

Sichere Programmierung

Projekt 1

Julian Sobott
(76511)
David Sugar
(76050)

1 Zu Aufgabe 1

Aus der Aufgabenstellung war gegeben, dass die Funktion `decode(text)`, die Buchstaben des übergebenen Textes in entsprechende Zahlen aus \mathbb{Z}_{26} umwandeln und diese dann in einer Liste zurückgeben soll. Daraus ergibt sich der Definitionsbereich $D = \{a, \dots, z\}$ und Wertebereich $W = \{0, \dots, 25\}$ mit $f : D \rightarrow W$ für die Symbole und $decode() : D^* \rightarrow W^*$ für Wörter beliebiger Länge.

$f : D \rightarrow W$ wird durch `alph_to_num` realisiert, einem Python `dict`, dass von `ascii` Kleinbuchstaben aufsteigend auf die Zahlen von Null bis 25 abbildet und wiederum innerhalb von `decode()` in einer Schleife verwendet wird um jeden einzelnen Buchstaben des übergebenen Textes umzuwandeln. Werte außerhalb des Definitionsbereiches werden vom gegebenen Algorithmus ignoriert.

```
1 alph_to_num = {k:v for v , k in enumerate(string.ascii_lowercase)}
```

2 Zu Aufgabe 2

Die Funktion `encode(text)` stellt die Umkehrfunktion von `decode()` dar, für alle $w \in \{a, \dots, z\}^*$. Sie nimmt als Eingabe eine Liste von Zahlen $a \in \mathbb{Z}_{26}$ und gibt eine entsprechende Zeichenkette (String) zurück.

Das Abbilden von Zahlen auf die entsprechenden Buchstaben wird durch $num_to_alph : \{0, \dots, 25\} \rightarrow \{a, \dots, z\}$ realisiert.

```
1 num_to_alph = {v:k for v , k in enumerate(string.ascii_lowercase)}
```

Um den String schlussendlich zu bauen benötigt es dann nur einen Einzeiler.

```
1 "".join([ num_to_alph[d] for d in int_list ])
```

Dadurch, dass `decode()` und `encode()` jeweils Funktion und Umkehrfunktion darstellen ergibt sich: $w = \text{encode}(\text{decode}(w))$.

3 Zu Aufgabe 3

Um das gewünschte Dictionary `key_table` zu erstellen, haben wir die gleichnamige Funktion `key_table(m: int)` implementiert. Diese ermöglicht es nicht nur `key_table` für

\mathbb{Z}_{26} , sondern allgemein für $\mathbb{Z}_m, m \geq 2$ anzulegen. Dabei wird mithilfe einer For-Loop über alle $a \in \{1, 2, \dots, m-1\}$ iteriert und deren multiplikativ Inverses, mithilfe von `mcrypt.mul_inverse(n, m)`, berechnet. Falls ein mult. Inverses existiert wird dieses dann nach dem Schema $a : a^{-1}$ dem Dictionary hinzugefügt. Sollte $m < 2$ oder ein invalider Datentyp übergeben werden, wird `None` zurückgegeben. Andernfalls gibt die Funktion das erstellte Dictionary zurück.

```

1 for i in range(m):
2     i_neg = mul_inverse(i, m) # Berechnung d. mult. Inv.
3
4     if i_neg != None:
5         d[i] = i_neg          # Es gibt ein mult. Inv. -> add to dict

```

3.1 Berechnung des multiplikativ Inversen

Zur Berechnung des multiplikativ Inversen wird die Funktion `mul_inverse(n: int, m: int)` genutzt, die auf dem erweiterten Euklid'schen Algorithmus beruht. Grundsätzlich gilt, wenn es zu $n \in \mathbb{Z}_m$ eine Zahl $x \in \mathbb{Z}_m$ gibt mit $n * x = 1(mod m)$, so wird x als multiplikativ Inverses zu n in m bezeichnet, schreibe n^{-1} oder $\frac{1}{n}$.

Die Definition des multiplikativ Inversen bedeutet jedoch, dass sich $n * x$ und 1 um ein Vielfaches von m unterscheiden, d.h. $n * x + m * y = 1$. Für Gleichungen dieser Art kann nun x und y mithilfe des erweiterten Euklid bestimmt werden.

Anfangs wird jedoch erst einmal geprüft, ob n teilerfremd zu m ist und parallel die einzelnen Teiler jeder Division für später in einer Liste gespeichert.

```

1 q = [] # Liste von Teilern
2
3 while m != 0:
4     q += [n // m] # Teiler hinzufügen
5     (n, m) = (m, n % m)
6
7 if n != 1:
8     return None # n und m Teilerfremd ?

```

Dies ist zwingend notwendig, denn sollte gelten, dass n und m einen gemeinsamen Teiler $t > 1 \in \mathbb{Z}$ besitzen, dann gilt: $n = t\hat{n}$ und $m = t\hat{m}$, d.h. $n\hat{x} = 1(mod m) = t\hat{n}\hat{x} - t\hat{m}\hat{y} = 1 = t(\hat{n}\hat{x} - \hat{m}\hat{y}) = 1$. Es gibt jedoch kein $t > 1$, das diese Gleichung erfüllt, demnach müssen n und m teilerfremd sein.

Danach werden mittels der Teiler aus q , x und y berechnet, wobei nur x von Interesse ist und als Rückgabewert dient. Das letzte Statement dient dazu, dass x in \mathbb{Z}_m liegt.

```

1 q.reverse()
2 x = 1
3 y = 0
4
5 for t in q:
6     _x = y
7     _y = x - (_x * t)

```

```

8     x = _x
9     y = _y
10
11 return (x + module) % module

```

4 Zu Aufgabe 4

`acEncrypt(a, b, text)` nutzt zuerst `decode()` um mithilfe des gegebenen Textes eine entsprechende Liste von Ganzzahlen zu erzeugen.

```

1 t = decode(plain_text)

```

Danach wird über jedes Element der Liste iteriert und dieses mithilfe des Schlüssels (`a`, `b`) verschlüsselt.

```

1 for i in range(len(t)):
2     t[i] = (a * t[i] + b) % module

```

Schlussendlich wird die verschlüsselte Liste an `encode()` übergeben, die alle Zahlen wieder in einen String umwandelt, der danach zurückgegeben wird.

```

1 e = encode(t)
2 return e.upper()

```

Anfangs prüft die Funktion, ob überhaupt die richtigen Datentypen übergeben wurden. Sollte dies nicht der Fall sein, wird vom `logger` eine entsprechende Nachricht mit dem Level `Warning` ausgegeben und ein leerer String zurückgegeben. Sollte `a` nicht teilerfremd zu 26 sein, wird ebenfalls eine Nachricht geloggt, dieses mal mit dem Level `Info` und ein leerer String zurückgegeben.

Damit Einträge des Levels `Info` angezeigt werden, muss das jeweilige Script mit der Option `'-v'` (`verbose`) ausgeführt werden.

5 Zu Aufgabe 5

Die Fehlerprüfung von `acDecrypt()` ist identisch zu der von `acEncrypt`.

Nachdem auf Fehler geprüft wurde, wird als erstes dafür gesorgt, dass der Teilschlüssel `a` in \mathbb{Z}_{26} liegt. Dadurch wird sichergestellt, dass bei einem späteren Hash-Table lookup auch an der richtigen Stelle 'gesucht' wird.

```

1 a = a % module

```

Danach wird ein entsprechendes `key_table` erzeugt.

```

1 table = key_table(module)

```

Schlussendlich wird mit $(y-b)*a^{-1} = x$ jede Ziffer des übergebenen Cipher-Textes wieder entschlüsselt und zu einem String zusammengefügt, der als Rückgabewert dient. a^{-1} wird dabei in `table` mithilfe von `a` nachgeschlagen.

```
1 return encode([ ((y - b) * table[a]) % modulo for y in decode(cipher_text) ])
```

6 Zu Aufgabe 6

```
1 if __name__ == '__main__':
2     # Aufgabe 6
3     pt = "strenggeheim"
4     k1 = "db"
5     ct = "IFFYVQMJYFFDQ"
6     k2 = "pi"
7
8     k1_1, k1_2 = decode(k1)
9     k2_1, k2_2 = decode(k2)
10
11     ptoc = acEncrypt(k1_1, k1_2, pt)
12     ctop = acDecrypt(k2_1, k2_2, ct)
13
14     print("Aufgabe 6:")
15     print(ptoc)
16     print(ctop)
```

```
1 Aufgabe 6:
2 DGANOTTNWNZL
3 affinechiffre
```

7 Zu Aufgabe 7

Datei wurde entsprechend benannt.

8 Zu Aufgabe 8

Das `affinecipher.py` Skript besteht aus zwei Teilen, der `crypt(path: str, key: str, fun)` Funktion sowie einem `__main__` Part, der nur ausgeführt wird, wenn man die Datei auch wirklich als Skript und nicht etwa als Modul nutzt.

8.1 crypt()

Die `crypt()` Funktion hat drei Parameter, namentlich `path`, `key` und `fun`. Ihr wird der Pfad der zu ver- bzw. entschlüsselnden Datei als String, ein Schlüsselpaar ebenfalls als String, sowie entweder die Ver- oder Entschlüsselungsfunktion übergeben. Danach wird das Schlüsselpaar, mithilfe von `decode()`, in seine numerische Repräsentation umgewandelt. Schlussendlich wird die übergebene Funktion mit dem Schlüsselpaar sowie dem Inhalt der Datei als Argumente aufgerufen. Und der Rückgabewert auf der Kommandozeile ausgegeben.

```
1 def crypt(path: str, key: str, fun) -> None:
2     k1, k2 = decode(key)
3
4     with open(path, "r") as f:
5         print(fun(k1, k2, f.read()))
```

Dadurch, dass die `acEncrypt()` und `acDecrypt()` Funktionen dieselben Schnittstellen besitzen, kann hier auf eine Funktion zurückgegriffen werden, der die jeweils passende Ver- oder Entschlüsselungsfunktion übergeben wird. Dies spart etwas Code und vermeidet Redundanzen.

8.2 ____main____

Hier steht der Großteil des Codes.

8.2.1 Kommand Line Arguments

Um an die jeweiligen Kommandozeilenargumente zu kommen, haben wir das `argparse` Modul importiert.

```
1 import argparse
```

Mit dem folgenden Methodenaufruf kann dann ein `ArgumentParser` erzeugt werden, dem außerdem eine Beschreibung des Skripts als String übergeben werden kann.

```
1 parser = argparse.ArgumentParser(description="Encrypt or decrypt \\  
2 a file using the affine cipher")
```

Danach können dem erzeugten Parser-Objekt zu erwartende Argumente hinzugefügt werden. Es ist dabei möglich, Neben einem aussagekräftigen Namen, auch erwartete Werte sowie ein Hilfetext als Argumente zu übergeben.

```
1 parser.add_argument("mode", choices=["e", "d"], help="[e]ncrypt or \\  
2 [d]ecrypt the file")
3 parser.add_argument("key", help="String with exactly two lower \\  
4 case ascii letters")
5 parser.add_argument("path", help="File path")
```

Mit dem Methodenaufruf `parse_args()` kann dann ein Objekt erzeugt werden, mit dem auf die Kommandozeilenargumente, wie auf normal Instanz-Attribute, zugegriffen werden kann.

```

1 args = parser.parse_args()
2
3 mode = args.mode
4 key = args.key
5 path = args.path

```

Der Vorteil von `argparse` gegenüber dem direkten aufrufen von `sys.argv` ist, dass auf einfache Weise nutzerfreundliche Kommandozeilenschnittstellen geschaffen werden können. Übergibt der Nutzer z.B. falsche Argumente, so wird ihm direkt der passende Hilfstext mit Nutzungsinformationen angezeigt.

Mit den obigen Statements erzeugt uns `parseargs` beim aufrufen des Skriptes mit `./affinecipher.py -h` folgenden Output:

```

1 usage: affinecipher.py [-h] {e,d} key path
2
3 Encrypt or decrypt a file using the affine cipher
4
5 positional arguments:
6   {e,d}                [e]ncrypt or [d]ecrypt the file
7   key                  String with exactly two lower case ascii letters
8   path                File path
9
10 optional arguments:
11   -h, --help          show this help message and exit

```

8.2.2 Aufruf von `crypt()`

Je nach Betriebsmodus wird nach dem parsen der Argumente `crypt()` entweder mit der `acEncrypt()` oder der `acDecrypt()` aufgerufen, die sich wie oben beschrieben verhält.

8.3 Inbetriebnahme

Um das Skript wie ein normal Programm ausführen zu können, muss dieses wissen welchen Interpreter es für die nachfolgenden Zeilen verwenden soll. Um dies festzulegen wird der sog. `shebang` (`#!`) genutzt, gefolgt von dem absoluten Pfad des zu verwendenden Interpreters.

```

1 #! /usr/bin/python3

```

Diese Zeile sagt aus, dass die Nachfolgenden Zeilen mithilfe des `python3` Interpreters ausgeführt werden sollen.

Danach müssen dem Skript außerdem noch Ausführungsrechte (eng. execute permission) hinzugefügt werden. Dies geschieht über die Kommandozeile mit:

```

1 $ chmod +x affinecipher.py

```

Alternativ kann statt `+x` auch der entsprechende Oktalwert genutzt werden.

Mit `ls -l` lässt sich dann ggf. noch überprüfen ob der vorherige Befehl richtig ausgeführt wurde.

```

1 $ ls -l
2 ...
3 -rwxr-xr-x 1 sugar sugar 864 Okt 23 15:38 affinecipher.py
4 ...

```

Die Ziffern ganz links sagen uns, dass die Datei `affinecipher.py` user, group und other Ausführungsrechte (genau in dieser Reihenfolge beschrieben) hat.

Mit den wenigen hier beschriebenen Zeilen Code und unter Verwendung der Module `argparse` und `aclib` kann das in Aufgabe 8 geforderte Command Line Tool bereitgestellt werden, das Affine Chiffren nutzt um gewünschte Texte zu ver- oder entschlüsseln.

```

1 #! /usr/bin/python3
2
3 import sys
4 import argparse
5
6 from aclib import decode, acDecrypt, acEncrypt
7
8
9 def crypt(path: str, key: str, fun) -> None:
10     """
11     Encodes/ Decodes the file pointed to by 'path'
12     using the specified function 'fun'.
13     """
14     k1, k2 = decode(key)
15
16     with open(path, "r") as f:
17         print(fun(k1, k2, f.read()))
18
19
20 if __name__ == "__main__":
21     parser = argparse.ArgumentParser(description="Encrypt or...")
22     parser.add_argument("mode", choices=["e", "d"], help="[e]...")
23     parser.add_argument("key", help="String with exactly two...")
24     parser.add_argument("path", help="File path")
25     args = parser.parse_args()
26
27     mode = args.mode
28     key = args.key
29     path = args.path
30
31     if mode == "e":
32         crypt(path, key, acEncrypt)
33     elif mode == "d":
34         crypt(path, key, acDecrypt)

```