Pràctica 1 Cripto

Alberto Martino Arias

Ejercicio 1: Análisis de frecuencia y descifrado César

1. Objetivo: Analizar un texto cifrado con un cifrado César y proponer las claves más probables mediante análisis de frecuencias.

2. Metodología:

    - Limpiamos el texto dejando sólo letras para el conteo de frecuencias.

    - Contamos cuántas veces aparece cada letra usando `Counter`.

    - Identificamos la letra más frecuente en el texto cifrado.

    - Comparamos con las letras más frecuentes del inglés (`ETAOIN`) y calculamos el desplazamiento correspondiente para cada suposición.

    - Desciframos el texto para cada posible clave usando la función `caesar_decrypt`.

3. Resultado: Se generaron varias posibles claves y se pudo observar cuál descifrado se acercaba a un texto legible en inglés.

Ejercicio 2: Sustitución simple y homófona

1. Objetivo: Implementar y analizar dos tipos de cifrado:
    - Substitución simple: cada letra se reemplaza por otra del alfabeto según una permutación.
    - Substitución homófona: cada letra puede representarse por múltiples símbolos para dificultar el análisis de frecuencias.
2. Metodología:
    - Limpiamos el texto dejando sólo letras y mayúsculas.
    - Para la substitución simple, se generó una permutación aleatoria del alfabeto y se reemplazaron las letras.
    - Para la substitución homófona, se asignaron varios símbolos a las letras más frecuentes y uno o más símbolos a las demás.
    - Se implementó una función de análisis de frecuencias para ambos cifrados y se comparó la distribución de caracteres.
3. Resultado:
    - Se obtuvieron textos cifrados para ambos métodos.
    - La substitución simple mantiene un patrón más fácil de descifrar por frecuencia, mientras que la homófona difumina las frecuencias, dificultando el ataque por frecuencia.

Ejercicio 3: Descifrado de Vigenère con análisis de frecuencia

1. Objetivo: Descifrar un texto cifrado con Vigenère, estimando la longitud de la clave y utilizando análisis de frecuencias.

2. Metodología:

    - Limpiamos el texto dejando sólo letras para análisis.

    - Calculamos la longitud probable de la clave usando el índice de coincidencia (mide la probabilidad de que dos letras sean iguales en posiciones desplazadas).

    - Para cada posición de la clave, se identificaron las letras más frecuentes en cada subalfabeto.

    - Se generaron combinaciones posibles de claves basadas en las letras más frecuentes en catalán (`a, e, i, o, s, r, n, t, l, u`).

    - Se descifraron los textos conservando espacios y saltos de línea originales para mantener la legibilidad.

    - Se puntuó cada clave según cuántas letras coinciden con las frecuentes en catalán y se seleccionaron las más probables.

3. Resultado:

    - Se generaron varias claves candidatas y se descifró el texto completo.

    - La presentación final mantiene la estructura del texto original y permite inspeccionar rápidamente la legibilidad.

Universitat de Lleida

Ejercicio 4: Estimación de tiempo de ataque por fuerza bruta

Objetivo: Estimar el tiempo que tomaría un ataque por fuerza bruta para diferentes tipos de cifrado.

(a) Sustitución simple sobre 26 letras

- Una sustitución simple permuta las 26 letras del alfabeto.
- Número de claves posibles: 26! (factorial de 26).

$$26! \approx 4.03 \times (10^{26}) \text{ claves}$$

Si el ordenador prueba 10^6 claves:

Tiempo en segundos = $(4.03*(10^{26}))/(10^6) = 4.03*(10^{20})$ segundos

Convertimos a años:

Tiempo en años = $(4.03*(10^{20}))/(3.15*(10^7)) = 1.28*(10^{13})$ años

➡ Esto es imposible.

(b) Permutación simple con bloques de longitud 10

- Si tenemos bloques de 10 elementos y permutamos, número de claves: 10! 3.628.800 = $3.63*10^6$

- Con un ordenador que prueba 10^6 claves:

  Tiempo en segundos = $(3.63*(10^6))/(10^6) = 3.63$ s

- Muy rápido: menos de 4 segundos.

(c) Vigenère con clave de longitud k

- Vigenère usa un alfabeto de 26 letras y una clave de longitud k.

- Número de claves posibles: 26^k

- Tiempo estimado en segundos:

  Tiempo (s) = $(26^k)/(10^6)$

➡ El tiempo crece exponencialmente con la longitud de la clave.

Resumen aproximado con 1 millón de claves

Método	Número de claves	Tiempo estimado
Sustitución simple (26 letras)	4.03*10^26	1.28*10^13 años
Permutación bloques 10	3.63*10^6	3.6 s
Vigenère longitud 5	1.19*10^7	12 s
Vigenère longitud 10	1.41*10^14	4.5 años
Vigenère longitud 20	2*10^28	6.35*10^14 años