Implementación de algoritmos de transposición y sustitución

Algoritmo sustitución

Cifrado Polybios

Este cifrado fue realizado en la antigua Grecia y usaba el alfabeto griego en su versión original, aunque se ha adaptado a los demás alfabetos. Se basa en colocar las letras del alfabeto en una matriz, normalmente de 5×5, y en las cabeceras de las columnas y filas se le asigna unos números o letras siguiendo un patrón preestablecido por el usuario del cifrado.

Un cuadrado de Polibio es una tabla que permite a alguien convertir letras en números. Para que el cifrado sea un poco más difícil, esta tabla se puede aleatorizar y compartir con el destinatario. Para encajar las 26 letras del alfabeto en las 25 celdas creadas por la tabla, las letras 'i' y 'j' generalmente se combinan en una sola celda. Originalmente no había tal problema porque el alfabeto griego antiguo tiene 24 letras.

In [1]:

```
# Python Program to implement polybius cipher
#Codigo basado en https://www.geeksforgeeks.org/polybius-square-cipher/
# function to display polybius cipher text

def polybiusCipher(s):
    # convert each character to its encrypted code
    for char in s:
        # finding row of the table
        row = int((ord(char) - ord('a')) / 5) + 1
        # finding column of the table
        col = ((ord(char) - ord('a')) % 5) + 1
        # if character is 'k'
        if char == 'k':
            row = row - 1
            col = 5 - col + 1
        # if character is greater than 'j'
        elif ord(char) >= ord('j'):
            if col == 1 :
                col = 6
                row = row - 1
            col = col - 1
        print(row, col, end ='', sep ='')


if __name__ == "__main__":
    s = "amadogarciarosales"
    polybiusCipher(s)
```

```
1132111434221142132411423443113115 43
```

Algoritmo transposición

Cifrado de transposición columnar

El Cifrado de Transposición en Columnas es una forma de cifrado de transposición al igual que el Cifrado de Valla de Ferrocarril. La transposición en columnas implica escribir el texto sin formato en filas y luego leer el texto cifrado en columnas una por una.

En un cifrado de transposición en columnas, el mensaje se escribe en una cuadrícula de filas de igual longitud y luego se lee columna por columna. Las columnas se eligen en un orden codificado, decidido por la clave de cifrado. Dado que los cifrados de transposición no afectan las frecuencias de las letras, se pueden detectar a través del análisis de frecuencia. Al igual que otros cifrados de transposición, se puede atacar moviendo letras y haciendo anagramas. También puede ser atacado usando métodos de fuerza bruta si la clave no es lo suficientemente larga.

```
2]: #Columnar Transposition Cipher
    #Codigo basado en https://kaidzohar.blogspot.com/2017/08/columnar-transposition-cipher-code-in.html


    key=input ('Enter a key ')
    userval=input ('Enter a value ')
    col=len(key)
    if((len(userval)%col)!=0):userval+="x"*(len(userval)%col)
    userval=userval.replace(' ', '')#remove white spaces from key
    o=[]
    for i in key:
     o.append(i)  #generating list for keys
    h=[]
    for i in range(col):
     h.append(userval[i:len(userval):col])#generating list for plaintext column wise
    dic=dict(zip(o,h))    #adding both lists
    so=sorted(dic.keys())    #sorting alphabateically keys of cipher
    print(''.join(dic[i]for i in so))#join func for displaaying in string format

    Enter a key seguridadsistemas
    Enter a value amadogarcia
    xcxaxaxoxxxdx
```

Algoritmo transposición y sustitución

Cifrado de valla ferroviaria

El cifrado de valla ferroviaria (a veces llamado cifrado en zigzag) es un cifrado de transposición que algunas veces se combina con algún algoritmo de sustitución, que confunde el orden de las letras de un mensaje utilizando un

algoritmo básico. El cifrado de valla ferroviaria funciona escribiendo su mensaje en líneas alternas a lo largo de la página y luego leyendo cada línea por turno.

Los caracteres del mensaje de texto sin formato se permutan para crear el texto cifrado. En el cifrado de valla de riel, la permutación se obtiene a partir de un patrón muy simple. Otros cifrados de transposición utilizan otras manipulaciones para permutar los caracteres. La clave de cifrado para un cifrado de valla de ferrocarril es un número entero positivo.

```
]: # Python3 program to illustrate
   # Rail Fence Cipher Encryption and Decryption
   #Codigo basado en https://www.geeksforgeeks.org/rail-fence-cipher-encryption-decryption/?ref=gcse

   def encryptRailFence(text, key):

       rail = [['\n' for i in range(len(text))]
                   for j in range(key)]
```

```
if __name__ == "__main__":
    print(encryptRailFence("AmadoGarcia", 5))
    print(decryptRailFence("dnhaweedtees alf tl", 3))
```

```
AcmriaaadGo
delendfthe east wal
```

Referencias

Polybius Square Cipher - GeeksforGeeks. (2018). Retrieved 24 February 2022, from https://www.geeksforgeeks.org/polybius-square-cipher/

NOVA Online | Decoding Nazi Secrets | The Double Transposition Cipher. (2022). Retrieved 24 February 2022, from https://www.pbs.org/wgbh/nova/decoding

Rail Fence Cipher - Encryption and Decryption - GeeksforGeeks. (2017). Retrieved 24 February 2022, from https://www.geeksforgeeks.org/rail-fence-cipher-encryption-decryption/?ref=gcse

Åhlén, J. (2022). Columnar Transposition Cipher (online tool) | Boxentriq. Retrieved 24 February 2022, from https://www.boxentriq.com/code-breaking/columnar-transposition-cipher