ALGORITMOS TRADICIONALES DE CRIPTOGRAFÍA: RAIL FENCE Y MONOMIO-BINOMIO

REALIZADO POR:
ROBERTO BENAVIDES
MARÍA GRACIEL CRUZ
JUAN DIEGO OBANDO
SHARON VALDIVIA
SOL VELÁSQUEZ

RAIL FENCE

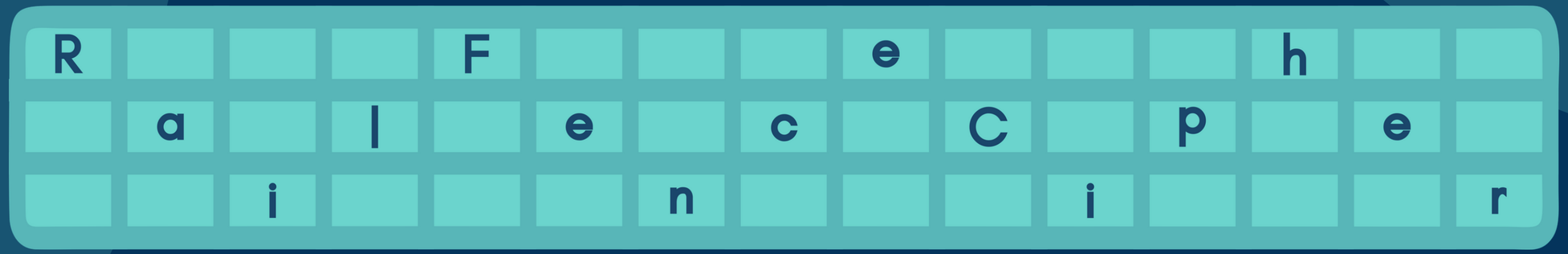
INTRODUCCIÓN

El cifrado Rail Fence también conocido como cifrado en ZigZag es una forma de cifrado por transposición. Su cifrado se realiza al colocar un texto plano en diferentes “líneas de riel” pero es sencillo de ser descifrado y se podría hacer manualmente.

CIFRADO

Texto Plano: RailFenceCipher

Clave: 3

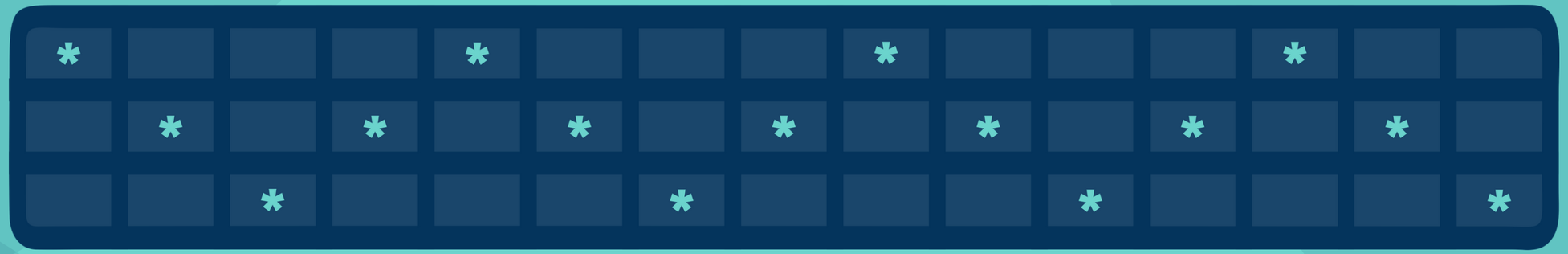


Texto cifrado:RFehalecCpeinir

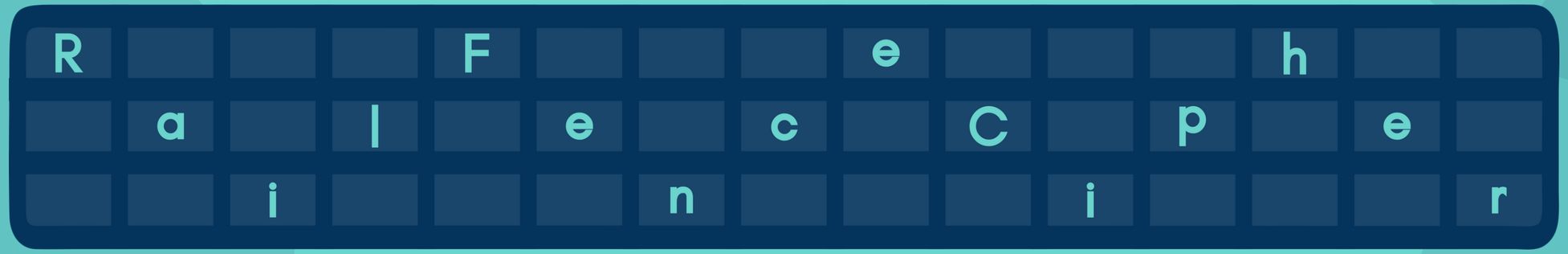
DESCIFRADO

Clave: 3

Texto cifrado:RFehalecCpeinir



Reemplazando los lugares marcados por el texto:



Texto Plano: RailFenceCipher

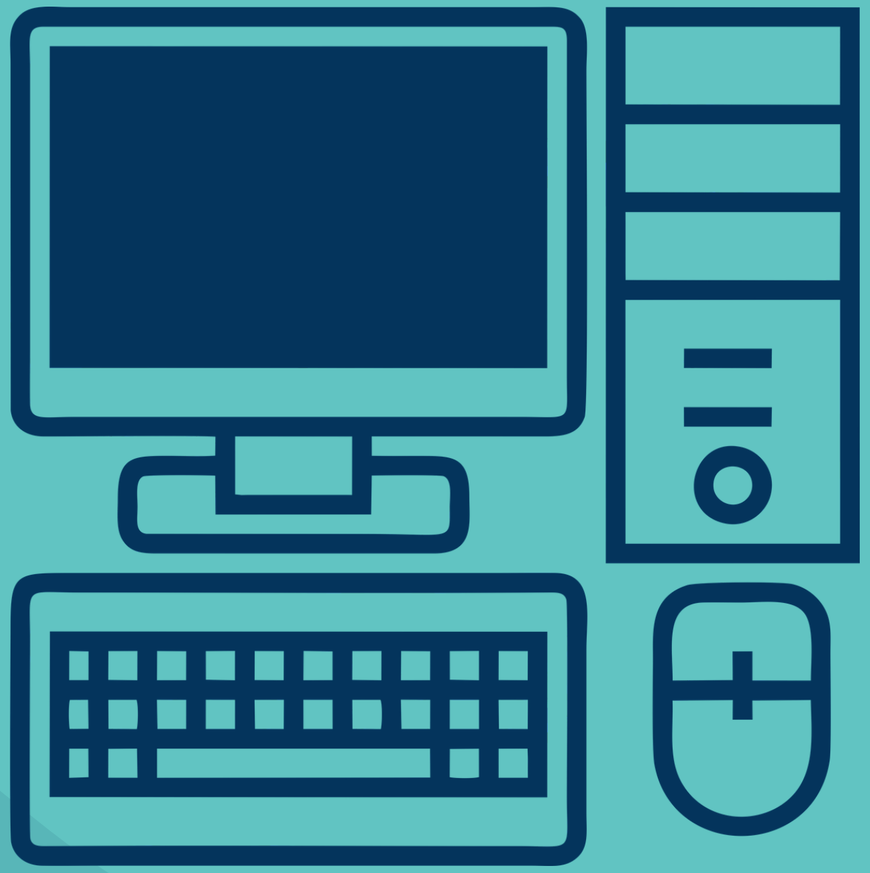
CRIPTOANÁLISIS

LA FRECUENCIA DE LETRAS SE MANTIENE

BRUTE FORCE ATTACK

INSEGURO

MONOMIO-BINOMIO

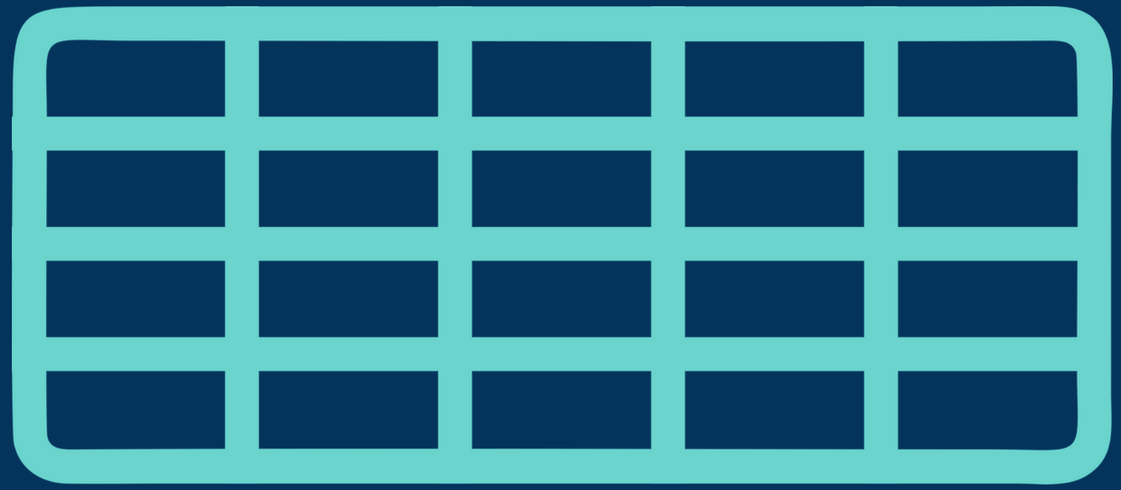


INTRODUCCIÓN

Sistema de cifrado basado en una sustitución simple. Se cree que su origen fue en Rusia.

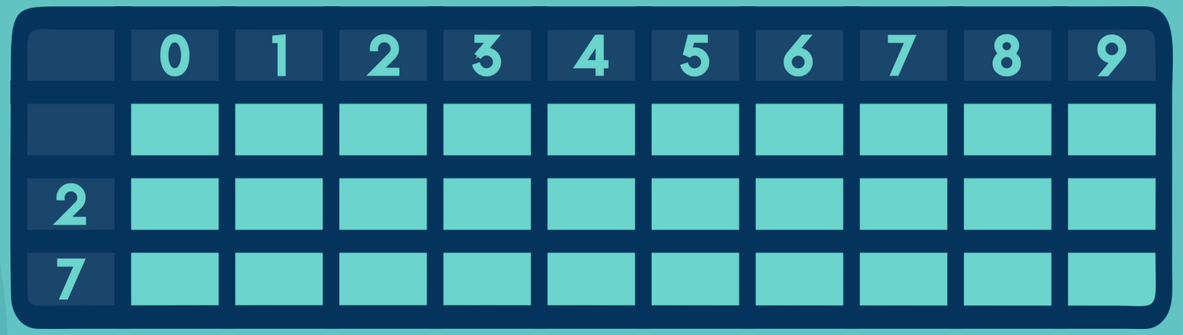
FUNCIONAMIENTO

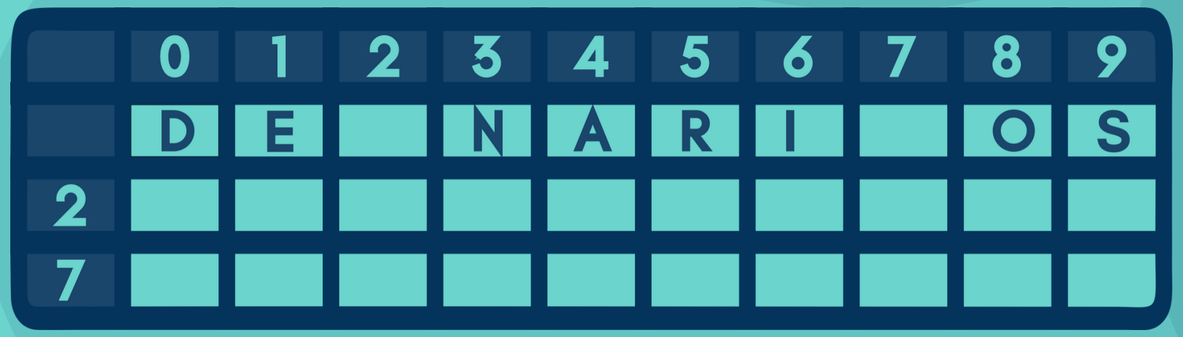
Cada letra del mensaje se sustituye por sus coordenadas en el tablero demediado.



CREAMOS UN TABLERO DE 11*4

Donde la primera columna y la primera fila marcan las coordenadas, las columnas se enumeran del 0 al 9 y las filas llevan un espacio vacío y 2 números aleatorios entre el 0 y 9.





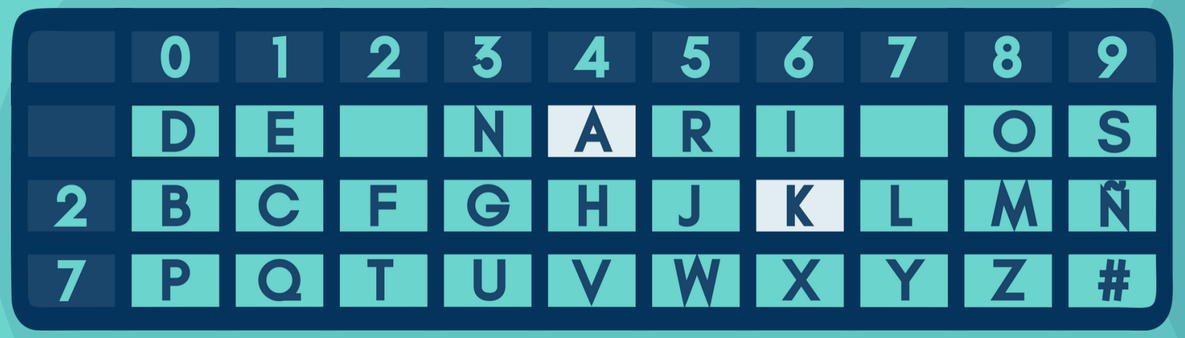
SE USA UNA PALABRA MNEMOTÉCNICA

Que conste de las 8 letras más usadas sin que se repita alguna, esta se coloca en la primera fila dejando en blanco los espacios escogidos para las columnas anteriormente.

SE COMPLETA EL ALFABETO

En las casillas restantes omitiendo las letras ya usadas en la palabra anterior. Se puede usar el espacio sobrante y agregar otra fila para mas caracteres.

	0	1	2	3	4	5	6	7	8	9
	D	E		N	A	R	I		O	S
2	B	C	F	G	H	J	K	L	M	Ñ
7	P	Q	T	U	V	W	X	Y	Z	#



LAS COORDENADAS PUEDEN SER DE UNA O DE 2 CIFRAS

dependiendo de su posición en la tabla, son de 1 cifra si se ubican en la primera fila y son de 2 si se ubican en la segunda o tercera fila. A=4, k=26

EJEMPLO

	0	1	2	3	4	5	6	7	8	9
	D	E		N	A	R	I		O	S
2	B	C	F	G	H	J	K	L	M	Ñ
7	P	Q	T	U	V	W	X	Y	Z	#

ESTE ES UN MENSAJE CIFRADO

↓

19721 19 733 281394251 216225408

DESCIFRADO

Usando la tabla, reemplazamos los números por sus respectivas letras, tomando en cuenta que el 2 o el 7 nos indica que tomemos la siguiente cifra como parte de las coordenadas.

DESCIFRADO

	0	1	2	3	4	5	6	7	8	9
	D	E		N	A	R	I		O	S
2	B	C	F	G	H	J	K	L	M	Ñ
7	P	Q	T	U	V	W	X	Y	Z	#

19721 19 733 281394251 216225408

↓

ESTE ES UN MENSAJE CIFRADO

CRIPTOANÁLISIS

El primer paso es realizar un análisis de frecuencias para descubrir que los 2 números que más se repiten son los que marcan las coordenadas de las filas, y los que le siguen pueden ser la letra a, e y o. Luego con estos datos se realiza un "BRUTE FORCE ATTACK".

EJEMPLO

Frecuencias

2	29
7	28
4	26
1	20
9	15
5	13
3	11
0	9
8	8
6	6

13 2749 21496272749 51972437219 82867261308 2749 27172549 774 7394049 13 274 7042742054 437215685 91 7073101 73945 127 197042168 9820543721 77 423512345 87254 226274 70454 2849 2145421721519

EN LAS CASILLAS RESTANTES OMITIENDO LAS LETRAS YA USADAS EN LA PALABRA ANTERIOR SE PUEDE USAR EL ESPACIO SOBRANTE Y AGREGAR OTRA FILA PARA MAS CARACTERES

	0	1	2	3	4	5	6	7	8	9
	D	E		N	A	R	I		O	S
2	B	C	F	G	H	J	K	L	M	Ñ
7	P	Q	T	U	V	W	X	Y	Z	#

BIBLIOGRAFIA

- Cifrado "Rail Fence". (2019). Retrieved 17 April 2020, from https://www.geocachingtoolbox.com/index.php?lang=es&page=railFenceCipher
- Kumar, A. Rail Fence Cipher - Encryption and Decryption - GeeksforGeeks. Retrieved 17 April 2020, from https://www.geeksforgeeks.org/rail-fence-cipher-encryption-decryption/

BIBLIOGRAFIA

- Knight, S. (2010). The Rail Fence Cipher. Retrieved 17 April 2020, from http://www.cs.trincoll.edu/~crypto/historical/railfence.html
- Wikipedia. (18 de Marzo de 2020). Obtenido de https://es.wikipedia.org/wiki/Monomio-binomio
- Wikiwand. (18 de Abril de 2020). Obtenido de https://www.wikiwand.com/es/Monomio-binomio