UANL
UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FCFM
FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS

Alumno: César Alonso García Villafaña

Matricula: 1859187

Profesor: Angel Salvador Pérez Blanco

Materia: Criptografía y seguridad

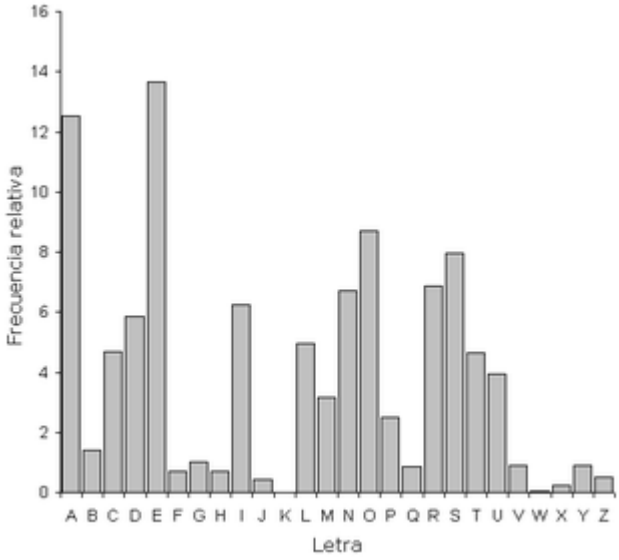
Grupo: 032

Método de cifrado César

Introducción:

Esta técnica fue utilizada por Julio César para comunicarse con sus generales.

El cifrado César, una de las técnicas de cifrado más simples y conocidas, se cuenta entre los métodos de cifrado más antiguos. Se basa en el cifrado monoalfabético, caracterizándose por su relativa debilidad en términos de seguridad, dado que su mensaje es fácilmente descifrable debido a sus técnicas de protección mínimas. El cifrado César se clasifica como un cifrado por sustitución, donde cada letra del texto plano se desplaza por un número fijo en el alfabeto. El principio fundamental del Cifrado César se basa en el intercambio de letras, reemplazando cada letra en el texto original por otra que se encuentre varias posiciones más adelante en el alfabeto.



El criptoanálisis del cifrado de Cesar es sencillo y se basa en el estudio de las frecuencias relativas de las letras en cada idioma.

Las **ventajas** son:

- Uno de los métodos más fáciles de usar en criptografía y puede proporcionar una seguridad mínima a la información.
- Uso de solo una tecla breve en todo el proceso
- Uno de los mejores métodos para usar si el sistema no puede usar ninguna técnica de codificación complicada
- Requiere pocos recursos informáticos

Las **desventajas** son:

- Uso de estructura simple
- Solo puede proporcionar seguridad mínima a la información
- La frecuencia del patrón de letras proporciona una gran pista para descifrar el mensaje completo.

¿Cómo descifrar el cifrado César?

Romper un cifrado César generalmente sigue uno de tres escenarios dependiendo de la cantidad de conocimiento que tenga el criptoanalista atacante:

- Sabe que el cifrado es un cifrado César.
- Sabe que el cifrado es un cifrado de sustitución, pero no un cifrado César.
- Desconoce por completo el tipo de cifrado al que se enfrentan.

En todos los escenarios propuestos, suponiendo que el cifrado se base en un cambio numérico simple, el código se puede descifrar fácilmente usando un ataque de fuerza bruta (probando todos los cambios posibles y determinando cuál funciona). Si consideramos un cifrado César con clave, las cosas se vuelven considerablemente más difíciles, aunque aun relativamente fáciles de descifrar.

Explicación de los pasos necesarios para el Cifrado César:

- El primer paso es elegir un número entero (generalmente entre 1 y 26) que servirá como nuestro desplazamiento y que representa cuántas posiciones tendremos que mover las letras del alfabeto para cifrar nuestros mensajes.
- Una vez hayamos elegido nuestro desplazamiento debemos escribir el mensaje que queremos cifrar.
- Ahora debemos reemplazar la letra inicial por la letra hallada después del número indicado en nuestro desplazamiento, repitiendo este mismo procedimiento con todas las demás letras del texto original hasta obtener la versión cifrada completa.
- Una vez hayas terminado todos los pasos anteriores estás listo para compartir tu texto de cifrado con la persona destinataria quien tendrá que decodificarlo utilizando el mismo desplazamiento utilizando por ti.

¿Sigue siendo efectivo este sistema de encriptación?

Uno de los principales problemas de seguridad de los cifrados de sustitución es que retienen las distribuciones de caracteres del texto subyacente; Algunas letras son más utilizada; Dado que los cifrados de sustitución crean un mapeo uno a uno entre letras de texto sin formato y letras de texto cifrado, al identificar la letra más común en un texto cifrado probablemente revelará la letra a la que se le asigna en el cifrado.

Descifrar un cifrado de sustitución general mediante análisis de frecuencia requiere más trabajo que un cifrado por desplazamiento porque la asignación de texto sin formato a texto cifrado debe determinarse para cada letra utilizada en el mensaje.

Mediante el uso de una combinación de pistas e información de frecuencia, los cifrados de sustitución se pueden romper fácilmente.

En resumen, hoy en día el cifrado César no tiene la suficiente eficacia para cifrar textos secretos ya que, con la tecnología actual, llevaría pocos minutos descifrar ese texto.

Ejemplo:

Supongamos que la clave es 9 y el mensaje a cifrar es:

EL PRÓXIMO LUNES HAY EXAMEN DE MATEMATICAS

Representamos en una tabla el nuevo alfabeto desplazado 9 posiciones:

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

Sustituimos cada letra por su correspondiente en el nuevo alfabeto. Nuestro mensaje quedará de la siguiente manera:

NT YAXGQUX TDVNB PJH NGJUVNV MN UJCNUJCQLJB

Por tanto, el emisor recibirá el siguiente mensaje:

NTYAXGQUXTDNBPJHNGJUVNVMNUJCNUJCQLJB

Método de vigenere.

Introducción

Vigenere es un método para cifrar texto alfabético. Utiliza una forma simple de sustitución polialfabética. Un cifrado polialfabético es cualquier cifrado basado en la sustitución, utilizando alfabetos de sustitución múltiple. El cifrado del texto original se realiza utilizando el cuadrado de Vigenère o la tabla de Vigenère.

Vigenère Blaise de

1523-1596

Historia

El cifrado Vigenère de hecho, se ha reinventado muchas veces. El método se describió por primera vez por Giovan Battista Bellaso en 1553, aunque por alguna razón se le atribuye su invención a Blaise de Vigenère (1523–1596). El cifrado es relativamente simple de entender e implementar y por tres siglos se consideró uno de los mejores por su resistencia a ser descifrado. Fue Friedrich Kasiski, sin embargo, en 1863, el primero en analizar y descifrar el esquema Vigenère.

¿En qué consiste el cifrado de vigenere?

El cifrado consiste en agregar la clave al texto sin formato. El cálculo se realiza letra por letra (la adición de letra se realiza de hecho por números, se suman los valores de las letras). El resultado se da módulo 26: si el resultado es mayor o igual a 26, reste 26 del resultado (donde 26 es la longitud del alfabeto).

Para hacer coincidir la longitud del texto con la clave, se repite

Matriz del cifrado de vigenere para el alfabeto español

La tabla consiste en los alfabetos escritos 26 veces en diferentes filas, cada alfabeto desplazado cíclicamente a la izquierda
En diferentes puntos del proceso de encriptación, el cifrado usa un alfabeto diferente de una de las filas. El alfabeto utilizado en cada punto depende de una palabra clave repetitiva.

	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	27
1	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
2	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	A
3	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	A	B
4	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
5	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	D
6	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	D	E
7	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
8	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
9	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
10	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
11	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
12	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
13	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
14	N	Ñ	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
15	Ñ	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
16	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	Ñ
17	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	Ñ	O
18	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P
19	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q
20	S	T	Y	S	T	Y	S	T	Y	S	T	Y	S	T	Y	S	T	Y	S	T	Y	S	T	Y	S	T	Y
21	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S
22	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T
23	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U
24	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V
25	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W
26	Y	Z	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
27	Z	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

Tablero Vigènere para el Alfabeto Español - C43S4RS ©

Para **cifrar** con Vigenere a través de una tabla con dos entradas.

El mensaje claro en la parte superior de la tabla y la letra de la clave en la columna izquierda. La letra encriptada se encuentra en la intersección

Ejemplo: Encripta el texto en claro “PARIS” con la clave “LOUP”

- Localice la letra **P** en la primera línea y la letra **L** en la primera columna, por lo tanto, la letra cifrada se encuentra en la intersección: **A**.
- Localice la letra **A** en la primera línea y la letra **O** en la primera columna, por lo tanto, la letra cifrada se encuentra en la intersección: **O**.
- Localice la letra **R** en la primera línea y la letra **U** en la primera columna, por lo tanto, la letra cifrada se encuentra en la intersección: **M**.
- Localice la letra **I** en la primera línea y la letra **P** en la primera columna, por lo tanto, la letra cifrada se encuentra en la intersección: **X**.
- Localice la letra **S** en la primera línea y la letra **L** en la primera columna, por lo tanto, la letra cifrada se encuentra en la intersección: **D**.

El **descifrado** de Vigenere requiere una clave (y un alfabeto). Para descifrar, tome la primera letra del mensaje y la primera letra de la clave, y reste sus valores. Si el resultado es negativo, agregue 26 al resultado (donde 26 es el número de letras en el alfabeto), el resultado corresponde al rango en el alfabeto de la letra clara.

Localice la primera letra de la clave en la columna izquierda y explore la línea hasta encontrar la primera letra del mensaje cifrado. Entonces, vuelva a subir la columna para leer la letra clara correspondiente (en la parte superior).

Referencias

- González, A. (2020, June 10). ¿Qué es el cifrado César y cómo funciona? Ayuda Ley Protección Datos. https://ayudaleyprotecciondatos.es/2020/06/10/cifrado-cesar/
- Marujita. (2023, May 17). Cifrado César. Muy Tecnológicos. https://muytecnologicos.com/diccionario-tecnologico/cifrado-cesar
- (N.d.). Ugr.Es. Retrieved October 27, 2023, from https://www.ugr.es/~anillos/textos/pdf/2011/EXPO-1.Criptografia/Img/img24.gif
- Sangaku S.L. (2023) El método César. sangakoo.com. Recuperado de https://www.sangakoo.com/es/temas/el-metodo-cesar
- (N.d.-b). Bing.com. Retrieved October 27, 2023, from https://th.bing.com/th/id/OIP.AEWVFwxJ44ruFqQ_ckf9MAHaGv?pid=ImgDet&rs=1
- Cifrado de Vigenere on dCode.fr [online website], retrieved on 2023-10-27, https://www.dcode.fr/cifrado-vigenere