COLOMBIA POTENCIA DE LA VIDA

TIC

Misión 2

Lección 3:
Taller de cifrado

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira

Taller de cifrado

Tiempo de ejecución: 6 horas

Planteamiento de la sesión:

En este taller se aplicarán los conceptos vistos de criptografía, está diseñado para emplear varios algoritmos de cifrado y que el estudiante conozca cómo se implementan en un sistema de cómputo.

Como segundo objetivo se introducirá el concepto de análisis criptográfico, realizando un ejercicio que intentará romper el cifrado de Vigenère (cifrado indescifrable) con el fin de estudiar las debilidades que pueden tener los algoritmos de cifrado.

Desarrollo de la sesión

Parte 1: Ejercicios de cifrados por sustitución (2 horas).

1. Escriba un programa en Python que, a partir de un texto cree una tabla base de cifrado Delastelle (puede ser bífido o trífido)

2. Desarrolle funciones para codificar un mensaje a partir de la tabla de cifrado creada en el punto 1.

3. Cree una función que permita decodificar el mensaje teniendo el mismo texto de entrada de la función 1. Se pueden emplear las funciones ya desarrolladas para facilitar el trabajo.

Parte 2: Análisis criptográfico (4 horas).

El criptoanálisis es el estudio de los sistemas de cifrado con el objetivo de vulnerar su seguridad (romper un cifrado) sin tener acceso a la clave secreta que se empleó para cifrar la información. Una de las técnicas más empleadas y que permite romper ciertos cifrados es el análisis de frecuencias, el cual, consiste en crear histogramas de las repeticiones de las letras para descifrar un mensaje encriptado.

Como se estudió en la lección 1, existen cifrados por sustitución los cuales, dependen de reorganizar el alfabeto y reemplazar las letras con el nuevo orden alfabético. Esto hacía más complejo de romper un cifrado en comparación con el algoritmo de César.
En este taller se estudiará el análisis de frecuencias para realizar la ruptura del cifrado por sustitución monoalfabético. Para esto se escogerá un alfabeto personalizado, por ejemplo

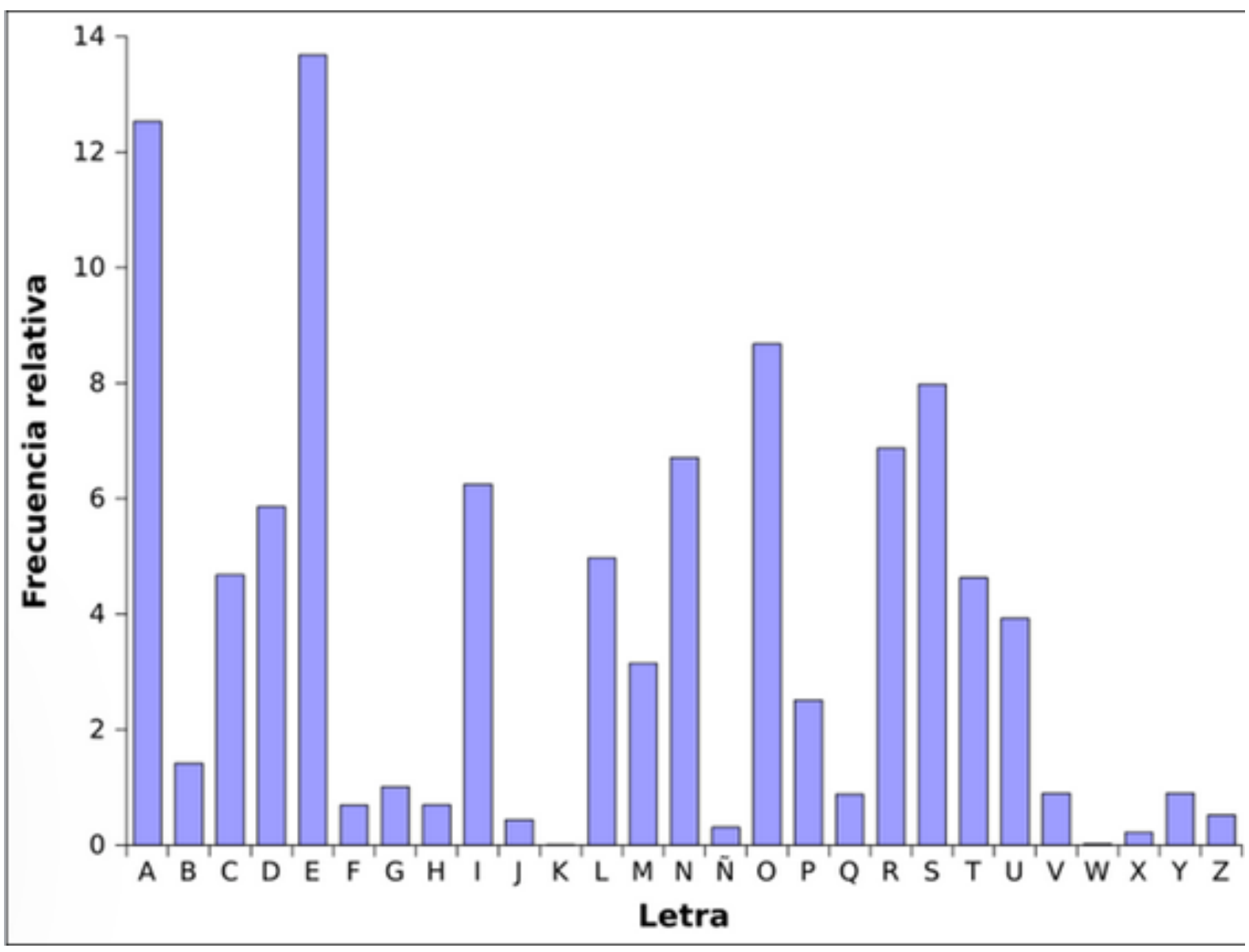
Murcielagobdfhjknñpqstvwxyz

Y procederemos a sustituir en un texto con este cifrado.

Ejercicios en clase:

1. Crear una función que permita realizar la sustitución de un texto con el nuevo alfabeto para codificar un texto.
2. Escoger un texto de, al menos, 3000 palabras para codificarlo con el método descrito
3. Escoger un alfabeto personalizado (reordenado) y codificar el mensaje. Se puede hacer en grupos de estudiantes, cada grupo entregará a otro grupo el mensaje cifrado solamente, sin darle pistas de la forma en la que ordenaron los textos.
4. Una vez los grupos tengan el texto cifrado, procederán a estudiar las frecuencias, esto es, crear un programa (pueden utilizarse bibliotecas como numpy) que tomen el texto y calculen cuantas veces aparece cada letra. Posteriormente deben graficar el histograma de apariciones de las letras.
5. Realizar el mismo procedimiento del numeral 4 sobre el texto propio y descargar de internet el histograma de frecuencias del idioma español, por ejemplo, se puede emplear el de Wikipedia en el link:

https://es.wikipedia.org/wiki/Frecuencia_de_aparici%C3%B3n_de_letras



6. Ordenar los dos histogramas de mayor a menor en orden de aparición y comparar los histogramas. Con base en la comparación, reemplace las letras según las frecuencias y valide si el texto pudo ser descifrado.

En caso de que aun no sea descifrado el texto, repita reordenando frecuencias, puede emplear las frecuencias de otros textos publicados y previamente analizados como el quijote, la regenta (todos disponibles en el link de Wikipedia)