Seguridad y protección de sistemas informáticos
Grado en Ingeniería Informática y Matemáticas
Universidad de Granada

Cifrado de Vigenère

Víctor Rebollo Pérez

11 de octubre de 2016

Índice

1. Calcular la longitud de la clave.

El cálculo de la longitud de la clave se ha realizado mediante los dos métodos propuestos

- **Método de Kasinski**. Consiste en buscar cadenas repetidas en el criptograma. Se ha implementado este método en lenguaje c++. Se encuentra en el archivo `kasinski.cpp`
- **Índice de coincidencia de Friedman**. Método de fuerza bruta en el cual hacemos un análisis de los índices de cada columna para diferentes tamaños de contraseña. La longitud de la clave será aquella en la que todas las columnas tengan un IC elevado. Se ha implementado en lenguaje c++. Se encuentra en el archivo `frecuencial.cpp`

2. Emplear análisis de frecuencias para descifrar el texto y calcular la clave.

Para desencriptar el texto seguimos los siguientes pasos.

- Colocamos el texto en tantas columnas como la longitud de la contraseña.

  A continuación, realizamos un análisis de frecuencia en cada una de las columnas. Con esto obtenemos para la primera columna:

  C E

  M A

  Y O

  Q S

  ...

  Donde los elementos de la primera y segunda columna son las letras más frecuentes en la columna y en el español respectivamente (en orden decreciente).

- Para conseguir la clave seguimos el siguiente razonamiento. El primer elemento del texto encriptado es una C. Según los análisis, en la columna 0 la C podría ser equivalente a la E. En caso de no serlo, sería una letra próxima en frecuencia como la A o la O.

  Seguimos este razonamiento a base de prueba y error hasta obtener la siguiente contraseña **YMGDAFM**.

- Una vez tenemos la contraseña es sencillo desencriptar el texto. Para ello, solo debemos aplicar la siguiente formula

  $D(C_i) = C_i - K_i + 1 \text{ mod(L)}$

Donde C_i es el caracter i del texto encriptado y K_i el elemento de la contraseña que le corresponde a C_i

Los resultados completos del análisis de frecuencias así como el texto desencriptado se encuentran en `resultado.txt`. Obtenido mediante `desencriptar.cpp`

3. Cada texto es un capítulo de un libro famoso. Averiguad el libro y el capítulo.

Con una busqueda simple obtenemos que el texto desencriptado pertenece a **El Quijote**, en particular al **Capítulo VI**