Solución al problema 2: Roscón Criptoanalítico

David Cabezas Berrido

Queremos descifrar el siguiente mensaje:

Dqxwpcmadqc, xcr pdradñsw dñ epwmñdoc.
Drjphmd odñwjwswq dq dñ craqsw fdñ jwppdw ecpc rcmdp gad ñw shdqdr mhdq.

El cifrado es una biyección del alfabeto a él mismo, sospecho esto porque *dñ* y *fdñ* tienen pinta de ser *el* y *del*.
He realizado un programa en `Python` para probar combinaciones y ayudarme a encontrar la solución:

```
enigma=list("""dqxwpcmadqc, xcr pdradñsw dñ epwmñdoc.
drjphmd odñwjwswq dq dñ craqsw fdñ jwppdw ecpc rcmdp gad ñw shdqdr mhdq.""")

solucion=enigma.copy()

print(''.join(solucion), '\n')

# Es muy probable que 'dñ' y 'fdñ' sean 'EL' y 'DEL'.
# Esto nos sugiere que la encriptación es una biyección del alfabeto sobre él mismo

# Función para cambiar letras del mensaje original (las nuevas las pongo en mayúscula pa
def cambio(a, b):
    for i in range(len(enigma)):
        if enigma[i]==a:
            solucion[i]=b.upper()

cambio('d','e')
cambio('ñ','l')
cambio('f','d')
print(''.join(solucion), '\n')

"""
EqxwpcmaEqc, xcr pEraELsw EL epwmLEoc.
ErjphmE oELwjwswq Eq EL craqsw DEL jwppEw ecpc rcmEp gaE Lw shEqEr mhEq.
"""

# 'ecpc' tiene que ser una palabra del tipo 'poco', 'como', 'PARA'

cambio('e','p')
cambio('c','a')
cambio('p','r')
print(''.join(solucion), '\n')
```

```
"""
EqxwRAmaEqA, xAr REraELsw EL PRwmLEoA.
ErjRhmE oELwjwswq Eq EL Araqsw DEL jwRREw PARA rAmER gaE Lw shEqEr mhEq.
"""
# 'rAmER' será un verbo como 'lamer' (pero la L ya es la ñ) o 'SABER

cambio('r','s')
cambio('m','b')
print(''.join(solucion), '\n')

"""
EqxwRABaEqA, xAS RESaELsw EL PRwBLEoA.
ESjRhBE oELwjwswq Eq EL ASaqsw DEL jwRREw PARA SABER gaE Lw shEqES BhEq.
"""

# 'PRwBLEoA' suena a 'PROBLEMA'

cambio('w','o')
cambio('o','m')
print(''.join(solucion), '\n')

"""
EqxORABaEqA, xAS RESaELsO EL PROBLEMA.
ESjRhBE MELOjOsOq Eq EL ASaqsO DEL jORREO PARA SABER gaE LO shEqES BhEq.
"""

# 'jORREO' a 'CORREO' y 'xAS' a 'HAS'

cambio('j','c')
cambio('x','h')
print(''.join(solucion), '\n')

"""
EqHORABaEqA, HAS RESaELsO EL PROBLEMA.
ESCRhBE MELOCOsOq Eq EL ASaqsO DEL CORREO PARA SABER gaE LO shEqES BhEq.
"""

# 'RESaELsO' a 'RESUELTO'

cambio('a','u')
cambio('s','t')
print(''.join(solucion), '\n')

"""
EqHORABUEqA, HAS RESUELTO EL PROBLEMA.
ESCRhBE MELOCOTOq Eq EL ASUqTO DEL CORREO PARA SABER gUE LO ThEqES BhEq.
"""
```

```
# 'EqHORABUEqA' a 'ENHORABUENA', 'ESCRhBE' a 'ESCRIBE', 'gUE' a 'QUE'
cambio('g','q')
cambio('q','n')
cambio('h','i')
print(''.join(solucion), '\n')

"""
ENHORABUENA, HAS RESUELTO EL PROBLEMA.
ESCRIBE MELOCOTON EN EL ASUNTO DEL CORREO PARA SABER QUE LO TIENES BIEN.
"""
```