IIC3253-2019/1 - Criptografía y Seguridad Computacional
Depto. de Ciencia de la Computación
Pontificia Universidad Católica de Chile
Tarea 1

Profesor: Tomás Barros

Fecha de Entrega: 15/4/2019

Se le pide implementar un software en Python que permita deducir la llave utilizada y descifrar texto cifrado con una máquina de enigma que tiene las siguientes características:

- Sólo usa las 26 letras del alfabeto inglés,
- No usa patch panel,
- Tiene un reflector con el siguiente mapa de letras:

```
a <-> b, o <-> p
c <-> d, q <-> r
e <-> f, s <-> t
g <-> h, u <-> v
i <-> j, W <-> x
k <-> l, y <-> z
m <-> n
```

- Puede usar entre uno y 6 discos. La lógica es la vista en clases, cada vez que se presiona una tecla, el disco de más a la derecha se gira en una posición. Cuando un disco completa una vuelta, hace rotar un espacio aquél disco inmediatamente a su izquierda (al mismo tiempo, es decir cuando avanza el espacio para volver a la posición original, avanza un espacio el de la izquierda en conjunto),
- No tiene ninguna información de cómo están construidos los posibles discos, pueden tener cualquier configuración.

El software debe leer, desde un archivo con codificación UTF-8, los textos a descifrar. Vendrán uno por línea y en orden ascendente para la cantidad de discos utilizados. Cada línea tiene un dígito indicando el número de discos que se utilizó, un espacio, y a continuación el texto cifrado. Además todos los textos originales (antes de cifrar) empiezan con la palabra `hola`.

Para cada línea, su software debe entregar la llave (es decir la configuración de los discos y la posición inicial) y el texto descifrado.

Su tarea se ejecutará durante 5 minutos. Si logra romper un cifrado de dos discos, logrará un 6 en la nota. Luego, se ordenarán de mayor a menor las tareas según cuántos textos logró descifrar en esos 5 minutos y se distribuirá un punto más en proporción a la cantidad de textos descifrados. Las tareas que logren descifrar más líneas, obtendrán un 7.

Su tarea debe tener un README comprensible de cómo se ejecuta. La calidad del código también será evaluada (nombres de variables, comentarios, coherencia... en resumen, siga las recomendaciones en https://www.python.org/dev/peps/pep-0008/) y podrá generarle que su nota disminuya o aumente según sea el caso.

Reglas de entrega:

- La tarea es **individual**, la copia no será tolerada.
- La entrega será hasta las 23:59:59 del viernes 15/4/2019. **No hay atrasos, no habrá prórroga**
- Una tarea que no compila tiene automáticamente un 1.