Der Kasiski-Test

Bestimmung des Schlüsselwortes bei bekannter Schlüssellänge

Stellen wir uns vor, wir haben den untenstehenden verschlüsselten Text abgefangen.

```
YMVCZAIIHMVBOMIINBKVBMRVILIUZAXVSBIJYMRWZPPVM
```

Wir wissen über ihn, dass er auf **Deutsch** verfasst ist und mit dem **Vigenère-Verfahren** verschlüsselt wurde. Zudem wissen wir, dass der Schlüssel die **Länge 4** hat. Wir müssten jetzt nur noch wissen, welche vier Buchstaben das Schlüsselwort bilden...

Die Idee: Wir teilen den Text in Stücke der Länge 4 auf und schreiben diese untereinander:

Y	M	V	C
Z	A	I	I
H	M	V	B
O	M	I	I
N	B	K	V
B	M	R	V
I	L	I	U
Z	A	X	V
S	B	I	J
Y	M	R	W
Z	P	P	V
M			

Überlegung 1: Was haben die Buchstaben in einer Spalte gemeinsam? Wie sind sie beim Verschlüsseln aus dem Klartext entstanden?

Überlegung 2: Wir haben eine charakteristische Eigenschaft deutscher Texte kennengelernt. Wie kann diese einen Hinweis auf den ersten, zweiten, dritten und vierten Schlüsselbuchstaben geben?

Hilfestellung: Die folgenden Häufigkeitsdiagramme zeigen die Anteile der Buchstaben in den jeweiligen Spalten: {{ :faecher:informatik:oberstufe:kryptographie:vigenere:kasiski:kasiski.png

}}