Instituto de ciencias básicas

Criptografía y seguridad en redes
Tarea 3

Integrantes : Matias Torres Gonzalez
Profesor : Nicolás Boettcher
Ayudantes : Macarena Velásquez y Francisco Lara
Fecha : 26 de mayo del 2021

1. Introducción

Para este trabajo se utilizo el algoritmo twofish. En el presente informe se darán a conocer los procesos hecho para realizar la tarea

2. Generar el html desde python

Para generar el html se utilizo el siguiente codigo:

```
#Crea el archivo .html y lo abre
with open('html_archivo.html', 'w') as f:
    f.write(str(html_archivo))
webbrowser.open("html_archivo.html")
```

También se utilizo la librería webbrowser para que una vez creado el archivo html este se abriera automáticamente.

3. Modificar variables Python

En este caso solo se permite modificar la clave de cifrado:

```
#Ingresar clave de cifrado
key = input('Ingrese una clave para cifrar: ')
#Ejemplo: )H&53,PMyCBuY[72C_Mc
x = Twofish(b"""key""")
```

4. Generar archivo cifrado Python

En este caso el mensaje a cifrar será ”mimamamemimamama”

```
8    #Mensaje cifrado:
9    y = x.encrypt(b"mimamamemimamama")
10   Cifrado = str(y)
11
```

Una vez elegida una clave de cifrado y el mensaje encriptado se agregan las dos variables a lo que será el html:

```
html_archivo = """<!DOCTYPE html>
<html lang="es">
    <head>
        <meta charset="URF-8">
        <meta http-equiv="X-UA-Compatible" content="IE=edge">
            <meta name="viewport" content="wodth=device-width, initial-scale=1.0">
        <title>Tarea 3 Crypto</title>
    </head>
    <body>
        <p>Este sitio contiene un mensaje secreto</p>
        <div class="twofish" id="""+Cifrado+"""></div>
        <div class="key" id="""+key+"""></div>
    </body>
</html>
"""
```

5. Tampermonkey

Lo primero que se realiza es obtener las variables necesarias del html, en este caso la clave de cifrado y el mensaje:

```
// Obtiene las variables
var code = document.getElementsByClassName("twofish");
var c = code[0].id;
var key = document.getElementsByClassName("key");
var k = key[0].id;
```

Después se descencripta el mensaje con:

```
var decryted = twofish.decrypt(key,msg);
```

6. Conclusión

En este trabajo no se logro realizar la tarea completa, pero aun así se logro comprender el funcionamiento del algoritmo twofish y implementar el cifrado, lamentablemente la segunda parte no se pudo realizar porque no se logro comprender como funcionaba la libreria twofish en Javascript