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: 29/4/2019

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 más coma (,) y espacio ( ),
- 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.

Suponiendo que existen sólo 6 discos, se le entrega un archivo (quijote_misma_llave.txt) con texto plano (codificación UTF-8) y su equivalente cifrado con la máquina enigma. En cada línea se le indica que discos usó, el texto plano y el texto cifrado (separados por ;). Por ejemplo, la línea:

```
[2,1];la lengua queda y los ojos listos;msorpssjekozztjqlyjjmnwqhzuczochl
```

Quiere decir que se cifró con los discos 1 y 2, con el 1 más a la derecha (es decir, el que gira cada vez que se presiona una tecla y que está junto al reflector) el texto `la lengua queda y los ojos listos` y se obtuvo como cifrado el texto `msorpssjekozztjqlyjjmnwqhzuczochl`

Su software debe deducir/encontrar la mayor parte de las configuraciones de los discos.Su tarea se ejecutará durante 5 minutos (todas las tareas se ejecutarán en la misma máquina).

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 29/4/2019. **No hay atrasos, no habrá prórroga**
- Una tarea que no compila tiene automáticamente un 1.