Instituto Tecnológico y de Estudios Superiores de Monterrey

Actividad 2.1. Cifrado César, sustitución monoalfabética y Vigenère

Juan Pablo Echeagaray González

A00830646

Análisis de Criptograrfía y Seguridad

MA2002B.300

Dr.-Ing. Jonathan Montalvo-Urquizo

26 de mayo del 2022

1. Sobre el cifrado César

El cifrado de César fue el más sencillo de implementar de todos los métodos vistos, su tiempo de encriptado y desencriptado (aún sin conocer la llave) es mínusculo a comparación de los demás. La única barrera encontrada es la incertidumbre del lenguaje original del *plaintext*. Para la implementación sugerida solamente se toman en cuenta caracteres de lenguas romances, lo cual no nos asegura poder realizar un proceso de criptoanálisis en una situación general.

El proceso de encriptado y desencriptado con una llave conocida le tomó a la máquina de prueba un promedio de $21\mu s$; cuando no disponía de una llave se realizó un ataque por fuerza bruta, el tiempo de desencriptado incrementó a $278\mu s$. El incremento de tiempo no es tan grande porque solamente se deben de probar un total de 26 diferentes llaves para desencriptar el mensaje; al final de este proceso se necesita de un ser humano que rectifique los resultados.

2. Sobre el cifrado monoalfabético

El cifrado monoalfabético es mucho más fuerte que un simple cifrado César, se pasa de un espacio de n posibles llaves a $n!$, un espacio que tiene un tamaño de al menos 25 ordenes de magnitud superior cuando solamente se tiene un alfabeto consistente de letras.

Enumerar todas las posibles llaves e intentar desencriptar el mensaje podría ser una solución factible en equipos con un mayor poder de cómputo; sin embargo, una aproximación por fuerza bruta de ese estilo no es necesario para romper este cifrado. Dado que este método sigue siendo una simple sustitución, podemos hacer uso de herramientas estadísticas para encontrar el mensaje original, de forma más específica, se realiza un *análisis de frecuencias*.

Suponiendo que el criptoanalista conozca el lenguaje original del *plaintext*, este puede comenzar el proceso de desencriptado al analizar la frecuencia relativa de cada caracter dentro del *ciphertext*; después se pueden comparar estas frecuencias con algunas tablas de frecuencias de letras en el lenguaje a tratar. En la primera iteración se pueden remplazar las primeras n letras más frecuentes del *ciphertext* con las n primeras letras más frecuentes de las tablas conocidas.

Después de esta iteración se analiza el texto, con la esperanza de que esta sustitución torne más legibles algunas secciones del *ciphertext*. De aquí, se puede ir determinando de forma empírica las sustituciones a realizar, por ejemplo, si uno encuentra después de la primera iteración el texto *tha* y se sabe que el texto original está escrito en inglés, se propone la sustitución $a \to e$.

Este método tomó más tiempo de implementar y romper que el anterior, pero se tornó bastante sencillo de romper una vez que se conocían los remplazos adecuados. Este caso de estudio fue más sencillo de resolver dada la longitud del texto original de alrededor de $48,000$ caracteres

3. Sobre el cifrado Vigenère