AB: Verschlüsselungsverfahren entwickeln Datum:

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.

Aufgabe

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

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

Regeln

- Sie *müssen*:
  - Die verschlüsselte Nachricht dem (virtuellen) „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)