Presentación

En esta práctica nos familiarizaremos con el lenguaje de programación Python implementando un sistema histórico, concretamente una variante del cifrado de los Cuatro-Cuadrados. Este criptosistema fue propuesto por el criptógrafo francés Félix-Marie Delastelle (1840-1902).

Objetivos

Los objetivos de esta práctica son:

1. Familiarizarse con el entorno de trabajo en Python y el *framework unittest*.
2. Implementar un criptosistema histórico.

Descripción de la Pràctica a realizar

El cifrado de los Cuatro-Cuadrados fue propuesto por el criptógrafo francés Félix-Marie Delastelle (1840-1902). Es un sistema de sustitución poligráfica en el que el tamaño de los bloques de letras a cifrar es de dos carácteres. En la página en inglés de la wikipedia [1] podéis encontrar la explicación detallada del criptosistema, así como de algún ejemplo. En nuestra práctica implementaremos una extensión del modelo que se explica en la wikipedia. En lugar de utilizar matrices de 5x5 para representar el alfabeto, usaremos matrices de 6x6. Esto nos permitirá incluir la 26 letras del alfabeto inglés junto con los 10 dígitos numéricos, del 0 al 9.

Para implementar el cifrado de los Cuatro-Cuadrados dividiremos el trabajo en tres funciones:

1. la generación de la clave,
2. el cifrado de un texto en claro,
3. y el descifrado de un texto cifrado.

Cada uno de los ejercicios corresponde a la programación de una de estas funciones. A continuación, se describen los detalles.

1. Implementación del cifrado de los Cuatro-Cuadrados (10 puntos)

1. Función que implementa la generación de la claves del crifrado de los Cuatro-Cuadrados. (**2 puntos**)

[1] https://en.wikipedia.org/wiki/Four-square_cipher

La función tomará como argumentos las dos palabras que generan las matrices que conforman la clave, y devolverá estas cuatro matrices. El orden en que la función devolverá las cuatro matrices será: superior-izquierda, inferior-izquierda , superior-derecha, inferior-derecha.

- La variable `keyword1` contendrá la palabra usada para construir la matriz superior derecha.
- La variable `keyword1` contendrá la palabra usada para construir la matriz inferior izquierda.
- La función devolverá las cuatro matrices que forman la clave.

Ejemplo:

- `keyword1`: `HELLO5`
- `keyword2`: `WORLD3`
- `salida`: `[[['A', 'B', 'C', 'D', 'E', 'F'], ['G', 'H', 'I', 'J', 'K', 'L'], ['M', 'N', 'O', 'P', 'Q', 'R'], ['S', 'T', 'U', 'V', 'W', 'X'], ['Y', 'Z', '0', '1', '2', '3'], ['4', '5', '6', '7', '8', '9']], [['W', 'O', 'R', 'L', 'D', '3'], ['A', 'B', 'C', 'E', 'F', 'G'], ['H', 'I', 'J', 'K', 'M', 'N'], ['P', 'Q', 'S', 'T', 'U', 'V'], ['X', 'Y', 'Z', '0', '1', '2'], ['4', '5', '6', '7', '8', '9']], [['H', 'E', 'L', 'O', '5', 'A'], ['B', 'C', 'D', 'F', 'G', 'I'], ['J', 'K', 'M', 'N', 'P', 'Q'], ['R', 'S', 'T', 'U', 'V', 'W'], ['X', 'Y', 'Z', '0', '1', '2'], ['3', '4', '6', '7', '8', '9']], [['A', 'B', 'C', 'D', 'E', 'F'], ['G', 'H', 'I', 'J', 'K', 'L'], ['M', 'N', 'O', 'P', 'Q', 'R'], ['S', 'T', 'U', 'V', 'W', 'X'], ['Y', 'Z', '0', '1', '2', '3'], ['4', '5', '6', '7', '8', '9']]]`

2. Función que implementa el cifrado del criptosistema de los Cuatro-Cuadrados. (**4 puntos**)

   La función recibirá como variables de entrada dos parámetros: `message` i `key`; y devolverá el mensaje cifrado.

   - La variable `message` contendrá una cadena de caracteres con el texto en claro a cifrar. La cadena de caracteres podrá contener letras en mayúscula y minúscula y números.
   - La variable `key` contendrá la clave de cifrado, tal como la retorna la función de generación de claves.
   - La función devolverá una cadena de caracteres con el texto cifrado correspondiente al texto en claro.

   Ejemplo:

   - `key`: `[[['A', 'B', 'C', 'D', 'E', 'F'], ['G', 'H', 'I', 'J', 'K', 'L'], ['M', 'N', 'O', 'P', 'Q', 'R'], ['S', 'T', 'U', 'V', 'W', 'X'], ['Y', 'Z', '0', '1', '2', '3'], ['4', '5', '6', '7', '8', '9']], [['W', 'O', 'R', 'L', 'D', '3'], ['A', 'B', 'C', 'E', 'F', 'G'], ['H', 'I', 'J', 'K', 'M', 'N'], ['P', 'Q', 'S', 'T', 'U', 'V'], ['X', 'Y', 'Z', '0', '1', '2'], ['4', '5', '6', '7', '8', '9']], [['H', 'E', 'L', 'O', '5', 'A'], ['B', 'C', 'D', 'F', 'G', 'I'], ['J', 'K', 'M', 'N', 'P', 'Q'], ['R', 'S', 'T', 'U', 'V', 'W'], ['X', 'Y', 'Z', '0', '1', '2'], ['3', '4', '6', '7', '8', '9']], [['A', 'B', 'C', 'D', 'E', 'F'], ['G', 'H', 'I', 'J', 'K', 'L'], ['M', 'N', 'O', 'P', 'Q', 'R'], ['S', 'T', 'U', 'V', 'W', 'X'], ['Y', 'Z', '0', '1', '2', '3'], ['4', '5', '6', '7', '8', '9']]]`

- `message`: CRYPTOGRAPHY
- `salida`: AJOHTIIHOHBY

3. Función que implementa el proceso de descifrado del criptosistema de los Cuatro-Cuadrados. (**4 puntos**)

   La función tomará como variables de entrada dos parámetros: `ciphertext` i `key`; y devolverá el texto en claro.

   - La variable `ciphertext` contendrá una cadena de caracteres con el texto cifrado. La cadena de caracteres podrá contener letras en mayúscula y minúscula y números.
   - La variable `key` contendrá la clave de cifrado, tal y como la retorna la función de generación de claves.
   - La función devolverá una cadena de caracteres con el texto en claro correspondiente al texto cifrado.

   Ejemplo:

   - `key`: `[[['A', 'B', 'C', 'D', 'E', 'F'], ['G', 'H', 'I', 'J', 'K', 'L'], ['M', 'N', 'O', 'P', 'Q', 'R'], ['S', 'T', 'U', 'V', 'W', 'X'], ['Y', 'Z', '0', '1', '2', '3'], ['4', '5', '6', '7', '8', '9']], [['W', 'O', 'R', 'L', 'D', '3'], ['A', 'B', 'C', 'E', 'F', 'G'], ['H', 'I', 'J', 'K', 'M', 'N'], ['P', 'Q', 'S', 'T', 'U', 'V'], ['X', 'Y', 'Z', '0', '1', '2'], ['4', '5', '6', '7', '8', '9']], [['H', 'E', 'L', 'O', '5', 'A'], ['B', 'C', 'D', 'F', 'G', 'I'], ['J', 'K', 'M', 'N, 'P', 'Q'], ['R', 'S', 'T', 'U', 'V', 'W'], ['X', 'Y', 'Z', '0', '1', '2'], ['3', '4', '6', '7', '8', '9']], [['A', 'B', 'C', 'D', 'E', 'F'], ['G', 'H', 'I', 'J', 'K', 'L'], ['M', 'N', 'O', 'P', 'Q', 'R'], ['S', 'T', 'U', 'V', 'W', 'X'], ['Y', 'Z', '0', '1', '2', '3'], ['4', '5', '6', '7', '8', '9']]]`
   - `ciphertext`: AJOHTIIHOHBY
   - `salida`: CRYPTOGRAPHY

Criterios de valoración

Formato y fecha de entrega

La puntuación de cada ejercicio se encuentra detallada en el enunciado.

Por otro lado, es necesario tener en cuenta que el código que se envíe debe contener los comentarios necesarios para facilitar su seguimiento. En caso de no incluir comentarios, la corrección de la práctica se realizará únicamente de forma automática y no se proporcionará una corrección detallada. No incluir comentarios puede ser motivo de reducción de la nota.

La fecha máxima de envío es el **14/10/2019** (a las 24 horas).

Junto con el enunciado de la práctica encontrareis el esqueleto de la misma (fichero con extensión .py). Este archivo contiene las cabeceras de las funciones que hay que implementar para resolver la práctica. Este mismo archivo es el que se debe entregar una vez se codifiquen todas las funciones.

Adicionalmente, también os proporcionaremos un fichero con tests unitarios para cada una de las funciones que hay que implementar. Podeis utilizar estos tests para comprobar que vuestra implementación gestiona correctamente los casos principales, así como para obtener más ejemplos concretos de lo que se espera que retornen las funciones (más allá de los que ya se proporcionan en este enunciado). Nótese, sin embargo, que los tests no son exhaustivos (no se prueban todas las entradas posibles de las funciones). Recordad que no se puede modificar ninguna parte del archivo de tests de la práctica.

La entrega de la práctica constará de un único fichero Python (extensión .py) donde se haya incluido la implementación.