

```

from math import *
from time import *
def f(word):
    global n_w, w8
    n_w=0
    w8=0
    wzahl=[]
    # bei kürzeren Wörtern wird die Zeichenkette vorn mit Nullen gefüllt
    if len(word) < 8:
        wzahl.append(0);
    if len(word) < 7:
        wzahl.append(0);
    if len(word) < 6:
        wzahl.append(0);
    if len(word) < 5:
        wzahl.append(0);
    if len(word) < 4:
        wzahl.append(0);
    if len(word) < 3:
        wzahl.append(0);
    if len(word) < 2:
        wzahl.append(0);
    if len(word) < 1:
        wzahl.append(0);

    i=0
    #das Wort Buchstaben für Buchstaben durchgehen und die Zeichen ersetzen
    #Zeichen als Koeffizienten merken
    while len(word) > i:
        j=0
        letter=word[i]
        if letter == "0":
            wzahl.append(0)
        if letter == "c":
            wzahl.append(1)
            j=1
        if letter == "e":
            wzahl.append(2)
            j=2
        if letter == "i":
            wzahl.append(3)
            j=3
        if letter == "n":
            wzahl.append(4)
            j=4
        if letter == "o":
            wzahl.append(5)
            j=5
        if letter == "r":
            wzahl.append(6)
            j=6
        if letter == "t":
            wzahl.append(7)
            j=7

        # Oktawert w8 berechnen
        # Dezimalwert n_w berechnen
        w8=w8 + j*10**(len(word)-1-i)
        n_w=n_w + j*8**(len(word)-1-i)
        i=i+1

def f1(zahl8):
    global w

```

```

w=[]
zahl8_str=str(zahl8)
print "zahl8 als Zeichenkette =", zahl8_str, ""
i=0

#das Wort Buchstaben für Buchstaben durchgehen und die Zeichen ersetzen
#Zeichen als Koeffizienten merken
while len(zahl8_str) > i:
    letter=zahl8_str[i]
    if letter == "0":
        w.append(0)
    if letter == "1":
        w.append("c")
    if letter == "2":
        w.append("e")
    if letter == "3":
        w.append("i")
    if letter == "4":
        w.append("n")
    if letter == "5":
        w.append("o")
    if letter == "6":
        w.append("r")
    if letter == "7":
        w.append("t")
    i=i+1

#Eingabefenster
w = input("Dein Wort",False)
#Start der Berechnung mit Zeitmessung
startzeit=time()
if(len(w) <= 8):

    #Aufruf der Funktion mit dem eingegebenen Wort
    print "das Wort ist: ", w
    # Aufruf der Funktion f
    f(w)
    print "word = ", w
    print "w8 = ", w8
    print "n_w = ", n_w

else:
    print "wort zu lang"

print "RSA-Algorithmus"

N=long(4073*4127)
phi=long(4072*4126)
# Long als Datentyp für große ganze Zahlen
e=3
print "public key = [N, e] = [",N,",", e, "]"

#RSA
#Chiffrieren
print "Chiffrieren"
c_w=long(n_w**e % N)
# Long als Datentyp für große ganze Zahlen
c_w1=int(c_w)
# umwandeln nach der Berechnung in ein Int für weitere Verarbeitung
print "c_w = ", c_w1
print "Chiffriertes Wort im 8-er System:", int(oct(c_w1))
f1(int(oct(c_w1)))
print "Chiffriertes Wort:", w

```

```
zeit=time()
print "Zeit =", int(zeit-startzeit), "s"
print "Dechiffrieren"

#Dechiffrieren
#private key ermitteln [N,d]
# Inverse Aufgabe  $e*d \equiv 1 \pmod{\phi(N)}$ 
d=1
while d < phi:
    rest = d*e % phi
    if rest == 1:
        break
    else:
        d=d+1

zeit=time()
print "private key = [N, d] = [",N,", ", d,"]"
print "Zeit =", int(zeit-startzeit), "s"

n_w=long(c_w1**d % N)
n_w1=int(n_w)
print "n_w = ", n_w1
#zurück Dezimalzahl in Oktazahl
#print "oct(n_w3) = ", oct(n_w3)
print "dechiffriertes Wort im 8-er System:", int(oct(n_w1))
f1(int(oct(n_w1)))
print "Dechiffriertes Wort:",w
endzeit=time()
print "Zeit =", int(endzeit-startzeit), "s"
```