

A Aufgabenstellung

Oft muss man kleine Hilfsprogramme für die Kommandozeile (CLI) implementieren. Dafür benötigt man häufig eine komplexe Logik für die Kommandozeilenparameter (siehe z.B. die Befehle git oder ip unter Linux).

Wir lernen nun die Python-Bibliothek argparse kennen, mit der wir mit geringem Aufwand derartige Programme entwickeln können.

Das Ziel dieser Übung besteht darin, zwei CLI-Applikationen zu entwickeln:

- cvcrypt.py zum Ver- und Entschlüsseln von Dateien mittels Caesar- oder Vigenère-Chiffre.
- cvcrack.py zum Knacken des Schlüssels von Dateien, die mittels Caesar- oder Vigenère-Chiffre verschlüsselt wurden.

B Allgemeine Hinweise:

- Software Reuse: Keine Methoden mehrfach implementieren: z.B. Importiere kasiski.py aus der vorhergehenden Übung¹
- Benutze die Python-Bibliothek argparse siehe Foliensatz / Vorbesprechung
- Überprüfe immer vor dem Einlesen einer Datei, ob diese auch existiert²
- Fehlermeldungen sollen wie unter Linux üblich auf dem Stderror-Device ausgegeben werden³. Benutze standardisierte Fehlermeldungen⁴
- Beim Einlesen der Datei werden alle Umlaute, Sonderzeichen, Zeilenumbrüche, etc. entfernt und die Großbuchstaben in Kleinbuchstaben umgewandelt
- Benutze die beiliegenden Dateien, um die Lösung zu überprüfen
- Alle Dateien kommen in das Git Repository
- Type-Annotantions = Type-Hints verwenden⁵
- Dokumentation mit PyDoc
- "Hauptprogramm" mit if __name__ == "__main__":

C cvcrypt.py: Beispielaufrufe und Usage

```
> python cvcrypt.py --verbose --cipher caesar --encrypt --key "b" rk.txt rk_ceb.txt
Encrypting Caesar with key = b from file rk.txt into file rk_cb.txt
> python cvcrypt.py --cipher caesar --encrypt --key "b" rk.txt rk_ceb.txt
> python cvcrypt.py --verbose --cipher vigenere --encrypt --key "hugo" rk.txt rk_vehugo.txt
Encrypting Vigenere with key = hugo from file rk.txt into file rk_vehugo.txt
> python cvcrypt.py --verbose --cipher v --decrypt --key "hugo" rk_vehugo.txt rk_vdhugo.txt
Decrypting Vigenere with key = hugo from file rk_vehugo.txt into file rk_vdhugo.txt
> python cvcrypt.py --cipher v --decrypt --key "hugo" mich_gibts_nicht.txt rk_vdhugo.txt
mich_gibts_nicht.txt: No such file or directory
> python cvcrypt.py
usage: cvcrypt.py [-h] [-c {caesar,c,vigenere,v}] [-v | -q] [-d | -e] [-k KEY] infile [outfile] cvcrypt.py: error: the following arguments are required: infile
> python cvcrypt.py --help
usage: cvcrypt.py [-h] [-c {caesar,c,vigenere,v}] [-v | -q] [-d | -e] [-k KEY] infile [outfile]
```

Version vom 5. März 2025 1/2

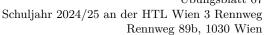
 $^{^{1}}$ from kasiski import ...

²https://pythonspot.com/read-file/

 $^{^3} https://www.w3docs.com/snippets/python/how-do-i-print-to-stderr-in-python.html\\$

 $^{^4 {\}rm https://www.geeks forgeeks.org/python-os-strerror-method/}$

 $^{^5 {\}rm siehe~z.B.~https://mypy.readthedocs.io/en/stable/cheat_sheet_py3.html}$





```
cvcrypt - Caesar & Vigenere encrypter / decrypter by ZAI / HTL Rennweg
positional arguments:
  infile
                        Zu verschlüsselnde Datei
  outfile
                        Zieldatei
options:
                        show this help message and exit
  -h, --help
  -c {caesar,c,vigenere,v}, --cipher {caesar,c,vigenere,v}
                        Zu verwendende Chiffre
  -v, --verbose
  -q, --quiet
  -d, --decrypt
  -e, --encrypt
                        Encryption-Key
  -k KEY, --key KEY
```

D cvcrack.py: Beispielaufrufe und Usage

```
> python cvcrack.py --cipher caesar --verbose rk_ceb.txt
Cracking Caesar-encypted file rk_ceb.txt: Key = b
> python cvcrack.py --cipher caesar rk_ceb.txt
> python python cvcrack.py --cipher vigenere rk_vehugo.txt
> python cvcrack.py -v --cipher vigenere rk_vehugo.txt
Cracking Vigenere-encypted file rk_vehugo.txt: Key = hugo
> python cvcrack.py mich_gibts_nicht.txt
mich_gibts_nicht.txt: No such file or directory
> python cvcrack.py
usage: cvcrack.py [-h] [-c {caesar,c,vigenere,v}] [-v | -q] infile
cvcrack.py: error: the following arguments are required: infile
> python cvcrack.py --help
usage: cvcrack.py [-h] [-c {caesar,c,vigenere,v}] [-v | -q] infile
cvcrack - Caesar & Vigenere key cracker by ZAI / HTL Rennweg
positional arguments:
  infile
                        Zu knackende Datei
options:
  -h, --help
                        show this help message and exit
  -c {caesar,c,vigenere,v}, --cipher {caesar,c,vigenere,v}
                        Zu verwendende Chiffre
  -v, --verbose
                        Zeigt Infos an (siehe Beispiele in der Angabe)
                        Liefert nur den wahrscheinlichsten Key zurück
  -q, --quiet
```

Version vom 5. März 2025 2 / 2