T3	**Seguridad Informática** #6 Fernando Escamilla Hernández #15 Nancy Paredes Moreno #18 Jahel Pérez Gutiérrez #26 Arturo Serrano Valencia #29 Paul Torres Rivera #31 Sandro Iván Yllescas Lamas	**7B**	**E #2**

Métodos de encriptación escritos en Python 2.7.10

¿Qué es la criptografía?

La palabra criptografía es un término genérico que describe todas las técnicas que permiten cifrar mensajes o hacerlos intangibles sin recurrir a una acción específica.

La criptografía se basa en la aritmética: En el caso de un texto, consiste en transformar las letras que conforman el mensaje en una serie de números (en forma de bits ya que los equipos informáticos usan el sistema binario) y luego realizar cálculos con estos números para:

- Modificarlos y hacerlos incomprensibles. El resultado de esta modificación (el mensaje cifrado) se llama texto cifrado, en contraste con el mensaje inicial, llamado texto simple.
- Asegurarse de que el receptor pueda descifrarlos.

El hecho de codificar un mensaje para que sea secreto se llama cifrado. El método inverso, que consiste en recuperar el mensaje original, se llama descifrado.

Uso de la criptografía

La criptografía se usa tradicionalmente para ocultar mensajes de ciertos usuarios. En la actualidad, esta función es incluso más útil ya que las comunicaciones de Internet circulan por infraestructuras cuya fiabilidad y confidencialidad no pueden garantizarse. La criptografía se usa no sólo para proteger la confidencialidad de los datos, sino también para garantizar su integridad y autenticidad.

A continuación se mencionan 4 tipos de criptografía.

Mencionaremos primero dos métodos antiguos, El método del cifrado del Cesar, El método de la Excítala, la codificación ASCII y la codificación del código morse son métodos que actualmente se usan con frecuencia.

Python es un lenguaje de programación de alto nivel con una sintaxis muy minimalista que se asemeja bastante a la realización de un pseudocódigo. La primera parte de este documento es una referencia del lenguaje Python.

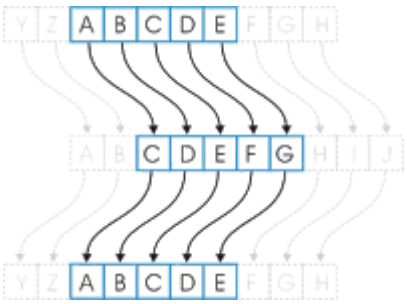
El objetivo es realizar esos métodos mencionados en el lenguaje de programación Python a través de un archivo en txt.

Método del cifrado del Cesar

Es una de las cifras criptográficas más antiguas conocidas hasta el momento, y qué de cierto modo sentó unas bases para que este tema siguiera creciendo a través de la historia, su funcionamiento no es para nada complicado, podríamos decir que es un tanto intuitivo, pero muy eficaz, considerando la época en que fue desarrollado.

Funcionamiento.

Consistía en escribir el mensaje con un alfabeto que estaba formado por las letras del alfabeto latino normal desplazadas tres posiciones a la derecha.



Primero que nada debemos crea las listas que contendrán un alfabeto, que en este caso es el abecedario en minúsculas y mayúsculas.

El receptor del mensaje conocía la clave secreta de éste (es decir, que estaba escrito con un alfabeto desplazado tres posiciones a la derecha), y podía descifrarlo fácilmente haciendo el desplazamiento inverso con cada letra del

mensaje. Pero para el resto de la gente que pudiese accidentalmente llegar a ver el mensaje, el texto carecía de ningún sentido.

Aparentemente es un cifrado muy débil y poco seguro, pero en la época de Julio César no era de conocimiento general la idea de ocultar el significado de un texto mediante cifrado. De hecho, que un mensaje estuviese por escrito ya era un modo de asegurar la confidencialidad frente a la mayoría de la población analfabeta de la época.

Código morse

El código Morse es un código o sistema de comunicación que permite la comunicación telegráfica a través de la transmisión de impulsos eléctricos de longitudes diversas o por medios visuales, como luz, sonoros o mecánicos. Este código consta de una serie de puntos, rayas y espacios, que al ser combinados entre sí pueden formar palabras, números y otros símbolos.

Este sistema de comunicación fue creado en el año 1830 por Samuel F.B. Morse, un inventor, pintor y físico proveniente de los Estados Unidos, quien pretendía encontrar un medio de comunicación telegráfica. La creación de éste código tiene su origen en la creación del señor Morse de un telégrafo, invento que le trajo bastante dificultades, ya que, en un principio, el registro de este fabuloso invento le fue negado tanto en Europa como en los Estados Unidos. Finalmente, logró conseguir el financiamiento del gobierno americano, el que le permitió construir una línea telegráfica entre Baltimore y Washington. Un año después se realizaron las primeras transmisiones, resultando éstas bastante exitosas, lo que dio pie a la formación de una enorme compañía que cubriría a todos los Estados Unidos de líneas telegráficas.

Método del cifrado Escítala.

En siglo V a.c. los lacedemonios, un antiguo pueblo griego, usaban el método de la *escítala* para cifrar sus mensajes. El sistema consistía en una cinta que se enrollaba en un bastón sobre el cual se escribía el mensaje en forma longitudinal

Una vez escrito el mensaje, la cinta se desenrollaba y era entregada al mensajero.

Para enmascarar completamente la escritura es obvio que la cinta en cuestión debe tener caracteres en todo su contorno. Como es de esperar, la llave del sistema residía precisamente en el diámetro de aquel bastón, de forma que solamente el receptor autorizado tenía una copia exacta del mismo bastón en el que enrollaba el mensaje recibido y, por tanto, podía leer el texto en claro.

Este método para cifrar mensajes consiste en cambiar el orden de las letras que componen el mensaje. Es decir las letras son las mismas pero se colocan en diferente orden, no se encuentran colocadas al azar, sino que hay un orden para realizarlo, por lo que es un método de cifrado bastante simple.

Codificación ASCII

El código ASCII (siglas en inglés para American Standard Code for Information Interchange, es decir Código Americano (Estándar para el intercambio de Información).

Este código nació a partir de reordenar y expandir el conjunto de símbolos y caracteres ya utilizados en aquel momento en telegrafía por la compañía Bell. En un primer momento solo incluía letras mayúsculas y números, pero en 1967 se agregaron las letras minúsculas y algunos caracteres de control, formando así lo que se conoce como US-ASCII, es decir los caracteres del 0 al 127.

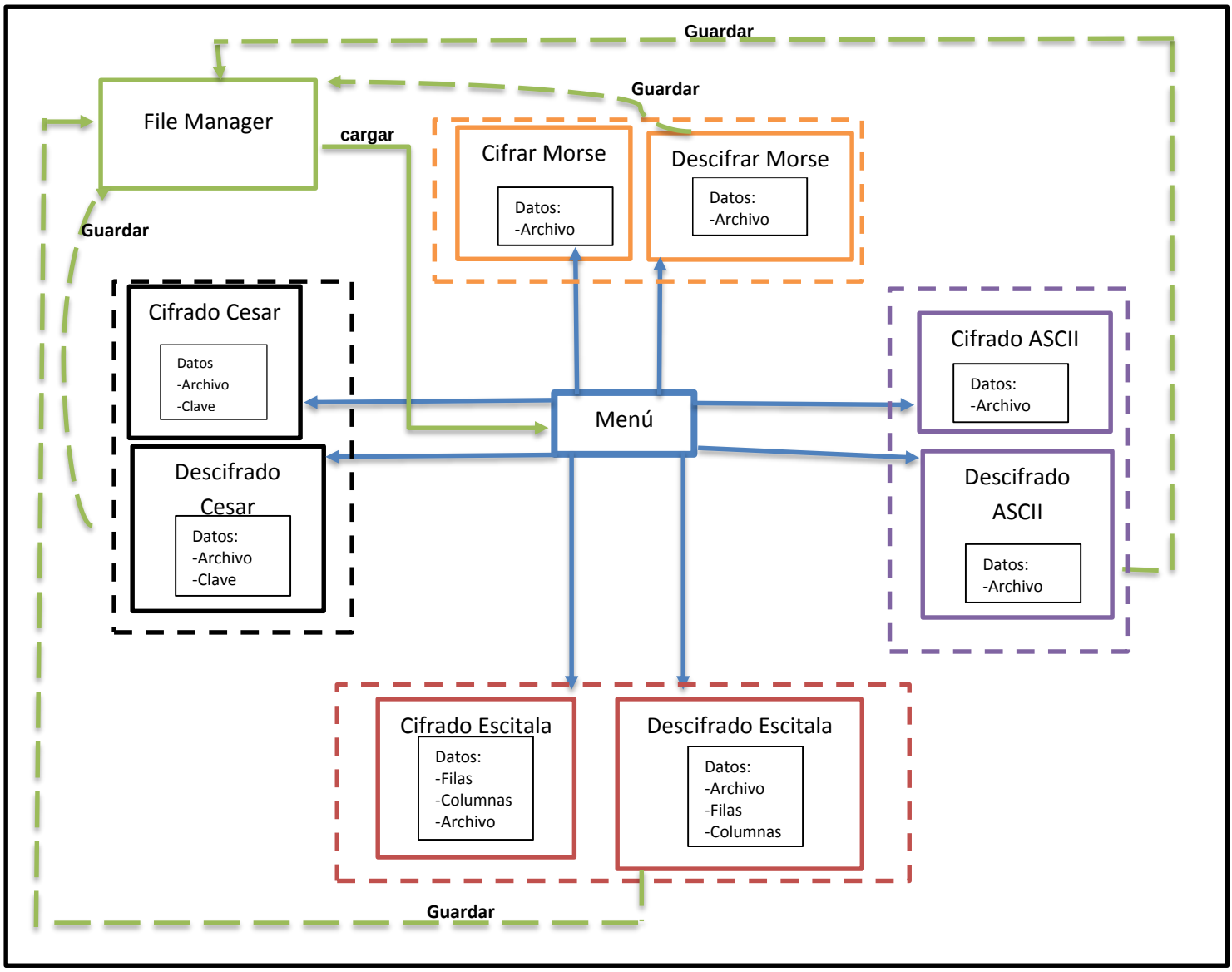
Así con este conjunto de solo 128 caracteres fue publicado en 1967 como estándar, conteniendo todos lo necesario para escribir en idioma inglés.

Casi todos los sistemas informáticos de la actualidad utilizan el código ASCII para representar caracteres, símbolos, signos y textos (273).

Requerimientos

Para poder ejecutar el código necesita el intérprete de Python 2.7.10, que puede descargar desde www.python.org. El intérprete a descargar debe ser acorde a su sistema operativo.

Aplicación de cifrados



Lógica

1. El programa solicita el archivo que contiene el mensaje
2. Se muestra el menú para cifrar, puede escoger todas las opciones de cifrado, ya que el archivo que contiene el mensaje está disponible para todos los cifrados
3. Para descifrar el programa le solicitará la ruta del archivo que desea descifrar y en dado caso, los datos necesarios para el descifrado.

Simbología

- Los recuadros en color naranja contienen el cifrado y descifrado Morse
- Los recuadros en color morado contienen el cifrado y descifrado ASCII
- Los recuadros en color ginda contienen el cifrado y descifrado Escitala
- Los recuadros en color negro contienen el cifrado y descifrado Cesar
- La línea continua color verde, representa la carga del archivo
- La línea punteada color verde, representa la creación y guardado de archivos
- Las líneas color azul, representan las opciones del menú