.es%2Fciencia%2Fabci-cifra-vigenere-misterioso-codigo-tardo-tres-siglos-descifrar-201811192150_noticia.html