Criptografía y seguridad
Tarea 1: Readme

Andrea Itzel González Vargas
Carlos Gerardo Acosta Hernández

Entrega: 15/02/17
Facultad de Ciencias UNAM

En el archivo de nombre *bytes.py* (ubicado en un directorio superior a este), se encuentra el código fuente del primer ejercicio de esta tarea.

Para la realización de esta sección práctica utilizamos **Python 3**, por lo que es muy importante utilizar el intérprete de dicha versión y no su antecesor para que el programa funcione como esperamos.

Decidimos seguir la sintáxis propuesta en los lineamientos para la ejecución del programa. Una ejecución debe verse entonces como:

```
$ python3 bytes.py <archivo1> <archivo2>
```

Siendo el nombre de los archivos -expresados con una ruta relativa al directorio actual o una absoluta- argumentos forzosos para la operación del programa.

Al término de la ejecución, podremos encontrar dos archivos "nuevos" (si se está ejecutando una segunda vez, se sobreescribirán los anteriores) resultantes, además del archivo del programa y los de entrada (esto sólo en caso de que los mantengamos en ese mismo directorio). El resultado del inciso *a)* tendrá por nombre, tal como fue especidicado, **xor.out**, mientras que el inciso *b)* será identificado como **multiplicacion.out**.

```
tarea1/
|__ archivo_A.in
|__ archivo_B.in
|__ bytes.py
|__ multiplicacion.out
|__ xor.out
```

Comentarios

Luego de considerar funcional nuestro programa, decidimos hacer uso de las pruebas que se nos compartieron en el "Google Classroom" del curso. Nos encontramos con algunas incongruencias entre los resultados que obteníamos y los resultados que eran señalados como los correctos.

Específicamente en el caso de la multiplicación (inciso *b)*), se trataba de unos cuantos bytes resultado que no coincidían con nuestras ejecuciones. No tan extrañados de esto y atribuyéndolo a un posible error de implementación, revisamos nuestro código sin encontrar nada significativo y haciendo adecuaciones ajenas al hallazgo.

Fue entonces que nos dimos a la tarea de hacer a mano la multiplicación y reducción de un par de esos bytes desiguales y descubrimos que nuestro algoritmo ofrecía un resultado correcto. Ya no estamos seguros del problema existente en este ejercicio y nuestro plazo de entrega está llegando a su fin, pero esperamos poder aclararlo próximamente.