Aufgabe 2.1 (4+2 Pkt.)

In der Vorlesung wurde die Vigenère-Chiffre besprochen. Ein Angriff auf die Chiffre besteht aus zwei Schritten: Bestimmung der Schlüssellänge und eine anschließende Häufigkeitsanalyse der Verschiebechiffren. Die Friedman-Methode zur Bestimmung der Schlüssellänge basiert auf Koinzidenzindizes.

a) Lösen Sie die SPOX-Aufgabe *Friedman-Methode für Vigenère-Chiffren*.

b) Im Rubikon finden Sie einen Vigenère-verschlüsselten deutschen Text (*Aufgabe-2.1.txt*). Bestimmen Sie die Schlüssellänge. Um welchen Klartext handelt es sich (Angabe der ersten Zeile ist ausreichend)?

Aufgabe 2.2 (2+1 Pkt.)

Der folgende Vigenère-verschlüsselte deutsche Text soll mit der Kasiski-Methode entziffert werden, dabei sind Leerzeichen und Zeilenumbrüche zu ignorieren.

```
vixjd alras vgwkk xhthf jaiga eudza gcwlm lwtan vegaw iwdfe
gugrt tkgxr wtsso ikcva lrvek fwhxh eelbz lndks xknok cwrxh
yegsd ivgwn gzuhk huhmd fuxaw rmqsg nmybx qwimr rwbru hxmke
gcwrn mvefo xaxmy ekzms zdlan ruhmv mrwds llnte bcwni zjtxh
wnudc agmli ls
```

a) Welche Buchstaben-Tripel kommen mehrfach im Text vor? Wie lang ist der Schlüssel?

b) Bestimmen Sie den Schlüssel und den Klartext.

Hinweis: Als Schlüssel wurde (unvorsichtigerweise) ein deutsches Wort verwendet. Es bietet sich die Methode mit paarweisen Koinzidenzindizes an, z. B. mit Hilfe der Häufigkeitstabelle im Rubikon.

Aufgabe 2.3 (1+1+2+1 Pkt.)

Aus dem Koinzidenzindex für einen kompletten Vigenère-verschlüsselten Text lässt sich bereits eine grobe Schätzung für die Länge des verwendeten Schlüssels berechnen.

Wir nehmen an, die Chiffre c sei durch Vigenère-Verschlüsselung aus einem Klartext m der Länge n entstanden. Der verwendete Schlüssel sei eine zufällig unter Gleichverteilung gezogene Zeichenfolge der Länge ℓ. Der Text m sei „typisch“ für die zugrundeliegende Sprache mit Koinzidenzindex I_{lang}. Für zufällig unter Gleichverteilung gezogene Zeichenfolgen über dem verwendeten Alphabet Σ ergebe sich dagegen der Koinzidenzindex $I_{\text{rand}} = 1/|\Sigma|$.

a) Wie lautet der Koinzidenzindex I der Chiffre, wenn der Schlüssel die Länge $\ell = 1$ besitzt?

b) Wie lautet der Koinzidenzindex I der Chiffre, wenn der Schlüssel sehr lang ist ($\ell = n$)?

c) Stellen Sie eine Formel für I bei beliebiger Schlüssellänge $\ell \in \{1, \ldots, n\}$ auf.

Tipp: Bei gegebener Schlüssellänge gibt es Paare von Positionen, die mit derselben Cäsar-Chiffre verschlüsselt werden, und Paare von Positionen, die mit unabhängig voneinander gewählten Cäsar-Chiffren verschlüsselt werden. Sie dürfen annehmen, n sei durch l teilbar.

d) Lösen Sie die Formel aus c) nach ℓ auf, um die gesuchte Näherung zu erhalten.

Aufgabe 2.4 (2 Pkt.)

Sie haben in der Vorlesung die Playfair-Verschlüsselung kennen gelernt. Verschlüsseln Sie den Text `KRYPTOGRAPHIEMACHTFREUDE` mittels folgender Playfair-Verschlüsselung der Zweierpaare von Buchstaben. Verwenden Sie dabei den Buchstaben

- (zyklisch) direkt rechts neben dem Buchstaben bei gleicher Zeile,
- (zyklisch) direkt unterhalb des Buchstaben bei gleicher Spalte, bzw.
- den Buchstaben auf der im Uhrzeigersinn nächsten Ecke des aufgespannten Rechteckes in allen anderen Fällen.

Verwenden Sie zur Verschlüsselung den Schlüssel `CIPHER`.
Hinweis: Denken Sie daran, `I` und `J` als den gleichen Buchstaben zu behandeln!