



## Vigenère-Verfahren – Lösung

a) MWVISTSBX

b) KONZENTRATION

c) Nimm den ersten Klartextbuchstaben. Suche die Spalte mit diesem Buchstaben. Suche die Zeile mit dem zugehörigen Schlüsselbuchstaben. Der Schnittpunkt der beiden ist der verschlüsselte Buchstabe. Wiederhole dieses Vorgehen für alle Buchstaben des Klartextes.

d) Nimm den ersten Buchstaben der verschlüsselten Nachricht. Suche die Zeile mit dem zugehörigen Schlüsselbuchstaben. Suche innerhalb dieser Zeile nach dem verschlüsselten Buchstaben. Gehe an dieser Stelle in der Tabelle nach oben. Dort steht der Klartext-Buchstabe. Wiederhole dieses Vorgehen für alle Buchstaben der verschlüsselten Nachricht.

*Hier könnten SuS auch auf (f) kommen.*

e) individuelle Lösungen → Diese Frage führt zum nächsten Thema: *Brechen von Vigenère*.

f) Wie beim Cäsar-Verfahren kann man für jeden Schlüsselbuchstaben den 'Gegenbuchstaben' wählen:

**B=1** => **Z=25** weil  $1+25=26$

**I=8** => **S=18** weil  $8+18=26$

**T=19** => **H=7** weil  $19+7=26$

Also ist der neue Schlüssel: **ZSH**

