Brechen der Vigenère-Verschlüsselung (Teil 1) - Lösung

Aufgabe 1

```
DASISTDASHAUSVOMNIKOLAUSUNDNICHTDASVOMWEIHNACHTSMANN
TAGTAGTAGTAGTAGTAGTAGTAGTAGTAGTAGTAGTAGTAGTAGTAGT
WAYBSZWAYAAALVUFNODORTUYNNJGIIATJTSBHMCXINGAIATYFATG
```

'*DAS*' -> '*WAY*'

'*DAS*' -> '*WAY*'

'*DAS*' -> '*JTS*'

Der Abstand der beiden '*WAY*'s beträgt 6. 6 = 2 · 3 Der Schlüssel könnte also '2' oder '3' oder '6' lang sein.

CHT → '*IAT*' kommt zweimal vor und hat den Abstand 15. 15 = 5 · 3

'3' kommt in beiden Primfaktorzerlegungen vor und könnte die Schlüssellänge sein.

Es ist natürlich möglich, dass die Folgen nur zufällig im Kryptotext gleich sind, im Klartext aber nicht.

Aufgabe 2

a)

```
QMO at index 3 and 48 - difference = 45
MOP at index 4 and 49 - difference = 45
PCZ at index 26 and 61 - difference = 35
PCZ at index 61 and 156 - difference = 95
XMW at index 77 and 197 - difference = 120
GIP at index 84 and 149 - difference = 65
IPH at index 85 and 150 - difference = 65
```

b) Zerlegen in Primfaktoren ergibt:

$45 = 5 \cdot 9$ $\qquad$ $120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5$

$35 = 5 \cdot 7$ $\qquad$ $65 = 5 \cdot 13$

$95 = 5 \cdot 19$

c) Die 5 ist der einzige Primfaktor, der in allen Zerlegungen auftritt und wird mit großer Wahrscheinlichkeit die Schlüssellänge sein.

Hinweis: Das Schlüsselwort ist BLUME