

Manual técnico – Crypto Spyro

Crypto Spyro es un algoritmo de cifrado simétrico el cual incluye las operaciones básicas que un algoritmo de cifrado debe contemplar de manera que se pueda crear confusión y difusión en el mensaje a cifrar. El presente documento tiene como objetivo demostrar el funcionamiento de este algoritmo.

Requerimientos Técnicos:

Versión: Node.js 12.*.*

Navegador (*recomendado): Google Chrome

Funcionamiento

Cifrado

1. El algoritmo recibe una cadena de caracteres y un password.
 - a. Por ejemplo:
 - i. cadena: es nuestro criptograma
 - ii. password: seguridad2021

La cadena de caracteres se acomoda matrices de 4x4

e	s	_	n
u	e	s	t
r	o	_	c
r	i	p	t

o	g	r	a
m	a	_	_

-	-	-	-
-	-	-	-

2. El texto es reacomodado en dirección de espiral en el sentido de las manecillas del reloj

e	s	-	n
c	r	i	u
-	t	p	e
o	r	t	s

o	g	r	a
c	r	i	m
-	-	-	a
-	-	-	-

3. Se realiza una transposición de filas por columnas

e	c	-	o
s	r	t	r
-	i	p	t
n	u	e	s

o	c	-	-
g	r	-	-

r	i	-	-
a	m	-	-

4. Se aplica la siguiente función hash al password para obtener la clave
 clave: Seguridad2021
 Clave generada a partir del password:

La función hash recibe el password y genera la siguiente la clave:
 4590678156762526934599481340312712682053370853510109930956218541753786
 82163761n

5. Se realiza una operación XOR con la clave y cada carácter
 clave:
 4590678156762526934599481340312712682053370853510109930956218541753786
 82163761n

Caracter. S :- 01010011

clave XOR S = 1011001011100010

6. Finalmente, se aplica una operación de desplazamiento de bits a la derecha y el resultado se convierte a base 16

Original : 10**11001011100010**
 Shifted: **11001011100010**10

Interfaz Gráfica

Para utilizar la interfaz gráfica abre el archivo "index.html" en tu navegador.

Encrypt your plain text

Plain text:

Ingresa aquí el texto a cifrar

Your password:

Ingresa aquí la clave

Encrypt

Your cryptogram:

Texto cifrado

Decrypt your cryptogram

Cryptogram:

Texto cifrado

Your password:

Ingresa aquí la clave

Decrypt

Your plain text:

The image shows a web application interface for text encryption and decryption. It is divided into two main sections: 'Encrypt your plain text' and 'Decrypt your cryptogram'. Each section contains a form with a text input field, a password input field, a button to perform the action (Encrypt or Decrypt), and a result field. The interface is dark-themed with green accents.