**EncryptEd**

* **Descripción**

El proyecto consiste en un juego educativo / juego para encriptar y desencriptar mensajes conociendo las claves. La idea nació a raíz de no encontrar ningún software educativo e interactivo para aprender sobre criptografía. EncryptEd consiste en unas lecciones sobre cada tipo de cifrado en él, una serie de retos y unas máquinas en las que se puede encriptar y desencriptar mensajes.

* **Desarrollo**

Este proyecto consta de los siguientes elementos de desarrollo de software:

* + 2073 líneas de código.
  + 6 módulos.
  + 61 funciones.
  + 23 ficheros de datos.
  + Librerías:
    - PyCryptoDome, binascii, base64, os, json.

A screenshot of a computer

Description automatically generated

Figura 1. Estructura de módulos

* **Menús**

El juego tiene varios menús, con submenús y subcategorías en cada submenú.

A black background with text

Description automatically generated

Este primer menú es el main\_menu, dentro de él tiene los submenús lecciones\_menu, retos\_menu y maquinas\_menu. Además, tiene una opción de Sigue Aprendiendo en la que se encuentran links para aprender criptografía a mayor nivel y una opción para salir del juego.

A screen shot of a computer

Description automatically generated

El menú de lecciones tiene en él una introducción al mundo de la criptografía y luego una serie de submenús de diferentes tipos de cifrados, en cada uno se encuentran algunos de los cifrados más importantes de cada categoría.

A computer screen shot of white text

Description automatically generatedA screen shot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

En el menú de retos, encontramos 10 retos, de dificultad ascendiente pero muy simples, son unos retos interactivos con pistas sobre el cifrado y acceso a máquinas para poder desencriptar los mensajes cifrados. En ellos, se debe usar las máquinas implementadas en el juego para poder desencriptar los mensajes.

A screenshot of a computer

Description automatically generated

Por último, tenemos el menú de máquinas:

A screen shot of a computer

Description automatically generated

Dentro de cada submenú tenemos los mismos cifrados que se encontraban en las lecciones:

A screenshot of a computer screen

Description automatically generatedA screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Front - End**

* **Entrada al programa**

Al entrar, el programa pide el nombre del usuario ya que algunas de las lecciones son “interactivas” en cuanto a que el nombre del usuario aparece, para crear un acercamiento con el usuario.

* **Lecciones**

La primera opción en el menú de lecciones es “Introducción”. En ella explica la estructura del programa, así como para que sirve cada submenú. Sigue con una explicación y definición de criptografía y explica la importancia de ella en la historia y sus usos modernos. Luego hace una recomendación de aprendizaje para aquellos usuarios completamente nuevos a la criptografía.

Después de ello, el programa devuelve al usuario al menú de lecciones donde se pueden elegir entre las diferentes categoría de cifrado y sus distintos cifrados en ellas.

Todas las lecciones siguen una estructura muy similar:

1. Historia del cifrado elegido
2. Explicación del funcionamiento del cifrado
3. Ejemplo explicando el funcionamiento del cifrado de forma visual.
4. Retos básicos (algunos tienen 1 y otros 2 retos). (Si el usuario se cansa de intentar descifrar el mensaje y no es capaz, cada dos intentos, se le dará la opción de terminar los retos y volver a intentarlos en otro momento).

* **Retos**

El menú de los retos contiene 10 retos, que varían en dificultad y en tipo de cifrado. Se ha intentado que sean retos totalmente fuera del ámbito matemático ya que a muchas personas la criptografía les asusta por culpa de las matemáticas, en cambio, he intentado que sea un juego más centrado en que el usuario se convierta en un detective y, dadas x pistas, consigan descifrar el mensaje, ya teniendo las matemáticas metidas en un programa que hacen el trabajo para ellos.

* **Máquinas**

En cada máquina se encuentra la opción de encriptar o desencriptar:

Primero veremos la función de encriptar.

A black background with white text

Description automatically generated

Nos pedirá un texto a introducir:

A black background with white text

Description automatically generated

Y, en este cifrado, el cifrado César, nos pide ahora una llave numérica:

A screenshot of a computer code

Description automatically generated

Al introducir una llave y pulsar enter:

A screenshot of a computer program

Description automatically generated

El programa nos devuelve el texto encriptado, el tipo de cifrado y la llave usada.

Veamos ahora cómo funciona el modo de desencriptar. Introduciré el texto que acabamos de encriptar y como conocemos la llave debería devolver el texto inicial:

A screenshot of a computer program

Description automatically generated

Como podemos ver, devuelve el texto inicial

* **Sigue Aprendiendo**

A screen shot of a computer

Description automatically generated

Aquí se puede ver el menú que se abre al elegir la opción de Seguir Aprendiendo. Como se observa, hay 4 tipos de cifrados y unas animaciones que ayudan a entender los cifrados más complejos.

**Back - End**

* **Main**

A computer screen shot of a computer code

Description automatically generated

El main es muy simple, lo que hace es pedir el input del nombre del usuario y lo guarda en un archivo .txt y el programa lo vuelve a abrir cuando haga falta. Luego llama al main\_menu(), que es el menú principal:

A screenshot of a computer

Description automatically generated

En cuanto a la navegación del juego, se basa principalmente en el uso de este tipo de menús.

* **Lecciones**

Las lecciones se basan básicamente en abrir el json con la información requerida y manejar los inputs que se reciben al hacer los retos en cada una de las lecciones.

A screen shot of a computer program

Description automatically generated

He cogido un ejemplo, donde se puede ver el manejo del json y en la parte inferior de la captura de pantalla, el manejo de las respuestas y si el usuario quiere seguir contestando los retos. Para resolver los retos, usa las máquinas que se explicarán más adelante.

* **Retos**

Los retos son una mezcla de lecciones y máquinas.

Primero cargan el texto del json “retos” e imprimen su contenido. Luego funcionan como los retos de las lecciones, pero con mezclas más complejas, es decir, mezcla distintos cifrados en un mismo ejercicio dadas unas pistas para poder resolverlo. Un ejemplo:

A screen shot of a computer program

Description automatically generated

* **Máquinas**

Las máquinas son la parte más compleja de todo el programa ya que en ellas tienen la lógica de cada tipo de cifrado integrado en el programa. Sigue las reglas generales de cada cifrado, por lo que es una simulación idéntica al funcionamiento de los cifrados en la vida real.

Es cierto que he utilizado librerías para facilitarme la tarea de algunas partes de los cifrados más complejos ya que recrear cifrados como RSA, Curva Elíptica o AES, requieren un muy alto nivel de conocimiento de criptografía y matemáticas, además de algoritmos inmensos.

A continuación, está una captura de pantalla de ejemplo, que muestra todo el proceso desde la generación de llaves, hasta encriptar o desencriptar para el cifrado RSA.

A screen shot of a computer program

Description automatically generated

Los cifrados clásicos han sido todos programados por mí, sin usar ningún tipo de librerías, en AES, DES, RSA y Curva Elíptica tuve que usar librerías debido a su complejidad, pero si que cree la lógica del cifrado y su algoritmo.

* **Otros**

Para imprimir el menú y limpiar la terminal tengo una función: clear\_terminal()

A screen shot of a computer

Description automatically generated

Al iniciar el juego, se pide el nombre al usuario, y por “privacidad” al finalizar el programa, el archivo de texto: nombre.txt se elimina automáticamente para borrar el nombre:

Aquí coge el nombre:

A computer code with many colorful text

Description automatically generated with medium confidence

Aquí lo borra:

A computer code with green and yellow text

Description automatically generated

Por último, tengo un archivo que se llama convertidor.py. En este archivo, lo que hacía era coger un archivo .txt e imprimir en la terminal el texto con los saltos de línea como \n y con las líneas alineadas como estaban en el .txt para pasarlas a un json donde ahora tengo todos los textos de las lecciones, retos, etc. Esto lo hice de esta forma ya que fue un cambio a mitad de proyecto cuando ya estaban escritos todos los textos y retos.

A computer screen shot of text

Description automatically generated