Ein Verschlüsselungsverfahren entwickeln

Szenario

Alice und Bob möchten eine geheime Botschaft austauschen. Sie haben jeweils ein Schloss mit passendem Schlüssel zur Verfügung. Alice hat zusätzlich noch einen Briefumschlag für das Verschicken der Nachricht.

Arbeitsauftrag (15 Min.)

Simulieren Sie den Nachrichtenaustausch zwischen Alice und Bob. Entwickeln Sie dazu ein geeignetes Verschlüsselungsverfahren ausschließlich mit den Ihnen zur Verfügung gestellten Hilfsmitteln (s. Abbildung rechts).

Ziel: Der Postbote darf die Nachricht nicht mitlesen. (Trotzdem muss Bob die Nachricht entschlüsseln können!)

Regeln

- Sie müssen die verschlüsselte Nachricht dem „Postboten“ übergeben. Dieser liefert die Nachricht aus.
- Sie dürfen sich vorab persönlich treffen.
- Sie dürfen **nicht** die Nachricht persönlich übergeben. (Persönliche treffen dienen nur dem Austausch über das anzuwendende Verfahren).

Lösungsvorschlag (Stichpunkte)