Verschlüsseln ohne Austausch geheimer Informationen

Auch bei unknackbaren Verschlüsselungsverfahren besteht stets die Gefahr, dass jemand das geheime Schlüsselwort erfährt. Bevor Nachrichten verschlüsselt werden können, müssen sich die Kommunikationspartner stets auf einen gemeinsamen Schlüssel einigen. Deshalb haben in der zweiten Hälfte des 20. Jahrhunderts einige Wissenschaftler erforscht, ob es nicht ein Verfahren geben kann, bei dem keine geheimen Schlüssel ausgetauscht werden müssen.

Szenario

Stellen Sie sich folgende Situation vor: Alice und Bob haben je ein Schloss mit Schlüssel. Alice möchte Bob ein Geheimnis in einer verschlossenen Kiste übermitteln.

Fragestellung:

Wie kann Alice den Inhalt der Kiste sicher übermitteln, ohne Bob den Schlüssel für ihr Schloss zu geben?

Aufgabe: Sichere Übertragungsmethode finden

- Schreiben Sie eine Nachricht an Ihre Partnergruppe. „Verschlüsseln“ Sie die Nachricht mit Hilfe eines Umschlages und eines Schlosses.
- Übermitteln Sie die Nachricht an den Postboten, der sie dem Empfänger zustellt.
- **Ziel:** Der Postbote darf die Nachricht nicht mitlesen. Trotzdem muss der Empfänger die Nachricht entschlüsseln können!

Regeln

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