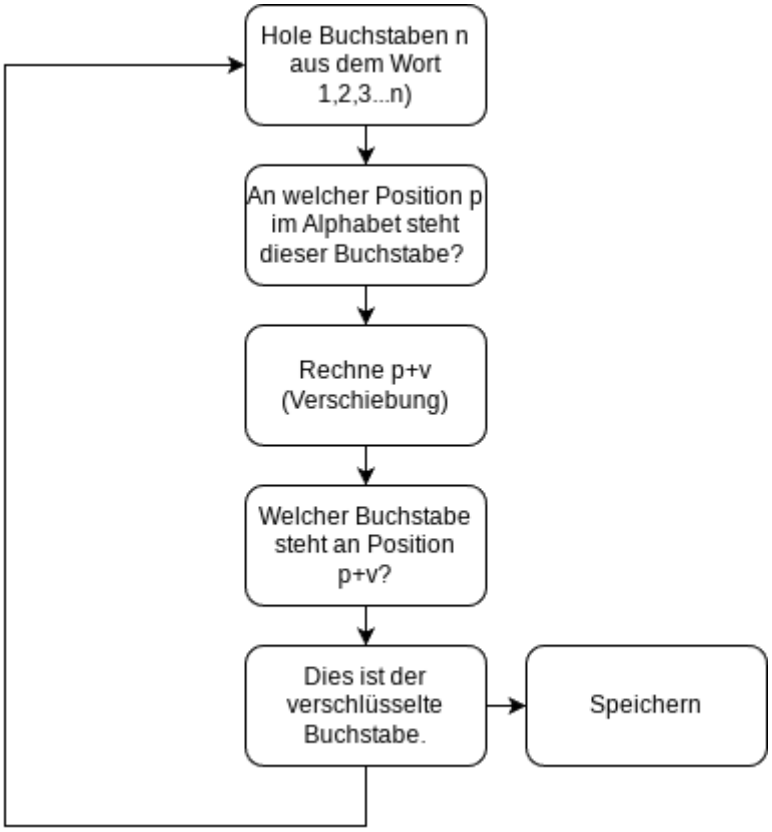
Kryptologie

Die CESAR-Verschlüsselung

Die Verschlüsselungsscheibe

CESAR-Verschlüsselung mit Python programmieren

Algorithmus für die Verschlüsselung mit CESAR



Für die Programmierung einer Ver- und Entschlüsselung mit der CAESAR-Verschlüsslung benötigt man folgende Elemente:

Beispiel für eine Modulorechnung

```
for i in range(100):
    x=i%5
```

```
    print(x)
```

Die Modulorechnung benötigt man für die Verschiebung, wenn die Rechnung p+v (siehe Algorithmus) über den letzten Buchstaben hinausgeht.

Funktionen zu Strings

- `lower()` gibt einen String in Kleinbuchstaben aus. Der entschlüsselte Text ist immer in Kleinbuchstaben.
- `len()` gibt die Länge eines Strings (oder einer Liste) zurück.
- `index()` gibt die Position des Zeichens in einem String zurück.

Iteration über einen String

Eine Iteration ist, wenn man in einem Algorithmus eine bestimmte Anweisung in einer Schleife immer wieder ausführt, wobei sich mindestens ein Parameter mit jedem Durchgang ändert. Dies ist häufig ein Zähler. In dem folgenden Beispiel wird mit jedem Durchgang der Schleife ein neuer Buchstabe aus dem String `s` geholt.

```
s = "Theodor-Heuss-Schule"
print(s.lower())
for c in s:
    a = s.index(c)
    print("Buchstabe ", c, " taucht erstmalig an Position ", a,  "auf.")

print(f"Der erste Buchstabe in {s}: {s[0]}")
for i in range(len(s)):
    print(f"Dies ist der {i+1}. Buchstabe: {s[i]}")
```

CESAR Verschlüsselung

Dies hier ist das Grundgerüst für ein Skript, das die CESAR-Verschlüsselung realisiert. Es muss nur noch ein wenig Code ergänzt werden. Natürlich gibt es auch andere Lösungen.

```
ALPHABET = "abcdefghijklmnopqrstuvwxyz"
```

```
def encrypt(text, key):
    encryptedText = ""
    text = text.lower()
    # Hier wird der Text verschlüsselt.

    return encryptedText.upper()

def decrypt(text, key):
    return ""

text = input("Den Text eingeben: ")
key = int(input("Den Schlüssel eingeben: "))
geheim = encrypt(text, key)
klar = decrypt(geheim, key)
print("Der verschlüsselte Text: ", geheim)

print("Der aus dem Geheimtext entschlüsselte Text: ", klar)
```

Passwörter knacken

Passwörter in Passwortlisten finden

```
from getpass import getpass

with open("1000-most-common-passwords.txt", "r") as file:
  password_list_1000 = file.read().splitlines()
with open("1000000-most-common-passwords.txt", "r") as file:
  password_list_1000000 = file.read().splitlines()

pwd = getpass("Gib dein Passwort ein: ")

if pwd in password_list_1000:
    print(f"Dein Passwort ist in der Liste der tausend häufigsten Passwörter.")
    exit(0)

if pwd in password_list_1000000:
    print(f"Dein Passwort ist in der Liste der millionen häufigsten Passwörter.")
    exit(0)

print("Dein Passwort ist nicht in der Liste der meisten Passwörter.")
```

Dateidownloads

Diese beiden Dateien müssen im selben Verzeichnis wie der Programmcode gespeichert sein.

- 1000-most-common-passwords.txt
- 1000000-most-common-passwords.txt