

Die Caesar-Verschlüsselung

caesar.py

Schon im Altertum war es wichtig, Nachrichten so zu verschicken, dass sie der Feind, selbst wenn er sie abgefangen hat, nicht verstehen konnte. Julius Caesar verwendete dazu oft den nach ihm benannten Caesar Code. Wenn eine Nachricht verschlüsselt werden sollte, musste vorerst ein „*Schlüssel*“ vereinbart werden. Dieser Schlüssel k war eine Zahl zwischen 1 und 25. Die Rohnachricht wurde dann verfasst und jeder Buchstabe um k Stellen im Alphabet verschoben. Um die geheime Nachricht zu entschlüsseln, mussten die Buchstaben im gegenläufigen Sinn zurück verschoben werden. Wir werden jetzt mit dem TI-Nspire™ CX II-T CAS die Caesar-Verschlüsselung programmieren.

```

caesar.py 11/14
az="abcdefghijklmnopqrstuvwxyz"
def versch(s,k):
    r=""
    for c in s:
        if c in az:
            r+=az[(az.index(c)+k)%26]
        else:
            r+=c
    return r
def entsch(s,k):
    return versch(s,-k)

```

```

Python-Shell 11/11
>>>#Running caesar.py
>>>from caesar import *
>>>versch("veni, vidi, vici",17)
'mvez, mzuz, mztz'
>>>entsch("mvez, mzuz, mztz",17)
'veni, vidi, vici'
>>>versch("galliaomniaestdivisa",10)
'qkvvskywxskocdnfsck'
>>>entsch("qkvvskywxskocdnfsck",10)
'galliaomniaestdivisa'
>>>

```

- Wir beginnen mit der Eingabe des Alphabets im string az.
- Die Prozedur versch(s,k) verschlüsselt die Nachricht s mit dem Schlüssel k. Der String der verschlüsselten Botschaft r ist anfänglich leer.
- Für jeden einzelnen Buchstaben c aus s wird mit az.index(c) die Position im Alphabet bestimmt, worauf man mit (az.index(c)+k)%26 den entsprechend verschobenen Buchstaben erhält. %26 = mod(26) ist notwendig, da man ja durch die Addition mit k auch über 26 hinauskommen kann und dann wieder bei a zu zählen beginnt. Der gewonnene Buchstabe wird an r angefügt.
- Für den Fall, dass c kein (Klein-) Buchstabe ist, wird das Zeichen unverschlüsselt angefügt.
- Am Ende wird die verschlüsselte Nachricht r ausgegeben.
- Die Prozedur entsch(s,k) verschiebt das Alphabet um k Positionen nach links und man kommt wieder zum ursprünglichen Text zurück.