Práctica 3
Facultad de Ciencias
Criptografía y Seguridad

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

12 de Febrero 2020

1. Criptoanálisis

Se les darán textos planos escritos en un formato *.txt* y deberán aplicar las técnicas de criptoanálisis correspondientes para lograr descifrar los textos, no necesariamente se deberá de resolver mediante programación, aunque deberán de explicar en un PDF el procedimiento, sin necesidad de poner las cuentas, simplemente qué fue usado, qué prueba y en qué sentido (Ataque de fuerza bruta, Prueba de Kasiski...).

Se asegura que todos los *archivos.txt*, fueron cifrados con los algoritmos ocupados de las dos prácticas anteriores, todos escritos en el idioma español (mod 27).

La fecha de entrega para ésta práctica es de 2 semanas, sin embargo deberán entregar cuál fue la llave que fue usada para cifrar cada texto correspondiente.

2. Información de los textos

Los textos son textos populares, diseñados para que en cuanto rompan una parte del texto, de manera casi inmediata logren romper el resto del texto sabiendo de qué trata el texto, buscando poemas, letras famosas e incluso dichos más que populares, además tendrán que resolver las congruencias para lograr decifrar todos los mensajes. Como se especifica arriba, se usaron 4 cifrados:

1. César $c \equiv m + k \mod N$
2. Afín $c \equiv k_1 m + k_2 \mod N$
3. Hill $\overline{c} \equiv A\overline{m} \mod N$
4. Vigenere $c \equiv x_i + m \mod N$

Parte del trabajo de la práctica es identificar qué cifrado se usó con cual.

Cada cifrado tiene su respectiva llave, de manera que otro objetivo de la práctica es que logren obtener las respectivas llaves de cada cifrado, expresado como se debe y fue visto en clase.

Se deberá entregar todos los archivos que se hayan programado y los que hayan sido herramientas externas, especificados en el README de la práctica además de los correspondientes textos decifrados.

3. Punto extra

Esta práctica cuenta con un punto extra, el archivo *Five.txt* fue cifrado de una manera distinta, aunque a simple vista parezca un texto descifrado, en realidad cuenta con un mensaje oculto, el objetivo de este texto es que encuentren el mensaje oculto dentro del texto y adjuntarlo en el README.