Práctica 1

Facultad de Ciencias
XOR, César y Afín

José de Jesús Galaviz Casas
galaviz@ciencias.unam.mx

Edgar Omar Arroyo Munguía
omar.am@ciencias.unam.mx

Luis Fernando Yang Fong Baeza
fernandofong@ciencias.unam.mx

29 de Enero 2020

1. Cifrado XOR

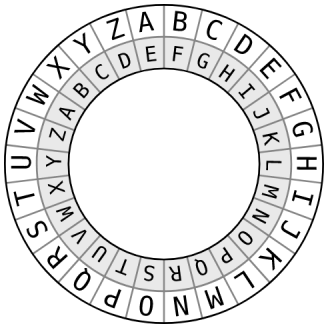
Para cifrado, consta de aplicar una operación *XOR* a todos los bits del mensaje, preservando el orden entre los bits pero sin importar a quién se le aplique primero la operación, de manera que supongamos que tengo el mensaje a enviar: `HOLA`, cada caracter corresponde a un número para la computadora, entonces, este mensaje cifrado bajo `XOR`, se ve como `INM@`, el trabajo de la práctica es implementar en el script *XOR_cypher.py* el constructor y las funciones de cifrado y descifrado para pasar las pruebas en el script *XOR_test.py*

a	b	$\oplus$
0	0	0
0	1	1
1	0	1
1	1	0

2. Cifrado César

En el script *caesar_cipher.py*, encontrarán una clase llamada *Caesar* que consta de únicamente 3 métodos, el constructor, el algoritmo de cifrado y decifrado, todos vacíos, la práctica consiste en completar los tres métodos programando los dos algoritmos correctos. Como el cifrado césar depende del alfabeto, éste es un atributo de clase y sobre la longitud de éste se debe de hacer la aritmética modular.

Para éste único cifrado, se considerarán casos extra, con una bandera que indica si hay que ignorar espacios o no, sin embargo, si el espacio es parte del alfabeto, no modifica el algoritmo de cifrado.



3. Cifrado Afín

Por último en el script de *affine_cipher.py* deberán programar el cifrado afín, este cifrado no se prueba tan meticulosamente, basta con entender el algoritmo y programarlo aunque las funciones auxiliares que implementen, deberán ir escritas en el script *utils.py* para una mejor limpieza del código.

$$\begin{aligned}
\mathrm{D}(\mathrm{E}(x)) &= a^{-1}(\mathrm{E}(x) - b) \bmod m \\
&= a^{-1}(((ax + b) \bmod m) - b) \bmod m \\
&= a^{-1}(ax + b - b) \bmod m \\
&= a^{-1}ax \bmod m \\
&= x \bmod m.
\end{aligned}$$

La fecha límite de entrega para la práctica es el 05 de Febrero del 2020 antes de las 23:59:59.