Pablo Andrés Zamora Vásquez
Carné 21780

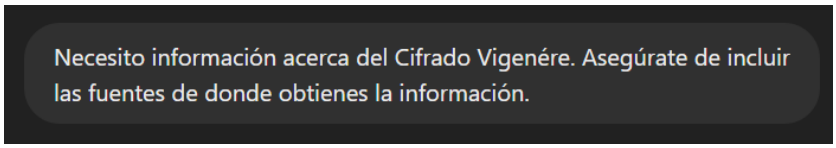
Ejercicio de Criptografía

Link del repositorio: https://github.com/pabloozamora/UVG_Cifrados.git
Link al chat de GPT-4o: https://chatgpt.com/share/6799b012-3084-800e-a6ee-66735e106543

Parte 1

1) Realizar la investigación de un cifrado a su elección del contenido "**historia de criptografia".**

Prompt hecho a GPT:



El cifrado de Vigenère es un método de encriptación alfabético basado en una tabla que consta de diferentes cifrados Caesar en secuencia. Fue descrito por primera vez por Gioven Battista Bellaso en 1553, pero su nombre proviene de Blaise de Vigenère, ya que este último publicó una variante más robusta en 1586.

El proceso de encriptación consiste en los siguientes pasos:

- Se elige una palabra clave que se concatena hasta igualar la longitud del texto plano.

- Se utiliza una tabla (de 26 x 26 letras, en caso de utilizar el abecedario inglés), en donde cada fila representa un desplazamiento del alfabeto. Cabe mencionar que el alfabeto que se utilizará tanto en la tabla como para el texto plano y la llave no necesariamente es el abecedario, puede componerse de cualesquiera símbolos.

- Finalmente, cada letra del texto plano se cifra buscando la intersección de esta y la letra correspondiente de la llave en la tabla.

En posible representar matemáticamente este proceso de la siguiente manera:

$$C(p_i) = (p_i + k_i)\ mod\ L$$

Pablo Andrés Zamora Vásquez
Carné 21780

En donde p_i es el caracter del texto plano en la posición i, k_i es el caracter de la llave en la posición i, y L es el tamaño del alfabeto.

Para descifrar el mensaje, se realiza el proceso inverso:

$$C(p_i) = (p_i - k_i + L) \, mod \, L$$

2) Mostrar un ejemplo de aplicación.

El cifrado de Vigenère ya no se considera seguro para aplicaciones críticas de seguridad; sin embargo, es una buena herramienta para comprender los fundamentos de criptografía y cómo han evolucionado los cifrados.

No obstante, me parece interesante una de las aplicaciones que se le dio en el pasado, antes de quedar obsoleto: Durante la Guerra Civil de Estados Unidos (1861-1865), el Ejército Confederado utilizaba una disco de cifrado de campo, el cual les permitía comunicarse utilizando el cifrado de Vigenère. El disco se componía de dos círculos que rotaban, simulando la intersección de las letras en una tabla de 26 x 26.

Fuente: Crypto Museum.

Pablo Andrés Zamora Vásquez
Carné 21780

Ejemplo de uso

Si se quisiera cifrar el texto plano “UNIVERSIDAD”, utilizando la llave “PABLO” y el abecedario inglés de 26 letras:

Primero, se concatenan los caracteres de la llave hasta que esta iguale la longitud del texto plano, de manera que:

p = UNIVERSIDAD
k = PABLOPABLOP

Luego, con el apoyo de la siguiente tabla:

	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

Fuente: Michigan Technological University

Se encuentra la intersección entre cada uno de los pares de caracteres correspondientes del texto plano y la llave:

U	N	I	V	E	R	S	I	D	A	D
P	A	B	L	O	P	A	B	L	O	P
J	**N**	**J**	**G**	**S**	**G**	**S**	**J**	**O**	**O**	**S**

Por tanto, el texto cifrado (*c*) sería: **JNJGSGSJOOS.**

Alternativamente, al utilizar la fórmula del cifrado, es posible obtener el mismo resultado:

Pablo Andrés Zamora Vásquez
Carné 21780

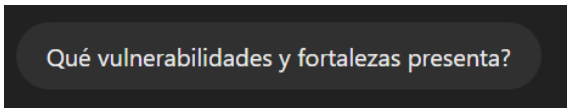
p_i	U	N	I	V	E	R	S	I	D	A	D
Valor	20	13	8	21	4	17	18	8	3	0	3

k_i	P	A	B	L	O	P	A	B	L	O	P
Valor	15	0	1	11	14	15	0	1	11	14	15

p_i	k_i	$p_i + k_i$	Mod 26	c_i
20	15	35	9	**J**
13	0	13	13	**N**
8	1	9	9	**J**
21	11	32	6	**G**
4	14	18	18	**S**
17	15	32	6	**G**
18	0	18	18	**S**
8	1	9	9	**J**
3	11	14	14	**O**
0	14	14	14	**O**
3	15	18	18	**S**

3) Explicar porque lo eligieron, cual creen que son sus ventajas y vulnerabilidades.

Prompt hecho a GPT:



Decidí investigar este cifrado ya que me pareció uno de los de mayor complejidad en cuanto a los cifrados históricos vistos en clase. Sin embargo, sé que ya no es usado actualmente, puesto que presenta varias vulnerabilidades que lo hacen obsoleto en la criptografía moderna.

Vulnerabilidades:

- Es bastante regular. Es decir, al utilizar una serie de cifras cíclicas, es posible simplemente buscar series de grupos de letras que se repitan periódicamente,

Pablo Andrés Zamora Vásquez
Carné 21780

especialmente si la llave es corta.

- Si el mensaje es lo suficientemente largo, es posible aplicar análisis estadísticos como análisis de frecuencias de las letras cifradas para determinar la clave.

- El cifrado fue roto por Charles Babbage y Kasiski, haciendo pública la técnica que utilizaron.

No obstante, el cifrado posee ventajas en comparación a otros más simples.

Ventajas:

- La llave tiene un comportamiento dinámico que cambia cómo se cifra cada caracter, por lo que una llave más larga y aleatoria sea la llave, más complicado será descifrar el mensaje.

- Al utilizar un sistema polialfabético; esto es, no se restringe a un solo alfabeto, resulta mucho más complejo que métodos como el cifrado Ceasar, lo que lo hizo parecer inquebrantable en su momento.

Bibliografía

Crypto Museum. *(2010). Vigenère Cipher*. Obtenido de: https://www.cryptomuseum.com/crypto/vigenere/

Hageman, M. (s.f.*). The Cipher Disk*. Obtenido de: http://www.civilwarsignals.org/pages/crypto/cipherdisk.html

Michigan Technological University. (s.f.*). The Vigenère Cipher Encryption and Decryption*. Obtenido de https://pages.mtu.edu/~shene/NSF-4/Tutorial/VIG/Vig-Base.html

CC3078 Cifrado de Información
Sección 10

Pablo Andrés Zamora Vásquez
Carné 21780