

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:

- `cvccrypt.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-Annotations = Type-Hints verwenden⁵
- Dokumentation mit PyDoc
- “Hauptprogramm” mit `if __name__ == "__main__":`

C cvccrypt.py: Beispielaufufe und Usage

```
> python cvccrypt.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 cvccrypt.py --cipher caesar --encrypt --key "b" rk.txt rk_ceb.txt
> python cvccrypt.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 cvccrypt.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 cvccrypt.py --cipher v --decrypt --key "hugo" mich_gibts_nicht.txt rk_vdhugo.txt
mich_gibts_nicht.txt: No such file or directory

> python cvccrypt.py
usage: cvccrypt.py [-h] [-c {caesar,c,vigenere,v}] [-v | -q] [-d | -e] [-k KEY] infile [outfile]
cvccrypt.py: error: the following arguments are required: infile

> python cvccrypt.py --help
usage: cvccrypt.py [-h] [-c {caesar,c,vigenere,v}] [-v | -q] [-d | -e] [-k KEY] infile [outfile]
```

¹from kasiski import ...

²<https://pythonspot.com/read-file/>

³<https://www.w3docs.com/snippets/python/how-do-i-print-to-stderr-in-python.html>

⁴<https://www.geeksforgeeks.org/python-os-strerror-method/>

⁵siehe z.B. https://mypy.readthedocs.io/en/stable/cheat_sheet_py3.html

cvccrypt - Caesar & Vigenere encrypter / decrypter by ZAI / HTL Rennweg

positional arguments:

infile	Zu verschlüsselnde Datei
outfile	Zielfile

options:

-h, --help	show this help message and exit
-c {caesar,c,vigenere,v}, --cipher {caesar,c,vigenere,v}	Zu verwendende Chiffre
-v, --verbose	
-q, --quiet	
-d, --decrypt	
-e, --encrypt	
-k KEY, --key KEY	Encryption-Key

D cvccrack.py: Beispielaufufe und Usage

```
> python cvccrack.py --cipher caesar --verbose rk_ceb.txt
Cracking Caesar-encrypted file rk_ceb.txt: Key = b
```

```
> python cvccrack.py --cipher caesar rk_ceb.txt
b
```

```
> python python cvccrack.py --cipher vigenere rk_vehugo.txt
hugo
```

```
> python cvccrack.py -v --cipher vigenere rk_vehugo.txt
Cracking Vigenere-encrypted file rk_vehugo.txt: Key = hugo
```

```
> python cvccrack.py mich_gibts_nicht.txt
mich_gibts_nicht.txt: No such file or directory
```

```
> python cvccrack.py
usage: cvccrack.py [-h] [-c {caesar,c,vigenere,v}] [-v | -q] infile
cvccrack.py: error: the following arguments are required: infile
```

```
> python cvccrack.py --help
usage: cvccrack.py [-h] [-c {caesar,c,vigenere,v}] [-v | -q] infile
```

cvccrack - 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)
-q, --quiet	Liefert nur den wahrscheinlichsten Key zurück