

Übungsblatt 10

E-Learning

Absolvieren Sie die Tests bis Di., 04.07., 8 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.

Achtung

Manche Tests haben relativ lange Bearbeitungszeiten (≥ 90 min.). Längere Inaktivität während dieser Zeit kann zum einem *timeout* und damit zu einem ungeplanten Ende des Tests führen.

Der Button *Test unterbrechen* verhindert den *timeout*, aber **stoppt nicht das weitere Ablaufen der Bearbeitungszeit**.

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., 04.07., 8 Uhr

Allgemein

Ihre Lösungen werden nur korrigiert, wenn Sie einer Übungsgruppe angehören, d.h. Teilnehmer einer Stud.IP-Veranstaltung *GdPI - Übung - (*Termin*)* sind.

Nur wer in Ilias etwas abgibt kann Punkte bekommen. Siehe dazu die Anmerkungen auf Übungsblatt 02.

Benutzen Sie Markdown mit AsciiMath um die Lösung der Aufgaben zu strukturieren und zu kodieren. Fassen Sie die **Lösungen aller Aufgaben in einer Datei** zusammen.

Formatieren Sie Ihre Abgabe so, dass **die einzelnen Aufgaben klar durch passende Überschriften voneinander** getrennt sind.

Geben Sie die Datei über das Lernmodul *GdPI 10 - Markdown+AsciiMath* ab.

Aufgabe 1 – 8 Punkte

TCP/IP

1. IP-Pakete können auf dem Weg vom Sender-Host zum Empfänger-Host verloren gehen. Wo und warum kann das passieren?
(2 Punkte)
2. IP-Pakete können beim Empfänger-Host in anderer Reihenfolge ankommen, als sie vom Sender-Host abgeschickt wurden. Kann der Empfänger-Host das bemerken? Mit Begründung.
(2 Punkte)
3. TCP-Segmente können auf dem Weg vom Sender-Host zum Empfänger-Host verloren gehen, weil sie in IP-Paketen transportiert werden.
Wie bemerkt der Empfänger-Host verloren gegangene Segmente und wie reagiert er darauf?
(2 Punkte)
4. TCP-Segmente können beim Empfänger-Host in falscher Reihenfolge ankommen, weil sie in IP-Paketen transportiert werden.
Wie bemerkt der Empfänger-Host eine falsche Reihenfolge der Segmente und wie reagiert er darauf?
(2 Punkte)

Aufgabe 2 – 20 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/>.

(20 Punkte)

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

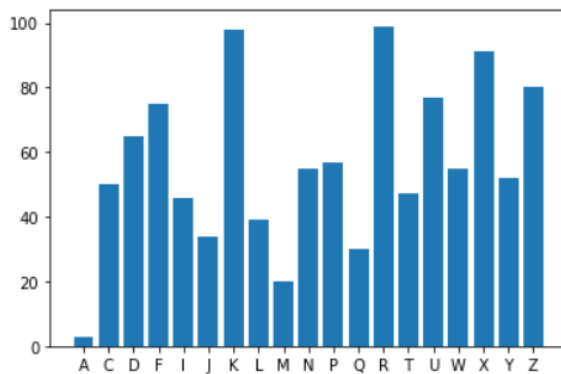
```
alphabet = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
```

```
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 3 – 16 Punkte

Substitution

Der Schlüsselraum einer Verschlüsselungsfunktion ist die Menge aller möglichen Schlüssel. Für eine (allgemeine) **bijektive** Substitution $s : \Sigma \times K \rightarrow \Sigma$ 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

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

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 (selbstinvers) wenn gilt $s(s(x, k), k) = x$. Der Schlüsselraum einer involutorischen Substitution enthält nur involutorische Schlüssel.

Beispiel

Die Caesar-Verschlüsselung mit Schlüsselraum $\{M\}$ ist involutorisch, dieser Spezialfall ist die ROT13-Verschlüsselung.

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

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 $s : \Sigma \times K \rightarrow \Sigma$, wenn folgendes gilt.

- a) s ist fixpunktfrei

(6 Punkte)

- b) s ist fixpunktfrei und involutorisch

(6 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.

Praktische Übung

Abgabe der Prüfsumme bis Di., 04.07., 8 Uhr

Testat ab Mo., 11.07.

Hilfe zum Bearbeiten der praktischen Übungen können Sie grundsätzlich jeden Tag in den Rechnerübungen bekommen.

Am **Mo., 03.07.**, 10-12 Uhr online (3 Tutor*innen) und 18-20 Uhr in Präsenz (2 Tutor*innen), finden **keine Testate** statt. Diese Rechnerübungen sind ausschließlich **für Fragen** reserviert.

Abgabe der Prüfsumme

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

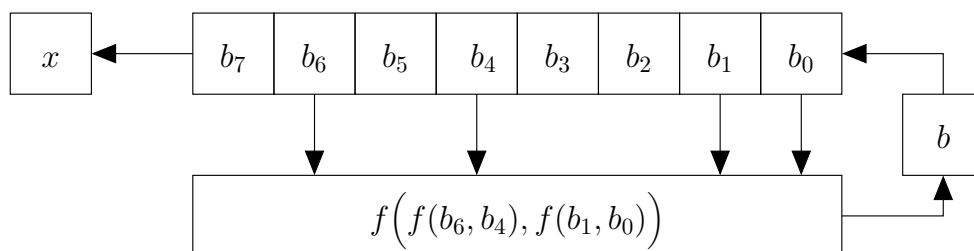
Aufgabe 1 – 20 Punkte

Vorbereitung

Bearbeiten Sie Aufgabe 2 dieser Übung.

Pseudozufall

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



Der Initial-Schlüssel (b_7, \dots, 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

Matrixtransposition

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)