Kryptografie

CAESAR-Verschlüsselung mit Python

Du weißt nun, wie die CAESAR-Verschlüsselung funktioniert und kennst dich auch schon etwas mit Python aus. Das ist eine gute Gelegenheit, beides zu verbinden und ein Python-Programm für die CAESAR-Verschlüsselung zu programmieren.

Zur Erinnerung einige Python-Befehle

- `print("Hallo, Welt!")` Gibt den Text "Hallo, Welt!" aus.
- `input("Gib etwas ein ein: ")` Gibt den Text "Gib etwas ein:" aus und wartet, bis der Nutzer die ENTER-Taste betätigt.
- `ord("A")` Wandelt den Buchstaben "A" in seinen Unicode (hier "65") um.
- `chr(65)` Wandelt den Unicode "65" in das passende Zeichen (hier "A") um.
- `"Ein Text".upper()` Wandelt "Ein Text" in "EIN TEXT" um.
- `"Ein Text".lower()` Wandelt "Ein Text" in "ein text" um.
- `for x in "Hallo, Welt":` Setzt `x` auf jedes Zeichen in "Hallo, Welt" und führt den Code hinter `:` aus.

Aufgabe 1

Bringe das folgende Programm-Puzzle in die korrekte Reihenfolge und teste deine Lösung mit TigerJython.

Hinweis *Du musst die Einrückungen selber noch passend setzen.*

```
neuesZeichen = chr(verschoben)
klartext = input("Klartextwort (ohne Leerzeichen): ")
if verschoben > ord("Z"):
geheimtext = ""
unicode = ord(zeichen)
schluessel = schluessel.upper()
schluessel = ord(schluessel)-ord("A")
print(klartext + " -> " + geheimtext)
# Schleife über alle Zeichen im Klartext
for zeichen in klartext:
klartext = klartext.upper()
verschoben = unicode + schluessel
schluessel = input("Schlüsselbuchstabe: ")
verschoben = verschoben - 26
geheimtext = geheimtext + neuesZeichen
```

Aufgabe 2

a) Erweitere das Programm so, dass es auch mit *Leerzeichen* im Klartext klarkommt.

b) Entwickle ein Programm zum *Entschlüsseln* eines Cäsar-Geheimtextes.

Aufgabe 3

Du weißt auch schon, dass die CAESAR-Chiffre für moderne Computer recht leicht zu knacken ist. Entwickle ein Programm, dass einen Geheimtext *ohne Kenntniss des Schlüssels* entschlüsseln kann.

Hinweis *Das Programm kann nicht selber erkennen, ob der entschlüsselte Text ein sinnvoller Klartext ist. Daher muss diese Entscheidung vom Benutzer getroffen werden.*

Hinweis *Nutze die Funktionen aus Aufgabe 2.*