Lucas Moreira Gomes, 29/06/2022, Aufgabe 1

Die zu entschlüsselnde Nachricht lautet:

Ta _7N6DDDhlg:W3D_H3C31N__0D3ef sHR053F38N43D0F i33___NA

Zur Entschlüsselung der Nachricht wurde die in der Übung gegebene Information, dass es sich um eine "Transpositions-Cipher" vom Typ Rails mit 4 Rails handelt, verwendet. Unter Berücksichtigung des erwarteten Layouts wurde Python verwendet, um das Ergebnis im richtigen Format zu lesen:

```python
message = 'Ta _7N6DDDhlg:W3D_H3C31N__0D3ef sHR053F38N43D0F i33___NA'

LengthMessage = len(message)+1

NewMessage = ''
Line = 0
AB = True
lenNewMessage = len(NewMessage)
for pos, i in enumerate(message):

    if lenNewMessage == 0:
        NewMessage += Line*'-'

    lenNewMessage = len(NewMessage)- Line*LengthMessage

    if Line == 0 or Line == 3:
        progress = '-'*(5)
    else:
        if AB:
            progress = '-'*(5-Line*2)
        else:
            progress = '-'*(Line*2-1)

    if lenNewMessage + len(progress)+1 < LengthMessage:
        NewMessage += i+progress
        AB = not AB
    elif lenNewMessage + len(progress) +1 == LengthMessage:
        print(pos)
        NewMessage += i+progress+ '\n'
        Line += 1
        AB = True
        lenNewMessage = len(NewMessage) - (Line*LengthMessage+1)
    elif lenNewMessage < LengthMessage:
        NewMessage += i+'-'*(LengthMessage-lenNewMessage-1) + '\n'
        Line += 1
        AB = True
        lenNewMessage = len(NewMessage) - (Line*LengthMessage+1)
    else:
        print('error')

print(NewMessage)

```

Das Ergebnis der obigen Funktion ist unten dargestellt.

```
lucasgomes@MacBook-Pro Aufgabe1 % /usr/local/bin/python3.9 "/Users/lucasgomes/Documents/Mestrado/2. Semester/HAW/CyberSecurity/CyberSecurity/Aufgabe1/RailFenceCipher.py"
46
T-----a----- -----_-----7-----N-----6-----D-----D-----D--
-h---l-g---:-W---3-D---_-H---3-C---3-1---N-_---_-0---D-3
--e-f--- -s---H-R---0-5---3-F---3-8---N-4---3-D---0-F---
--- -----i-----3-----3-----_-----_-----_-----N-----A----
```

Ergebnis durch Ablesen der Diagonalen:

The flag is: WH3R3_D035_7H3_F3NC3_8361N_4ND_3ND_D00AFDD3

Quelle: https://en.wikipedia.org/wiki/Transposition_cipher

https://en.wikipedia.org/wiki/Rail_fence_cipher