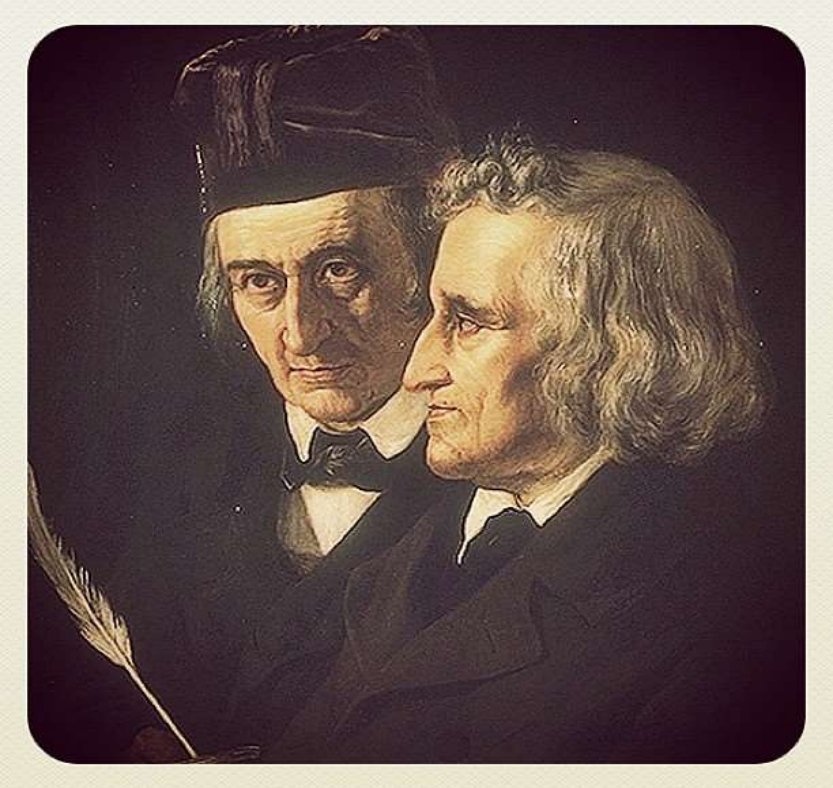
ENTSCHLÜSSELUNG EINIGER MÄRCHEN DER GEBRÜDER GRIMM OHNE KENNTNIS DES GEHEIMSCHLÜSSELS UND DER SCHLÜSSELLÄNGE



GymInf Fachdidaktik I – Herbstsemester 2022

Studienleistung in der Sequenz von Prof. Dr. Juraj Hromkovič und Regula Lacher

juraj.hromkovic@inf.ethz.ch, regula.lacher@inf.ethz.ch

Eingereicht am 1.1.2023 von:

Patrick Suter

GymInf-Student & Gymnasiallehrperson an der Kantonsschule Zug

patrick.suter@unifr.ch, patrick.suter@ksz.ch

1. Einleitung

Die Gebrüder Grimm haben von 1812 bis 1858 insgesamt 200 Märchen[1] verfasst. Diese Märchen geben dieser Studienleistung einen roten Faden, d.h., sie sind hier das verbindende Element. Viele Schüler:innen kennen aus ihrer Kindheit einige dieser Märchen, z.B. «Rapunzel», «Froschkönig», «Hänsel und Gretel». Die Märchen sind meist in einfach verständlicher deutscher Sprache geschrieben, da sie für Erwachsene, aber auch für Kinder gedacht waren.

Die Schüler:innen erlangen ein Verständnis, wie man verschlüsselte Märchen der Gebrüder Grimm entschlüsselt, ohne den Geheimschlüssel und dessen Schlüssellänge zu kennen. Zuerst wird das Vorwissen aus Informatik und Mathematik bis zu Beginn der 4. Gymnasialklasse mittels Repetitionsaufgaben aktiviert und darauf aufbauend werden die Lernenden angeleitet über graduell schwieriger werdende Aufgaben bis hin zur kompletten Entschlüsselung eines Märchens mittels Kasiski-Test und der Häufigkeitsanalyse.

Bei der ansteigenden Schwierigkeit der Aufgaben kommt «das Teile- und Herrsche-Prinzip» als eines der Grundprinzipien der Informatik zur Anwendung. Das schwierige Problem, also das Knacken eines verschlüsselten Märchens ohne Kenntnis des Geheimschlüssels und dessen Schlüssellänge, wird in die folgenden zwei Teilprobleme zerlegt, was eine Lösung erleichtert:

- Wie lang ist der Schlüssel?
- Wenn die Schlüssellänge bekannt ist, wie kommt man dann auf den Schlüssel?

In den folgenden Abschnitten wird das vorhandene Vorwissen beschrieben und es werden die Zielsetzungen erklärt; ein Überblick über das Aufgabenset schliesst diesen Abschnitt ab.

Vorwissen aus Informatik und Mathematik

- Die Schüler:innen kennen bereits aus früheren Informatik-Lektionen die wichtigsten Grundbegriffe und Hauptziele der Kryptographie, den Unterschied zwischen mono- und polyalphabetischen Verfahren.
- Die Schüler:innen haben bereits vorausgegangenen Informatik-Lektionen einfache Aufgaben zur Ver-/Entschlüsselung von Texten mittels Caesar-, Substitutions- und Vigenère-Verschlüsselung gelöst mittels der Brute-Force-Methode, Häufigkeitsanalyse einzelner Buchstaben und Tabula Recta.
- Die Schüler:innen kennen bereits aus dem Programmierunterricht der 3. Gymnasialklasse folgende Programmierelemente: Kommentare, Variablen, Ein- und Ausgabebefehle, Datentypen (Listen, Dictionaries), Verzweigungen, for- und while-Schleifen) und Funktionen (mit und ohne Rückgabewert).
- Die Schüler:innen kennen aus der Mathematik das Konzept der Primzahl, der Primfaktorzerlegung und des grössten gemeinsamen Teilers (ggT) und haben Aufgaben dazu gelöst.

[1] https://www.grimmstories.com/de/grimm_maerchen/list

Zielsetzungen

- Die Schüler:innen wenden ihr Vorwissen aus der Informatik und Mathematik bei den Aufgaben 1-4 zu Zahlen, Primfaktoren, zur Primfaktorzerlegung und zu dem ggT und der Häufigkeitsanalyse einzelner Zeichen an.
- Die Schüler:innen lernen das Konzept von Trigrammen und wenden für die Häufigkeitsanalyse in der Aufgabe 6 an.
- Die Schüler:innen wenden die erlernten Programmierkenntnisse in den Aufgaben 5 und 7 an, um die Häufigkeitsanalyse einzelner Zeichen und Trigramme in Python durchzuführen.
- Die Schüler:innen lernen das Konzept des Kasiski-Tests für die Bestimmung der der Schlüssellänge kennen und wenden dieses in den Aufgaben 8 und 9 an.
- Die Schüler:innen entschlüsseln ein verschlüsseltes Märchen mit bekannter Schlüssellänge und unbekanntem Schlüssel in Aufgabe 10.

Aufgaben-Übersicht

Diese Studienleistung offeriert folgende Aufgaben:

- Aufgabe 1: Zahlen in Märchen herausfinden
- Aufgabe 2: Primzahlen in Märchen erkennen
- Aufgabe 3: Grössten gemeinsamen Teiler (ggT) berechnen
- Aufgabe 4: Die Häufigkeit einzelner Buchstaben im Märchen «Rapunzel» manuell zählen
- Aufgabe 5: Die Häufigkeit einzelner Buchstaben in Python programmieren
- Aufgabe 6: Die Häufigkeit von Trigrammen im Märchen «Hänsel und Gretel» manuell zählen
- Aufgabe 7: Die Häufigkeit von Trigrammen in Python programmieren
- Aufgabe 8: Schlüssellänge nachvollziehen
- Aufgabe 9: Schlüssellänge selbst finden
- Aufgabe 10: Verschlüsseltes Märchen mit Schlüssellänge 3 entschlüsseln (Schlüssel unbekannt)

Aufgaben-Aufbau

Jede Aufgabe hat folgenden gleichen Aufbau:

Titel der Aufgabe (in fetter Schrift)

Aufgabe (in normaler Schrift)

Instruktion zum Lösen der Aufgabe (in kursiver Schrift)

Tipps (in blauer Schrift)

Lösungen (in roter Schrift)

2. Aufgaben

Aufgabe 1: Zahlen in Märchen herausfinden

Märchen benutzen häufig Zahlen. Ergänzen Sie den folgenden Lückentext.

Tipp: Recherchieren Sie die Nomen mit dem Zusatz Märchen im Internet.

Schneewittchen trifft __ Zwerge. Der böse Wolf will __ Geisslein fressen. In einem anderen Märchen gibt es ein Dutzend Brüder, nämlich __! Die Märchenhelden müssen oft __ Proben bestehen, ehe sie ans Ziel gelangen. Dornröschen schläft ___ Jahre. Und in einem weiteren Märchen kommen ___ Schwäne vor. Übrigens haben die Gebrüder Grimm von 1812 bis 1858 insgesamt ___ Märchen geschrieben.

7 Zwerge, 7 Geisslein, 12 Brüder, 3 Proben, 100 Jahre, 6 Schwäne, 200 Märchen

Aufgabe 2: Primzahlen in Märchen erkennen

Bestimmen Sie, ob es sich bei den folgenden Zahlen um Primzahlen handelt, und zeigen Sie, durch welche Zahlen diese teilbar sind.

Tipp I: Eine Primzahl ist eine natürliche Zahl, die grösser als 1 und ausschliesslich durch sich selbst und durch 1 teilbar ist.
Tipp II: Alle geraden Zahlen > 2 sind keine Primzahlen, da sie auch durch 2 teilbar sind.

Zahl	Primzahl?	Durch welche Zahlen ist die Zahl teilbar?
3		
6		
7		
12		
100		
200		

Zahl	Primzahl?	Durch welche Zahlen ist die Zahl teilbar?
3	Ja	3, 1
6	Nein	6, 3, 2, 1
7	Ja	7, 1
12	Nein	12, 6, 4, 3, 2, 1
100	Nein	100, 50, 25, 20, 10, 5, 4, 2 und 1
200	Nein	200, 100, 50, 40, 25, 20, 10, 5, 4, 2 und 1

Aufgabe 3: Grössten gemeinsamen Teiler (ggT) berechnen

Zerlegen Sie die Zahlen in ihre Primfaktoren, um sie als Multiplikation von Primzahlen darzustellen (sogenannte Primfaktorzerlegung). Berechnen Sie dann den ggT.

Tipp I: Die Zahl 1 wird in der Primfaktorzerlegung nicht aufgeführt, da es sich per Konvention nicht um eine Primzahl handelt.
Tipp II: In der Primfaktorzerlegung stehen Primzahlen. Die Zahl 9 kann also nicht in der Primfaktorzerlegung stehen, da sie keine Primzahl ist und in 3x3 zerlegt werden kann.

Zahl	Primfaktorzerlegung	ggT (3, 6, 12)
3		
6		
12		

Zahl	Primfaktorzerlegung	ggT (50, 90, 190)
50		
90		
190		

Zahl	Primfaktorzerlegung	ggT (30, 80, 105)
30		
80		
105		

Zahl	Primfaktorzerlegung	ggT (3, 6, 12) = 3
3	3	– Die Primzahl 3 ist in allen drei Primfaktorzerlegungen je 1x enthalten. – Die Primzahl 2 ist nur bei der Primfaktorzerlegung von 6 und 12 vorhanden, kann also nicht in den ggT miteinbezogen werden.
6	3x2	
12	3x2x2	

Zahl	Primfaktorzerlegung	ggT (50, 90, 190) = 10
50	5x5x2	– Die Primzahlen 2 und 5 sind in allen drei Primfaktorzerlegungen je 1x enthalten. – Die Primzahl 3 ist nur bei der Primfaktorzerlegung von 90 vorhanden. – Die Primzahl 19 ist nur bei der Primfaktorzerlegung von 190 vorhanden.
90	5x3x3x2	
190	5x2x19	

Zahl	Primfaktorzerlegung	ggT (30, 80, 105) = 5
30	5x3x2	– Die Primzahl 5 ist in allen drei Primfaktorzerlegungen je 1x enthalten. – Die Primzahl 2 ist bei der Primfaktorzerlegung von 80 4x vorhanden. – Die Primzahl 3 ist bei der Primfaktorzerlegung von 30 und 105 1x vorhanden. – Die Primzahl 7 ist nur bei der Primfaktorzerlegung von 105 1x vorhanden.
80	5x2x2x2x2	
105	5x7x3	

Aufgabe 4: Die Häufigkeit einzelner Buchstaben im Märchen «Rapunzel» manuell erkennen

Zählen Sie die Häufigkeiten einzelner Buchstaben mittels Strichliste. Addieren Sie die jeweiligen Häufigkeiten in der Spalte «absolute Häufigkeit», bilden Sie die Summe aller Buchstaben und rechnen Sie die «relative Häufigkeit» der drei häufigsten Buchstaben aus. Der Text verzichtet absichtlich auf die grammatikalisch Gross- bzw. Kleinschreibung. Kommas und Punkte an Satzenden dürfen Sie ignorieren.

Tipp: Relative Häufigkeit = absolute Häufigkeit / Summe aller Buchstaben

rapunzel war das schoenste kind unter der sonne. als es zwoelf jahre alt war, schloss es die zauberin in einen turm, der in einem walde lag, und weder treppe noch tuere hatte, nur ganz oben war ein kleines fensterchen. wenn die zauberin hineinwollte, so stellte sie sich hin und rief: rapunzel, rapunzel, lass mir dein Haar herunter. rapunzel hatte lange praechtige haare, fein wie gesponnenes gold.

	Strichliste	**Absolute Häufigkeit**	**Relative Häufigkeit**
a			
b			
c			
d			
e			
f			
g			
h			
i			
j			
k			
l			
m			
n			
o			
p			
q			
r			
s			
t			
u			
v			
w			
x			
y			
z			
Summe			

Lösung: a: 25, b: 3, c: 5, d: 12, e: 57 (17.8%), f: 4, g: 6, h: 14, i: 22, j: 1, k: 2, l: 18, m: 3, n: 38 (11.8%), o: 10, p: 8, q: 0, r: 26 (8.1%), s: 20, t: 16, u: 13, v: 0, w: 9, x: 0, y: 0, z: 8. Summe = 321

Aufgabe 5: Die Häufigkeit einzelner Buchstaben in Python programmieren

Das manuelle Zählen der Häufigkeiten einzelner Buchstaben in einem Text wie in Aufgabe 4 kann ziemlich mühsam und fehleranfällig sein. Deshalb dürfen Sie als Nächstes ein kleines Programm in Python schreiben, das die Häufigkeitsanalyse schneller als beim manuellen Zählen durchführen lässt. Diese Aufgabe hat 3 Teilaufgaben.

a) Schreiben Sie ein Programm, das einen Text und Buchstaben in der Kommandozeile abfragt, den gesuchten Buchstaben im Text zählt und dann die absolute Häufigkeit eines einzelnen Buchstabens ausgibt. Strukturieren Sie den Code gemäss den drei Blöcken:

1. *Input: Analysierender Text und gesuchter Buchstabe*
2. *Zählen: Gesuchten Buchstaben im Text zählen*
3. *Ausgabe: Gesuchter Buchstabe und dessen absolute Häufigkeit*

Tipp zum Input: Die Methode «input()» fragt bei der Programmausführung in der Konsole nach einer Eingabe. Mit dieser Methode können Sie nacheinander den zu analysierenden Text und den gesuchten Buchstaben abfragen. Speichern Sie die beiden Inputs in zwei Variablen «text» und «buchstabe».
Tipp zum Zählen: Die Methode «count()» zählt im Text die absolute Häufigkeit eines Buchstabens und kann auf der Variablen «text» aufgerufen werden.
Tipp zur Ausgabe: Die Methode «print()» gibt den Wert einer Variablen aus.

Lösung:

```
#Eingaben: Text und Buchstabe
text = input ("Geben Sie hier den Text ein, den Sie analysieren möchten: ")
buchstabe = input ("Geben Sie hier den Buchstaben ein, den Sie im Text zählen möchten: ")

#Zählen
zaehler = text.count(buchstabe)

#Ausgabe
print(buchstabe, zaehler)
```

b) Erweitern Sie Ihren Python-Code wie folgt:

- *Ausgabe: Gesuchter Buchstabe und dessen relative Häufigkeit*
- *Ausgabe: Länge des zu analysierenden Textes*

Tipp zur Berechnung der Textlänge: Um die Länge eines Strings in Python zu bestimmen, können Sie die «len()» Funktion benutzen. Als Antwort erhalten Sie die Anzahl der Elemente des Strings zurück.
Tipp zur Berechnung der relativen Häufigkeit: Die relative Häufigkeit ist die absolute Häufigkeit geteilt durch die Länge des zu analysierenden Textes.

Lösung:

```
#Eingaben: Text und Buchstabe
text = input ("Geben Sie hier den Text ein, den Sie analysieren möchten: ")
buchstabe = input ("Geben Sie hier den Buchstaben ein, den Sie im Text zählen möchten: ")

#Zählen
zaehler = text.count(buchstabe)

#Ausgabe
print(buchstabe, zaehler)
print(buchstabe, int(zaehler / len(text) * 100), "%")
print("Textlänge:", len(text))
```

c) Die Märchen der Gebrüder Grimm sind in deutscher Sprache mit Umlauten, Doppel-S, und mit Interpunktionszeichen geschrieben. Erweitern Sie Ihren Code wie folgt:

- *Umlaute und Doppel-S umformen (ß -> SS, Ü -> UE, Ä -> AE, etc.)*
- *Interpunktionszeichen eliminieren*
- *Text in Kleinschreibung umformen*

Wählen Sie ein anderes Grimm'sches Märchen auf der Webseite https://www.grimmstories.com/de/grimm_maerchen/list und führen Sie den Code aus.

Tipp zur Umformung: Mit der Methode «replace()» kann z.B. ein String in einen anderen String umgeformt werden.
Tipp zur Elimination: Die Elimination besteht in einer Umformung.
Tipp zur Umwandlung in die Kleinschreibung: Mit der Methode «lower()» kann z.B. ein String in Kleinbuchstaben geändert werden.

Lösung:

```python
#Eingaben: Text und Buchstabe
text = input ("Geben Sie hier den Text ein, den Sie analysieren möchten: ")
buchstabe = input ("Geben Sie hier den Buchstaben ein, den Sie im Text zählen möchten: ")

#Zählen
zaehler = text.count(buchstabe)

#Umlaute umformen
text = text.replace("ß", "SS")
text = text.replace("Ö", "OE")
text = text.replace("Ü", "UE")
text = text.replace("Ä", "AE")

#Interpunktion löschen
text = text.replace(".", "")
text = text.replace(",", "")
text = text.replace(":", "")
text = text.replace(";", "")
text = text.replace("'", "")
text = text.replace("-", "")


#Text in Kleinschreibung umwandeln
text = text.lower()

#Ausgabe
print(buchstabe, zaehler)
print(buchstabe, int(zaehler / len(text) * 100), "%")
print("Textlänge:", len(text))
```

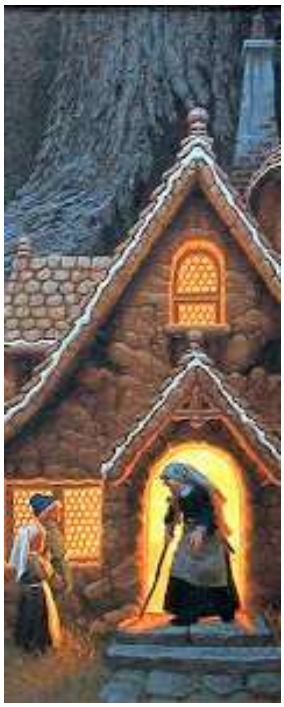
Aufgabe 6: Die Häufigkeit von Trigrammen im Märchen «Hänsel und Gretel» finden

Zählen Sie die Häufigkeiten der sechs häufigsten Trigramme in der deutschen Sprache, indem Sie diese im folgenden Text mit unterschiedlichen Farben übermalen. Tragen Sie die Häufigkeit in die Strichliste unten ein und summieren sie diese in der Spalte «absolute Häufigkeit».

Tipp I: Ein Trigramm kann auch ein Teilwort sein, z.B. das Trigramm «nde» als Teilwort des Wortes «Kinder».

Vor einem grossen Walde wohnte ein armer Holzhacker mit seiner Frau und seinen zwei Kindern; das Buebchen hiess Haensel und das Maedchen Gretel. Er hatte wenig zu beissen und zu brechen, und einmal, als grosse Teuerung ins Land kam, konnte er das taegliche Brot nicht mehr schaffen. Wie er sich nun abends im Bette Gedanken machte und sich vor Sorgen herumwaelzte, seufzte er und sprach zu seiner Frau: "Was soll aus uns werden? Wie koennen wir unsere armen Kinder ernähren, da wir für uns selbst nichts mehr haben?" - "Weisst du was, Mann," antwortete die Frau, "wir wollen morgen in aller Fruehe die Kinder hinaus in den Wald fuehren, wo er am dicksten ist. Da machen wir ihnen ein Feuer an und geben jedem noch ein Stueckchen Brot, dann gehen wir an unsere Arbeit und lassen sie allein. Sie finden den Weg nicht wieder nach Haus, und wir sind sie los." - "Nein, Frau," sagte der Mann, "das tue ich nicht; wie sollt ich's uebers Herz bringen, meine Kinder im Walde allein zu lassen! Die wilden Tiere würden bald kommen und sie zerreissen.".

6 häufigste Trigramme	Strichliste	Absolute Häufigkeit
ein		
ich		
nde		
die		
und		
der		



ein: 12, ich: 9, nde: 5, die: 3, und: 10, der: 6

Aufgabe 7: Die Häufigkeit von Trigrammen in Python programmieren

Das manuelle Zählen der Häufigkeiten von Trigrammen in einem Text wie in Aufgabe 6 kann ziemlich mühsam sein. Zudem ist das manuelle Zählen fehleranfällig. Deshalb dürfen Sie als Nächstes ein kleines Programm in Python schreiben, das die Häufigkeitsanalyse schneller als manuell durchführen lässt.

Schreiben Sie ein Programm, das einen Text und ein Trigramm in der Kommandozeile abfragt, den gesuchten Buchstaben im Text zählt und dann die absolute Häufigkeit des Trigramms ausgibt. Strukturieren Sie den Code gemäss den drei Blöcken:

1. *Input: Analysierender Text und gesuchtes Trigramm*
2. *Zählen: Gesuchten Buchstaben im Text mittels Iteration über den Text zählen*
3. *Ausgabe: Gesuchtes Trigramm und dessen absolute Häufigkeit*

Tipp zum Zählen: Mit einer for-Schleife können Sie über den Text iterieren. Dabei soll «trigramm_pos» als Variable mit der aktuellen Startposition des Trigramms nach jedem Schleifendurchgang um eins erhöht werden, bis diese den drittletzten Buchstaben im Text erhält. Der Schleifenkörper soll das Trigramm ab der jeweiligen Startposition mit dem gesuchten Trigramm vergleichen und bei Übereinstimmung den Zähler der Trigrammhäufigkeit um eins erhöhen.

Lösung:

```
#Eingaben: Text und Trigramm
text = input ("Geben Sie hier den Text ein, den Sie analysieren möchten: ")
trigramm = input ("Geben Sie hier das Trigramm ein, das Sie im Text zählen möchten: ")


#Iteration über Text und Zählung der absoluten Häufigkeit des gesuchten Buchstabens
zaehler = 0
trigramm_pos = 0

for trigram_pos in range (len(text)-2):
    if (text[trigramm_pos]+text[trigramm_pos+1]+text[trigramm_pos+2]) == trigramm:
        zaehler = zaehler + 1
    trigramm_pos = trigramm_pos + 1

#Ausgabe
print(trigramm, zaehler)
```

Aufgabe 8: Schlüssellänge nachvollziehen

Im Märchen «Das tapfere Schneiderlein» lesen Sie den vereinfachten Satz «Das ist das Haus von ihm und nicht das Haus des Wichtels.», welcher mit dem Schlüssel «tap» und der Schlüssellänge 3 verschlüsselt wird.
Das ergibt dann für die ersten Wörter den folgenden Geheimtext,
aufgelistet in Dreierblöcken:

Klartext: `das ist das hau svo nih mun dni cht das hau sde swi cht els`
Schlüssel: `tap tap tap tap tap tap tap tap tap tap tap tap tap tap tap`
Geheimtext: `wah bsi wah aaj lvd giw fuc wnx vhi wah aaj ldt lwx vhi xlh`

a) Schreiben Sie die Positionen für folgende Trigramme in dem Geheimtext auf:

Trigramm	**Startposition im Text**
«wah»	
«aaj»	

wah: 1, 7, 28
aaj: 10, 31

b) Berechnen Sie den Abstand der Positionen und führen Sie eine Primfaktorzerlegung durch:

Trigramm	**Abstand**	**Primfaktorzerlegung**
1.&2. «wah»		
2.&3. «wah»		
1.&3. «wah»		
1.&2. «aaj»		

1.&2. «wah»	6 = 7-1	3x2
2.&3. «wah»	21 = 28-7	7x3
1.&3. «wah»	27 = 28-1	3x3x3
1.&2. «aaj»	21 = 31-10	7x3

c) Finden Sie den grössten gemeinsamen Teiler (ggT) der obigen Primfaktorzerlegung:

ggT	

3 (Die 3 ist die einzige Primzahl, die in allen 4 Zahlen 1x enthalten ist. Die Primzahlen 2 und 7 sind nicht in allen 4 Zahlen enthalten.)

d) Entspricht diese Zahl der Schlüssellänge?

Schlüssellänge	

Ja

Aufgabe 9: Schlüssellänge selbst finden

Sie fangen den folgenden Geheimtext des letzten Absatzes eines Märchens ab und möchten die Schlüssellänge der Verschlüsselung herausfinden. Der Geheimtext ist in Zehnerblöcken mit je 50 Zeichen pro Reihe dargestellt, um die Zählbarkeit zu verbessern.

```
qbofhgojnk zqboyiabmw qbyjjylrqb oxeqsiafht htfjxsciwg
hfogpwxiph ghpzjrojnk zqbhcnjyps scwqpsofvc rjjwsszwpx
yvhjnsyxps tsavtsawyz jrpwiidxps ufaaxjnzth dscxwiqjji
yiwzdiesdn appscstxoz pnjrlxoosj jylrabdnas tqeusjnppn
cswfqtpsqb owesqjjzlz prpwscwkeg eykhojnkzq bwdypcezjr
efjnejjaty evcjnafyps cakfqwaioj qaojjpczjb psdsczi
```

a) Führen Sie den Kasiski-Test zur Bestimmung der Schlüssellänge durch, indem Sie die folgenden 3 Schritte anwenden:

1. *Suchen Sie das Trigramm «qbo», das 4x im obigen Geheimtext vorkommt, und notieren Sie deren Startpositionen im Geheimtext.*
2. *Berechnen Sie die Abstände der Positionen und zerlegen Sie sie in die Primfaktoren.*
3. *Finden Sie den grössten gemeinsamen Teiler (ggT) der Primfaktorzerlegung.*

Tipp zum ggT und Schlüssellänge: Falls der ggT der Primfaktorzerlegung 1 ist, so ist bei der Verschlüsselung ein Trigramm zufällig entstanden, was selten vorkommen kann. Der Schlüssel hat beim obigen Text sicher nicht die Länge 1, da sonst das Märchen lesbar wäre. In solchen Fällen schaut man, welches Trigramm dafür verantwortlich ist, dass der ggT = 1 ist, und man eliminiert dieses Trigramm.

Trigramm	**Startposition im Text**

Trigramm	**Abstand**	**Primfaktorzerlegung**
1.&2. «qbo»		
1.&3. «qbo»		
1.&4. «qbo»		
2.&3. «qbo»		
2.&4. «qbo»		
3.&4. «qbo»		

ggT = mögliche Schlüssellänge alle 4 gefundenen Trigramme	

An welcher Position ist ein Trigramm zufällig entstanden?	

ggT = mögliche Schlüssellänge 3 von 4 gefundenen Trigrammen (ohne das zufällig entstandene Trigramm)	

```
qbofhgojnk zqboyiabmw qbyjjylrqb oxeqsiafht htfjxsciwg
hfogpwxiph ghpzjrojnk zqbhcnjyps scwqpsofvc rjjwsszwpx
yvhjnsyxps tsavtsawyz jrpwiidxps ufaaxjnzth dscxwiqjji
yiwzdiesdn appscstxoz pnjrlxoosj jylrabdnas tqeusjnppn
cswfqtpsqb owesqjjzlz prpwscwkeg eykhojnkzq bwdypcezjr
efjnejjaty evcjnafyps cakfqwaioj qaojjpczjb psdsczi
```

Trigramm	**Startposition im Text**
qbo	1, 12, 29, 209

Trigramm	**Abstand**	**Primfaktorzerlegung**
1.&2. «qbo»	11 = 12-1	11
1.&3. «qbo»	28 = 29-1	2x2x7
1.&4. «qbo»	208 = 209-1	2x2x2x2x13
2.&3. «qbo»	17 = 29-12	17
2.&4. «qbo»	197 = 209-12	197
3.&4. «qbo»	180 = 209-29	2x2x5x3x3

ggT = mögliche Schlüssellänge alle 4 gefundenen Trigramme	**1**

An welcher Position ist ein Trigramm zufällig entstanden?	**12**

ggT = mögliche Schlüssellänge 3 von 4 gefundenen Trigrammen (ohne das zufällig entstandene Trigramm)	**4 = 2x2**

Schlüssel: wolf

Märchen: Der Wolf und die sieben jungen Geisslein

Klar-/Geheimtext in Satzform:

Und als der Wolf an den Brunnen kam und sich der Wolf ueber das
Qbo fhg ojn kzqb oy iab mwqbyjj ylr qbo xeqs iaf htht fjxsc iwg

Wasser bueckte und der Wolf trinken wollte, da zogen ihn die
hfogpw xiphghp zjr ojn kzqb hcnjyps scwqps, of vcrjj wss zwp

schweren Steine hinein, und er musste jaemmerlich ersaufen. Und als
xyvhjnsy xpstsa vtsawy, zjr pw iidxps ufaaxjnzthd scxwiqjj. Iyi wzd

die sieben Geisslein das sahen, kamen sie eilig herbeigelaufen und
ies dnapps cstxozpnj rlx oosjj, ylrab dna stqeu sjnppncswfqtps qbo

riefen laut: Der Wolf ist tot! Der Wolf ist tot! und tanzten mit
wesqjj zlzp: rpw scwk ege ykh! Ojn kzqb wdy pce! Zjr efjnejj aty

ihrer Mutter vor Freude um den Brunnen herum.
evcjn afypsc akf qwaioj qa ojj pczjbps dsczi.

Aufgabe 10:
Verschlüsseltes Märchen mit Schlüssellänge 3 entschlüsseln (Schlüssel unbekannt)

Ein Märchen wurde mit Schlüssellänge 3 mittels der Tabula Recta verschlüsselt. Den Schlüssel kennen Sie nicht. Sie wissen aber, dass der Schlüssel die Länge 3 hat. Können Sie den nachfolgenden Geheimtext entschlüsseln? Finden Sie heraus, aus welchem Märchen er stammt.

```
dpe  aby  noo  mzo  erb  ecz  ecm
ttl  zly  ily  ihm  eiu  ejv  cwy
nwy  rtc  njh  dsu  npw  hsc  eio
riy  liu  ejv  cwy  njh  dth  dac
cwm  cwq  igl  tth  ucx  srb  wpy
rbn  ecu  lay  vdy  gay  ico  niy
rsy  mwc  mby  lwy  rtc  njh  dac
ehm  ecm  irb  ubx  itu  srb  ecc
esy  rjh  dsc  eiu  ejv  cwy  ncc
czn  ecg  iix  ece  otj  frb  eco
nsz  ica  ecu  nec  czj  ire  pxw
kec  czo  nsx  auc  nvy  nsc  ejy
bgc  gth  ajw  hph  pxw  kec  czj
ire  pxw  kjh  dau  sth  aaf  evo
tth  kdy  rcf  exh  icx  itm  cwo
ehm  ea
```

a) Schreiben Sie alle Buchstaben und deren Häufigkeit im Märchentext an erster, zweiter und dritter Stelle in die nachfolgende Tabelle und zählen sie die absolute Häufigkeit der notierten Buchstaben. Als zusätzliche Hilfestellung sind die 3 häufigsten Buchstaben bereits notiert.

1. Stelle		**2. Stelle**		**3. Stelle**	
Buchstaben	Absolute Häufigkeit	Buchstaben	Absolute Häufigkeit	Buchstaben	Absolute Häufigkeit
e		c		y	
n		t		c	
i		j		h	

Tipp I: Die Buchstaben an den ersten Stellen sind:
danmeeetziieecnrndnherlecnddccituswrelvginrmmlrndeeiu

iseerdeecnceieofeniencipkcnannebgahpkcipkdsaetkreiicee

Tipp II: Die Buchstaben an den zweiten Stellen sind:
pbozrcctllhijwwtjspsiiijwjtawwgtcrpbcadaciswbwtjahcrb

trcsjsijwczcictrcsccezrxezsuvsjgtjpxezrxjatavtdcxctwha

Tipp III: Die Buchstaben an den dritten Stellen sind:

```
eyoobzmlyymuvyychuwcoyuvyhhcmqlhxbynuyyyoyycyychcmmbx
ubcyhcuvycngxejbozaucjewcoxcycychwhwcjewhuhfohyfhxmom
```

1. Stelle		2. Stelle		3. Stelle	
Buchstaben	Absolute Häufigkeit	Buchstaben	Absolute Häufigkeit	Buchstaben	Absolute Häufigkeit
e	23	c	15	y	20
n	13	t	11	c	15
i	12	j	10	h	12

b) Finden Sie in der obigen Tabelle in Teilaufgabe a) den häufigsten Buchstaben und notieren Sie diesen in der nachfolgenden Tabelle. Gemäss der Häufigkeitsanalyse über die Verteilung der Buchstaben in der deutschen Sprache ist dieser Buchstabe im Klartext vermutlich der Buchstabe «e».

1. Stelle der Trigramme		2. Stelle der Trigramme		3. Stelle der Trigramme	
Häufigster Buchstabe	Absolute Häufigkeit	Häufigster Buchstabe	Absolute Häufigkeit	Häufigster Buchstabe	Absolute Häufigkeit

1. Stelle		2. Stelle		3. Stelle	
Buchstaben	Absolute Häufigkeit	Buchstaben	Absolute Häufigkeit	Buchsta-ben	Absolute Häufigkeit
e	23	c	15	y	20

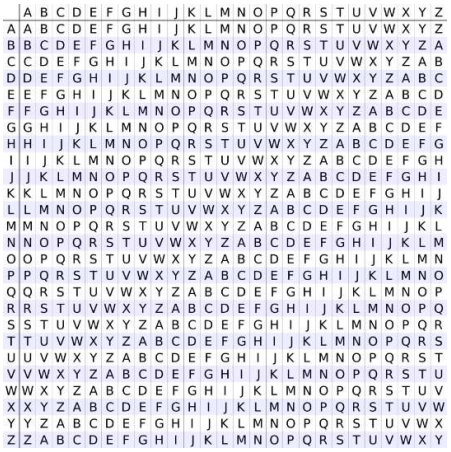
c) Tragen Sie nun die drei häufigsten Buchstaben in die Zeile «e» ein, denn mit hoher Wahrscheinlichkeit ist der häufigste Buchstabe im Klartext ein «e». Finden Sie mit der Caesar-Verschiebechiffre heraus, was der Geheimschlüssel ist; dieser steht nämlich in der Zeile «a».

	1. Stelle	2. Stelle	3. Stelle
e			
d			
c			
b			
a			

Tipp I: Bei der Caesar-Chiffre handelt es sich um eine Verschiebungsverschlüsselung um eine gewisse Anzahl Positionen.
Tipp II: Nehmen Sie für die 2. Stelle bitte den zweithäufigsten Buchstaben, da der häufigste Buchstabe nicht zum richtigen Schlüssel führt.

	1. Stelle	2. Stelle	3. Stelle
e	e	t	y
d	d	s	x
c	c	r	w
b	b	q	v
a	a	p	u

d) Entschlüsseln Sie die erste und zweite Zeile des Geheimtextes mittels des gefundenen Schlüssels und der Tabula Recta.



Erste Zeile

Geheimtext: dpe aby noo mzo erb ecz ecm
Schlüssel:
Klartext:

Zweite Zeile

Geheimtext: ttl zly ily ihm eiu ejv cwy
Schlüssel:
Klartext:

Tipp I: Schreiben Sie den Schlüssel wiederholend in die Zeile «Schlüssel».
Tipp I: Die erste Zeile der Tabula Recta betrifft den Schlüssel und die erste Spalte betrifft den Klartext.

Erste Zeile

Geheimtext: dpe aby noo mzo erb ecz ecm
Schlüssel: apu apu apu apu apu apu apu
Klartext: dak ame nzu mkue che nfe nst

Zweite Zeile

Geheimtext: ttl zly ily ihm eiu ejv cwy
Schlüssel: apu apu apu apu apu apu apu
Klartext: erz wei wei sse tae ubc hen

e) Wissen Sie nun, welches Märchen hinter dem Geheimtext steckt?

Antwort	

Märchen: Aschenputtel
Schlüssel: apu
Klartext in Satzform: Da kamen zum Küchenfenster zwei weisse Taeubchen herein, und danach die Turteltaeubchen, und endlich schwirrten und schwaermten alle Voeglein unter dem Himmel herein und liessen sich um die Asche nieder. Und die Taeubchen nickten mit den Koepfchen und fingen an pick, pick, pick, pick, und da fingen die uebrigen auch an pick, pick, pick, pick, und lasen alle guten Koernlein in die Schuessel.

3. Fazit

Das Fazit der hier vorliegenden Studienleistung wird anhand der folgenden Stichpunkte skizziert: Vorwissen, Zielsetzungen, Strukturierung, Aufgaben, Lerneffekte, roter Faden, Originalität und Relevanz.

Vorwissen

Das Vorwissen der Schüler:innen wurde in klarer Weise in der Einleitung niedergeschrieben. Es umfasst sowohl Vorwissen aus der Informatik wie auch der Mathematik. Das Vorwissen wird in den ersten einfachen Aufgaben aktiviert und vertieft.

Zielsetzungen

Die Zielsetzungen für die Schüler:innen sind in der Einleitung verständlich niedergeschrieben und zeigen den Bezug zu den Aufgaben.

Strukturierung

Die hier vorliegende Studienleistung ist übersichtlich strukturiert. Die Aufgaben entsprechen den Zielsetzungen und das Schwierigkeitslevel steigt kontinuierlich an, ohne die Schüler:innen zu überfordern.

Aufgaben

Das Aufgabenset von insgesamt 10 Aufgaben enthält sowohl Informatik-Aufgaben auf Papier und in Python als auch Mathematik-Aufgaben.

Die Aufgaben sind gemäss Zielsetzungen modularisiert und haben jeweils den gleichen Aufbau (**Titel,** Aufgabentext, *Instruktion,* Tipps, Lösungen).

Originalität / Roter Faden

Anhand des angewandten Themas der Märchen der Gebrüder Grimm zieht sich ein roter Faden durch die Studienleistung.

Relevanz

Die Entschlüsselung ohne Kenntnis des Schlüsselwortes und dessen Länge wird in den gymnasialen Lehrmitteln oft nur am Rande oder für die Studierenden planmässig erst wieder im Studium an der Universität. Die hier vorliegende Studienleistung schliesst diese Lücke auf gymnasialer Ebene.