Grundlagen der Praktischen Informatik **Sommersemester 2023**
Dr. Stefan Siemer Georg-August-Universität Göttingen
Timo Specht Institut für Informatik

Übungsblatt 10

E-Learning

Absolvieren Sie die Tests bis Di., 25.06., 14 Uhr

Die Tests sind in der Stud.IP-Veranstaltung *Grundlagen der Praktischen Informatik(Informatik II)* unter *Lernmodule* hinterlegt.

Sie können einen Test **nur einmal durchlaufen**. Sobald Sie einen Test starten steht Ihnen nur eine **begrenzte Zeit** zu Verfügung, um den Test zu bearbeiten.

Alle Punkte, die Sie beim Test erreichen, werden ihnen angerechnet.

ILIAS 4-Minuten-Aufgaben – 21 Punkte

Absolvieren sie die Tests *GdPI 10 - 4 Minuten - Kryptographie - ...* für jeden dieser Tests haben Sie nur 4 Minuten Zeit.
(21 Punkte)

Übung

Abgabe bis Di., 25.06., 14 Uhr

Allgemein

Die Aufgaben müssen in **Dreiergruppen** abgegeben werden. Vierergruppen sind ebenfalls möglich.

Es ist **wichtig**, dass Sie sich an folgendes **Verfahren für die Abgabe** halten.
Die Lösungen werden in geeigneter Form in der Stud.IP-Veranstaltung Ihrer Übungsgruppe über das Vips-Modul hochgeladen. Sie müssen diese Abgaben nicht mit Markdown+AsciiMath erstellen. Sie können Ihre Bearbeitungen auch mit LaTeX formatieren, es ist aber auch die direkte Eingabe von Text oder der Upload von Text- und Bilddateien in gängigen Formaten möglich.

Weitere Hinweise zur Abgabe der Lösungen finden Sie in den Aufgabenstellungen.

Aufgabe 1 – 24 Punkte

Python

Nachfolgend ist der Screenshot eines Jupyter-Notebooks abgebildet. Erläutern Sie den Inhalt der einzelnen Zellen ausführlich.
Hinweise

- Siehe *Modules* und *List Comprehensions* in der *Python Documentation* `https://docs.python.org/3/`.
- Die Dokumentation zur `matplotlib` finden Sie unter `https://matplotlib.org/`.

(24 Punkte)

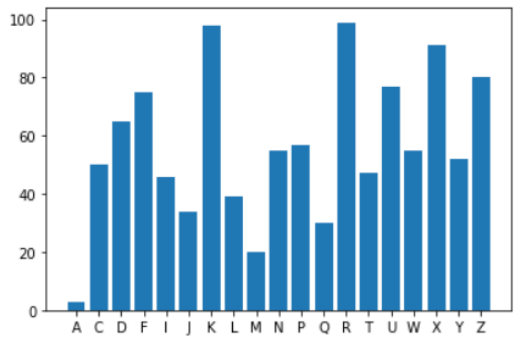
```
import random
import matplotlib.pyplot as plt
```

```
alphabet = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
```

```
freq = {c:random.randint(1,100) for c in alphabet if random.randint(1,10) > 2}
print(len(freq))
print(freq)
```

```
19
{'A': 3, 'C': 50, 'D': 65, 'F': 75, 'I': 46, 'J': 34, 'K': 98, 'L': 39, 'M': 20, 'N': 55,
'P': 57, 'Q': 30, 'R': 99, 'T': 47, 'U': 77, 'W': 55, 'X': 91, 'Y': 52, 'Z': 80}
```

```
plt.bar(range(len(freq)), freq.values(), align='center')
plt.xticks(range(len(freq)), freq.keys())
plt.show()
```



Aufgabe 2 – 20 Punkte

Substitution

Der Schlüsselraum einer Verschlüsselungsfunktion ist die Menge aller möglichen Schlüssel. Für eine (allgemeine) **bijektive** Substitution $s : \Sigma \times K \to \Sigma$ ist der Schlüsselraum K die Anzahl der möglichen Permutationen des Alphabets Σ.

Beispiel
Sei $\Sigma = \{A, B, C, D\}$ und (D, C, B, A) ein Element des Schlüsselraums, dann gilt

$$s\Big(x, (D, C, B, A)\Big) = \begin{cases} D & \text{für } x = A \\ C & \text{für } x = B \\ B & \text{für } x = C \\ A & \text{für } x = D \end{cases}$$

Ein Schlüssel k ist fixpunktfrei, wenn gilt $s_k(x) \neq x$ für alle $x \in \Sigma$. Der Schlüsselraum einer fixpunktfreien Substitution enthält nur fixpunktfreie Schlüssel.
Beispiel
Für die Caesar-Verschlüsselung sind, bis auf Z, alle Schlüssel fixpunktfrei.

Ein Schlüssel k ist involutorisch (selbstinverse) wenn gilt $s\Big(s(x, k), k\Big) = x$. Der Schlüsselraum einer involutorischen Substitution enthält nur involutorische Schlüssel.
Beispiel
Die Caesar-Verschlüsselung mit Schlüsselraum $\{M\}$ ist involutorisch, dieser Speziallfall ist die ROT13-Verschlüsselung.

1. Bestimmen Sie die Größe des Schlüsselraums K der (allgemeinen) Substitution $s : \Sigma \times K \to \Sigma$ für das Alphabet der Großbuchstaben $\Sigma = \{A, \ldots Z\}$.

   Der genaue Wert x muss nicht angegeben werden, aber die Größenordnung $10^n < x < 10^{n-1}$.
   (4 Punkte)

2. Sei $\Sigma = \{00, 01, 10, 11\}$. Bestimmen Sie den maximalen Schlüsselraum der Substitution $s : \Sigma \times K \to \Sigma$, wenn folgendes gilt.

   a) s ist fixpunktfrei
   (8 Punkte)

   b) s ist fixpunktfrei und involutorisch
   (8 Punkte)

   Hinweis. Es müssen die Schlüssel, nicht die Größe des Schlüsselraums angegeben werden.

Bemerkung
Die im 2. Weltkrieg eingesetzte Verschlüsselungsmaschine ENIGMA benutzte konstruktionsbedingt einen involutorischen und fixpunktfreien Schlüsselraum. Das war eine der größten Schwächen dieser Verschlüsselung.
(20 Punkte)

Praktische Übung

Abgabe der Prüfsumme bis Di., 25.06., 14 Uhr
Testat ab Di., 25.06., ab 18 Uhr

Hilfe zum Bearbeiten der praktischen Übungen können Sie grundsätzlich jeden Tag in den Rechnerübungen bekommen. Die Testate finden ebenfalls in **Dreiergruppen** und Vierergruppen statt. Dabei sind die Gruppen identisch zu denen, die auch die theoretischen Aufgaben zusammen bearbeiten. In diesem Fall reserviert nur ein Gruppenmitglied einen Termin. Es ist ausreichend, wenn nur **eine** Person aus der Gruppe eine Prüfsumme abgibt.

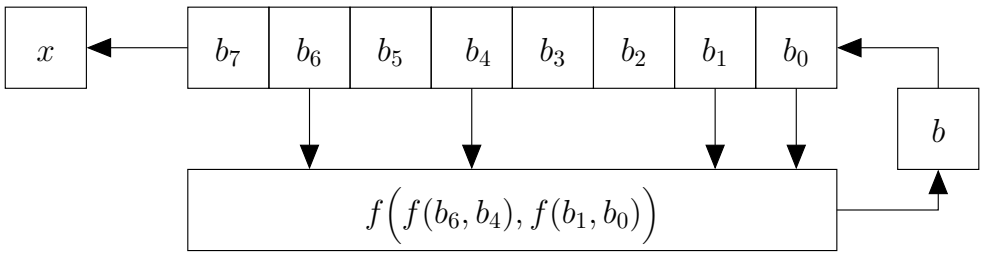
Abgabe der Prüfsumme

- Siehe vorherige Übungen.
- Übermitteln Sie die Prüfsumme mit dem Test *GdPI 10 - Testat*.

Aufgabe 1 – 20 Punkte

Pseudozufall

1. Erstellen Sie ein Python-Skript für das folgende 8-stelligen lineare Schieberegister aus dem Skript.
   - Alphabet $\Sigma = \{A, B, \ldots, Z\}$
   - $b, b_7, \ldots, b_0, x \in \Sigma$
   - $f(k, m) : \Sigma \times \Sigma \to \Sigma$ Verschlüsselungsfunktion der Caesar-Verschlüsselung



   Der Initial-Schlüssel $(b_7, \ldots, b_0)$ und die Länge der zu erzeugenden Folge von Pseudozufallszeichen wird dem Skript über die Kommandozeile übergeben.

2. Produzieren Sie eine Folge von 100000 Pseudozufallszeichen mit Initial-Schlüssel `REPUBLIK`.
   a) Wiederholt sich der Initial-Schlüssel?
   b) Stelle sie die Anzahl der Alphabetszeichen, die in der Folge der Pseudozufallszeichen vorkommen, mit `matplotlib` als Balkendiagramm dar.

(20 Punkte)

Aufgabe 2 – 15 Punkte

Matrixtranposition

Erstellen Sie ein Python-Skript, für die im Skript beschriebene Matrixtransposition. Die Zeilelänge, ob ver- oder entschlüsselt werden soll und die Nachricht (Klartext/Geheimtext) werden auf der Kommandozeile übergeben. Unvollständige Zeilen werden mit X aufgefüllt.

Testen Sie das Skript mit Zeilenlänge 5 und folgenden Nachrichten.

- Klartext `XVMAERZCAESARTREFFENDOLCHENICHTVERGESSEN`
- Geheimtext `XRSEDETEVZAFONVSMCRFLIESAATECCREEERNHHGN`

(15 Punkte)