Universidad del Valle de Guatemala
Diego Andrés Morales Aquino
21762

Cifrado Vigenére

El cifrado Vigenére es un método de cifrado por sustitución polialfabética que utiliza una clave repetitiva para encriptar texto. Cada letra del texto plano se cifra usando una tabla, donde la fila se selecciona según una letra de la clave y la columna según una letra del texto plano. Es más seguro que el cifrado César porque utiliza múltiples alfabetos.

Historia

El cifrado Vigenére, un método de sustitución polialfabética, fue descrito inicialmente por Giovan Battista Bellaso en 1553. Sin embargo, en el siglo XIX se le atribuyó erróneamente a Blaise de Vigenère, quien en realidad desarrolló el cifrado de clave automática, un sistema diferente pero relacionado. Este error contribuyó a la fama del cifrado Vigenère. En 1863 Friedrich Kasiski ideó un método general para descifrarlo.

El cifrado Vigenére es el más famoso entre los sistemas polialfabéticos, desde los siglos XIV y XV, Al-Qalqashandi mencionó este tipo de cifrados. Sin embargo, el cifrado Alberti, creado por Leon Battista Alberti, es reconocido como el primer cifrado polialfabético correctamente descrito. Este sistema fue diseñado para ocultar las frecuencias de las letras, revolucionando la criptografía al superar el análisis de frecuencia, el único método de descifrado conocido en su época.

El cifrado Vigenère fue utilizado para proteger cartas, mensajes militares y diplomáticos debido a su resistencia frente a ataques. Hoy en día solo se emplea en contextos no críticos, ya que su seguridad es fácilmente comprometida. (tutorialspoint, 2025)

Ventajas y desventajas

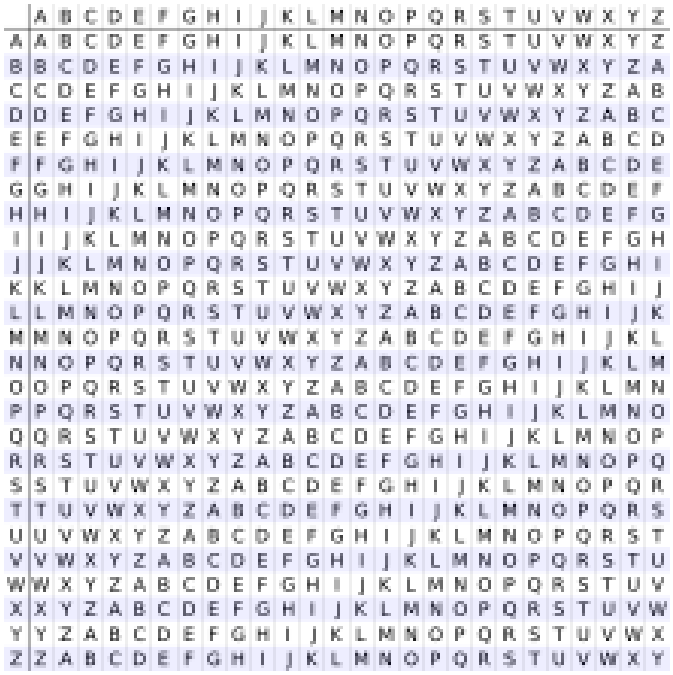
El cifrado Vigenére presenta varias ventajas que lo hicieron destacar en su época. Al ser un cifrado polialfabético, utiliza múltiples alfabetos de cifrado, lo que incrementa su complejidad y lo hace más seguro frente a los cifrados de sustitución simple. Además, permite flexibilidad en la gestión de claves, ya que se basa en palabras o frases que pueden cambiarse fácilmente para distintos mensajes, y una clave más larga y compleja mejora su seguridad. También ofrece resistencia al análisis de frecuencias, ocultando las características estadísticas del texto original y dificultando los métodos de descifrado basados en este análisis.

Entre las desventajas que presenta se encuentra que es vulnerable al análisis de Kasiski, ya que los patrones repetidos en el texto cifrado pueden revelar la longitud de la clave. Además, su seguridad depende de la longitud y aleatoriedad de la clave, lo que implica que claves cortas o predecibles lo debilitan. También puede ser comprometido mediante ataques con texto simple conocido, en los que un atacante con acceso al texto original y su versión cifrada puede deducir partes de la clave. Por último, aunque el cifrado Vigenére protege la confidencialidad del mensaje, no garantiza autenticidad ni integridad, dejando el contenido expuesto a manipulaciones. (learnUk, 2024)

El cifrado Vigenére me parece interesante porque, a diferencia de cifrados más básicos como el de desplazamiento, introduce una mayor complejidad al utilizar múltiples alfabetos de sustitución y el uso de llaves. Esto lo hace menos predecible y más desafiante para descifrar sin la clave adecuada. Aunque es fácil de descifrar actualmente, este me parece más completo que el resto de algoritmos históricos, pues el uso de una clave añade un nivel de personalización que lo hace más versátil que los demás.

Ejemplo

Tabla de Vigenére



	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

Para llevar a cabo el cifrado, se repite la llave cuantas veces sea necesario para cubrir la longitud total del mensaje a encriptar. Posteriormente, se selecciona cada par de caracteres (texto plano – llave) y se busca en la fila el carácter correspondiente al texto original y en la columna al de la llave. El carácter de la intersección se concatena al mensaje cifrado. Este proceso se repite para cada uno de los caracteres del mensaje.

Utilizando el mensaje “Having a pet can make you happy” y la llave “Trixie”, se obtiene el siguiente cifrado:

Plain	H	A	V	I	N	G	A	P	E	T	C	A	N	M	A	K	E	Y	O	U	H	A	P	P	Y
Key	T	R	I	X	I	E	T	R	I	X	I	E	T	R	I	X	I	E	T	R	I	X	I	E	T
Cipher	A	R	D	F	V	K	T	G	M	Q	K	E	G	D	I	H	M	C	H	L	P	X	X	T	R

Para el descifrado, de igual manera se debe repetir la llave para cubrir la misma longitud del mensaje cifrado. Posteriormente, se selecciona la fila que corresponda al carácter de la llave y,

a continuación, se debe buscar la posición en donde se encuentra la letra del texto cifrado en esa fila. Por último, buscar la etiqueta de la columna, en donde dicho carácter, corresponderá al texto sin cifrar.

Cipher	A	R	D	F	V	K	T	G	M	Q	K	E	G	D	I	H	M	C	H			L	P	X	X	T	R
Key	T	R	I	X	I	E	T	R	I	X	I	E	T	R	I	X	I	E	T			R	I	X	I	E	T
Plain	H	A	V	I	N	G	A	P	E	T	C	A	N	M	A	K	E	Y	O			U	H	A	P	P	Y

Link del repositorio:
https://github.com/Aq202/cifrados_uvg/tree/main/ejercicios/eje_criptograf%C3%ADa

Referencias

learnUk. (2024). *Cifrado Vigenère*. Retrieved from https://learnlearn.uk/edexcel-igcse-computer-science/vigenere-cipher/

tutorialspoint. (2025). *Criptografía - Cifrado Vigenére*. Retrieved from https://www.tutorialspoint.com/cryptography/cryptography_vigenere_cipher.htm