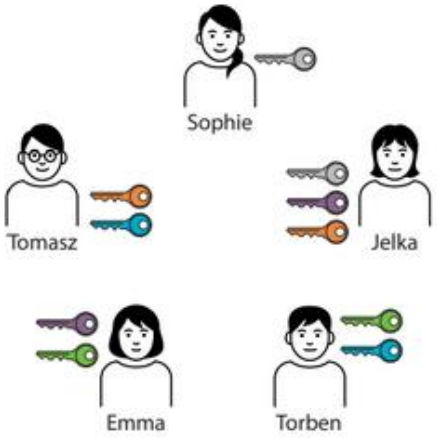
3 In der Gruppe kommunizieren

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.



a Kann Sophie eine Nachricht an Torben schicken, ohne dass jemand anderes als die fünf die Nachricht mitlesen kann? Begründen Sie Ihre Antwort.

b 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.

c 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.)

Tomasz schlägt vor, anstelle der symmetrischen Verschlüsselung ein asymmetrisches Verfahren zu nutzen.

d Erklären Sie im Beispiel knapp, welchen Vorteil er sich davon verspricht und welche Nachteile damit einhergehen.

4 Einweg- und Falltürfunktionen

a Beschreiben Sie, ob bzw. inwiefern die folgenden Vorgänge mit Einweg- oder Falltürfunktionen verglichen werden können.

i Erbsen und Linsen mischen
ii flüssige Farben mischen
iii Sand und Kies mischen
iv schriftliches Quadrieren einer großen Zahl