

Aufgabe 1

Finde mit der Häufigkeitsanalyse von CryptTool-Online (<https://www.cryptool.org/de/cto/frequency-analysis>) eine Lösung, um wie viele Buchstabe der nachfolgende Text im Alphabet verschoben wurde.

ktGHrWAJtHHtAC xHI spH RDsxtGtC txCtH ZApGlMItH Bxl WxAut txCtH hrwAJtHHtAH xC txCtC
VtwtxBitMI, JB XCuDGBpIxDCtC vtwtxB OJ HETxrwGC DstG OJ JtqtGIgpvtC. TxCt TCiHrWAJtHHtAJCv
xHI CJG Bxl txCtB EpHHtCstC hrwAJtHHtA BDtvAxrw. Qtx stG HNBBtIGxHrwtC ktGHrWAJtHHtAJCv vxql
tH CJG txCtC hrwAJtHHtA, Bxl stB KtG- JCs tCIHrWAJtHHtAI LxGs.

Wie lautet der zugehörige Klartext?

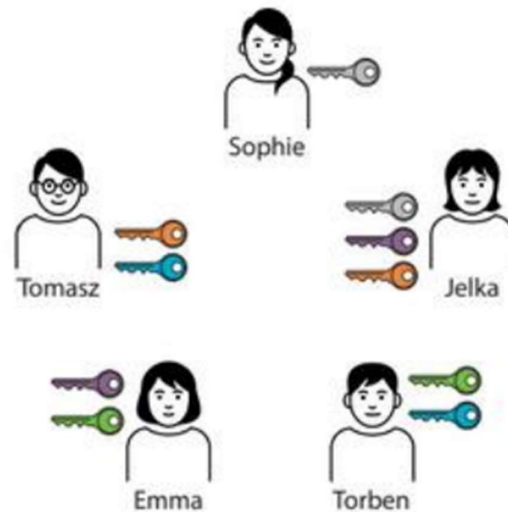
(auf <https://www.cryptool.org/de/cto/> steht ein Tool für die Cäsar-Verschlüsselung bereit)

Aufgabe 2

3 In der Gruppe kommunizieren

Tomasz, Sophie, Jelka, Emma und Torben wollen untereinander geheime Nachrichten austauschen. Dazu wollen sie zunächst eine symmetrische Verschlüsselung verwenden. Sie haben sich mehrere Schlüssel angelegt und wie in der Grafik dargestellt untereinander verteilt.

- Kann Sophie eine Nachricht an Torben schicken, ohne dass jemand anderes als die fünf die Nachricht mitlesen kann? Begründen Sie Ihre Antwort.
- Wie viele zusätzliche Schlüssel werden bei Verwendung der symmetrischen Verschlüsselung benötigt, damit jeder jedem anderen eine geheime private Nachricht schicken kann? Begründen Sie Ihre Antwort.
- Nachdem die fünf das System unter sich getestet haben, wollen sie der ganzen Klasse Zugriff auf ihr System geben. Wie viele Schlüssel brauchen sie insgesamt, wenn sie 15 weitere Mitschülerinnen und Mitschüler haben? Begründen Sie Ihre Antwort. (Tipp: Überlegen Sie zunächst, wie viele Schlüssel für jede weitere Person hinzukommen.)



Aufgabe 3

Entschlüssele das Wort OOGWPWESR, welches mit dem geheimen Schlüssel HOME verschlüsselt wurde.