Práctica 2 de Criptografía y Computación

Carlos Núñez Molina
Alessandro Zito
Gabriela Antolinez

1 Cifrado de Vigenére

Primero desciframos el texto cifrado mediante el **Cifrado de Vigenére**. Para ello usamos el método del **Índice de Coincidencia**.

Empezamos calculando el índice de coincidencia de todos los textos cifrados, del 1 al 5. Los índices obtenidos, en orden, son: 0.091, 0.064, 0.063, 0.032, 0.066. Sabemos que el índice de coincidencia medio de los textos en español es de 0.07. Como de todos los cifrados usados solo el de Vigenére cambia el índice de coincidencia del texto original, reduciéndolo al uniformizar las frecuencias de aparición de las distintas letras, sabemos que de todos los textos solo el número 4 ha sido cifrado con Vigenére, al tener un índice de coincidencia de 0.032.

Acto seguido, calculamos la longitud de la clave usada. Para ello, vamos iterando desde $n = 2$ en adelante, dividiendo el texto en sucesivas partes, pegando "saltos" de n letras y calculando el índice de coincidencia de todas estas partes, hasta que todos valgan alrededor de 0.07. Cuando $n = 12$, todas las subcadenas obtenidas tienen un índice de coincidencia alrededor de 0.07, por lo que sabemos que la clave debe ser de longitud 12.

Así, procedo a dividir el texto en las subcadenas correspondientes a dar saltos para $n = 12$ y les aplico un análisis de frecuencias como si cada subcadena hubiera sido cifrada con el Cifrado de Cesar. Las claves obtenidas (correspondientes al número de desplazamientos) son: 18, 4, 13, 0, 2, 8, 12, 8, 4, 13, 20, 15. Al concatenarlas y asociarles su letra correspondiente, obtenemos la clave ***RENACIMIENTO***.

Esta es la clave usada para cifrar el texto 4 con el Cifrado de Vigenére, y con la que podemos descifrar el texto. Para ello, obtenemos la *clave inversa*, es decir, la clave con la que, al cifrar el texto cifrado de nuevo con Vigénere, obtenemos el texto original. Esta clave se obtiene aplicando, para cada letra, los desplazamientos de Cesar en sentido contrario y es: *JWÑAYSOSWÑHM*.

2 Cifrado Escítalo

Por segundo, intentaremos a descifrar los textos mediante el **Cifrado de Escítalo**. Utilizamos la función **Análisis de Frecuencia**. Hacemos el análisis de frecuencia de todos los textos. Podemos ver que en el *texto 3* el análisis de frecuencia es parecida a la de un texto bastante largo escrito en español. Entonces, seguramente el texto será cifrado con Escítalo, porqué este tipo de encriptación no cambia el análisis de frecuencia de un texto. Después de hacer esto, ententamos iterando desde 2 hasta usando la fuerza bruta hasta que hemos descifrado el mensaje, y hacemos esto con la función *transposicion*. El numero que sale es $n = 23$.

3 Cifrado de Cesar

Luego, se descifraron los textos que se encontran cifrados con **Cifrado de Cesar** para lo cual se evaluaron las **frecuencias** de los textos. Así, evidenciamos que en el *texto 1* la letra más frecuente es la V con 25.636 por cien, seguida de la letra Z con 7.872 y la letra Ñ con 6.848; en el *texto 2* las letras mas frecuentes son la L con 12.59 por cien y la O con 11.836 por cien. Teniendo en cuenta que las letras más frecuentes en el español son la A y la E, identificamos que éstas se encuentran en la misma distancia entre sí que las letras *V y Z* y las letras *L y O* dado que en ambos casos hay 4 saltos. Por tanto se evalua que los textos fue cifrado con Cesar donde el número de saltos corresponde a 21 en el primer texto1 a 7 en el texto2, lo cual se logró comprobar al realizar la respectiva sustitución por cada letra llegando a descifrar los textos.