

Asymmetrische Verschlüsselung

- Alice will eine verschlüsselte Nachricht an Bob schicken
- Alice und Bob müssen sich vorab auf einen Schlüssel einigen
 - Oder geht es auch anders?

- Alice besitzt ein Vorhängeschloss mit Schlüssel



Abbildung 1: Bildquelle: Google, Apache License 2.0, via Wikimedia Commons

- Lässt sich damit das Kommunikationsproblem lösen?

- Alice schickt ihr Schloss **ohne Schlüssel** und **in geöffnetem Zustand** an Bob
- Bob legt seine geheime Botschaft in eine Kiste und verschließt diese mit Alice' Schloss
- Bob verschickt die Kiste an Alice
- Alice öffnet die Kiste mit dem Schlüssel zu ihrem Schloss

- Das Schloss kann ohne weitere Schutzmaßnahmen verschickt werden
- Die verschlossene Kiste kann nur von Alice geöffnet werden
- Wenn Alice mit mehreren Leuten kommunizieren möchte, könnte sie weitere baugleiche Schlösser kaufen und verteilen
- Wie kann Alice eine verschlüsselte Antwort an Bob schicken?

- Idee: Verwende unterschiedliche Schlüssel zum Ver- und Entschlüsseln
 - Ein Schlüssel wird öffentlich gemacht (**public key**)
 - Der andere Schlüssel bleibt geheim (**private key**)
- Der private key darf sich nicht aus dem public key rekonstruieren lassen!
- **Alle** Kommunikationspartner brauchen ein solches Schlüsselpaar

1. Bob besorgt sich Alice' **öffentlichen** Schlüssel
2. Bob verschlüsselt seine Nachricht an Alice mit diesem Schlüssel
3. Bob sendet die verschlüsselte Nachricht an Alice
4. Alice entschlüsselt die Nachricht mit ihrem **privaten** Schlüssel

- Das “Schlüsseltausch-Problem” scheint mit asymmetrischen Verfahren gelöst
- Gibt es dennoch Probleme oder gar Angriffsmöglichkeiten?
- Welcher der vier Schritte im Ablauf ist kritisch?
 1. Bob besorgt sich Alice’ öffentlichen Schlüssel
 2. Bob verschlüsselt seine Nachricht an Alice mit diesem Schlüssel
 3. Bob sendet die verschlüsselte Nachricht an Alice
 4. Alice entschlüsselt die Nachricht mit ihrem privaten Schlüssel

- Woher weiß Bob, dass er wirklich Alice' öffentlichen Schlüssel erhalten hat
- Wie könnte sich ein Angreifer (man-in-the-middle) in die Kommunikation zwischen Alice und Bob "einklinken"?
 - Der Angreifer muss lediglich Alice' öffentlichen Schlüssel durch seinen eigenen austauschen