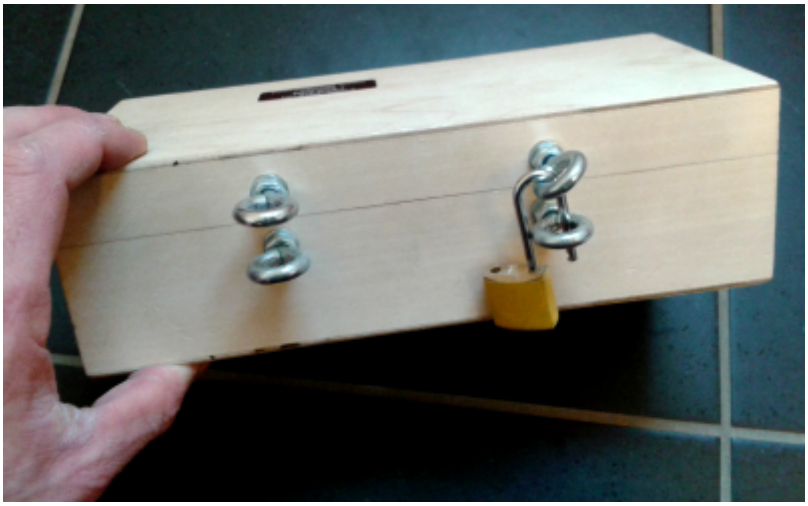
Die Kryptobox als Modell

[1)]



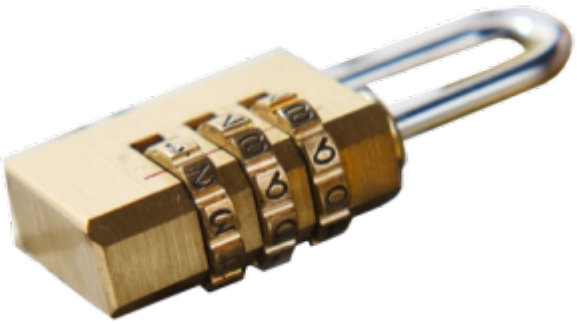
Die Kryptobox ist eine **Modellvorstellung**, die man auch basteln kann. Stell dir eine Box wie im Bild oben vor, durch die Ösen kann man Vohängeschlösser einfädeln, die die Kiste sicher abschließen. Die folgenden Randbedingungen nehmen wir als gegeben an:

- Kiste und Schloss widerstehen Brute-Force-Angriffen.
- Von allem, was man in der Hand hält, kann man auch Kopien machen (wie von Dateien).
- Dem Schloss sieht man nicht an, wie der zugehörige Schlüssel aussieht.
- Der Transport der Kiste zwischen Alice und Bob (überhaupt ihre gesamte Kommunikation) erfolgt über Dritte, die zwischen ihnen sitzen und **nicht** vertrauenswürdig sind.
- Wir vernachlässigen in diesem Modell Kommunikationsvorgänge, die zwischen mehr als zwei Kommunikationspartnern stattfinden (es unterhalten sich immer nur Alice und Bob).

Es liegt auf der Hand, dass man die Kiste mit verschiedenen Vorhängeschlösser schließen kann.

Variante A: Zahlenschloss

In Variante 1 verschließt Alice die Kryptobox mit einem Zahlenschloss. Um das Schloss zu verwenden muss die Person, die die Kryptobox verschließt einen Zahlencode festlegen, die Person die das Schloss öffnen will, muss diesen Zahlencode am Schloss einstellen.



(A1)

- Welche Information benötigt Bob, um die Kryptobox öffnen zu können?
- Wie müssen Alice und Bob vorgehen, um die Kryptobox mit dem Zahlenschloss verwenden zu können?
- Um welche Art Verschlüsselung handelt es sich, wenn die Kryptobox mit dem Zahlenschloss verwendet wird?
- Erstelle einen Merksatz, der beschreibt, wofür die Kryptobox gemeinsam mit einem Zahlenschloss ein geeignetes Modell darstellt.

Variante B: Bügelschloss mit Schlüssel

In Variante 2 wird die Kryptobox durch ein Bügelschloss mit Schlüssel verschlossen. Dabei ist es wichtig, sich klarzumachen, dass das Schloss **ohne Schlüssel verschlossen** werden kann, jedoch nur **mit Schlüssel wieder geöffnet** werden kann.

(A2)

Alice möchte die Kryptobox an Bob verschlüsseln, die Box also so verschließen, dass nur Bob die Box wieder öffnen kann.

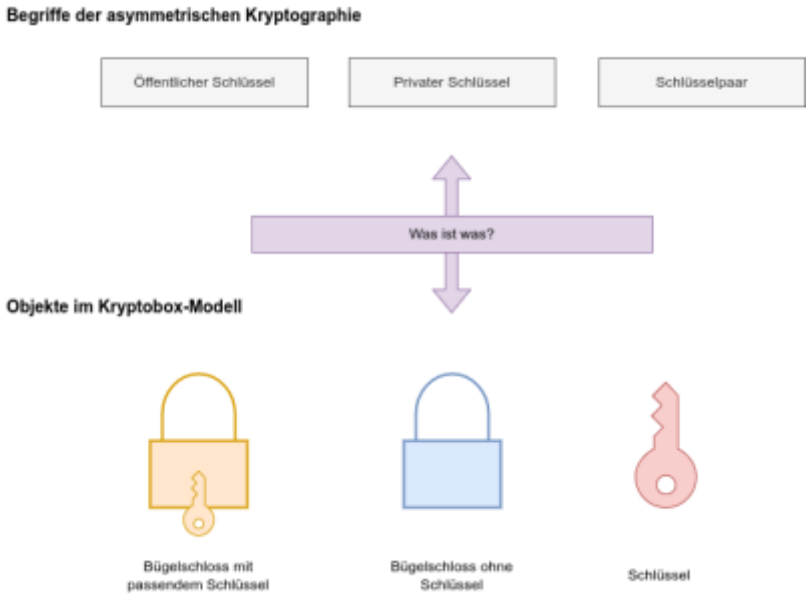
- Was benötigt Alice dazu?
- Was benötigt Bob, um die Box wieder zu öffnen?
- Was würde benötigt, damit Bob als Antwort wieder eine verschlüsselte Nachricht an Alice schreiben kann?

Die Kryptobox als Modell der asymmetrischen Verschlüsselung

- Bei der asymetrischen Verschlüsselung hat jeder Kommunikationspartner ein **Schlüsselpaar**.
- Das Schlüsselpaar besteht aus einem **geheimen Schlüssel** und einem dazu **passenden öffentlichen** Schlüssel.
- Der **geheime Schlüssel** darf unter keinen Umständen in falsche Hände gelangen - **meist ist er besonders geschützt**, beispielsweise durch ein Passwort oder auf einer SmartCard.
- Der **öffentliche Schlüssel** hingegen **wird** großzügig an alle Kommunikationspartner **verteilt**, von denen man möchte, dass diese verschlüsselte Nachrichten schicken können sollen.
- Diese Art der Verschlüsselung heißt asymmetrisch, da Nachrichten, die mit dem öffentlichen Schlüssel **verschlüsselt** sind nur mit dem dazu passenden privaten Schlüssel **entschlüsselt** werden können.

(A3)

Ordne die Begriffe öffentlicher Schlüssel, privater Schlüssel, Schlüsselpaar den passenden Objekten des Kryptobox-Modells zu:



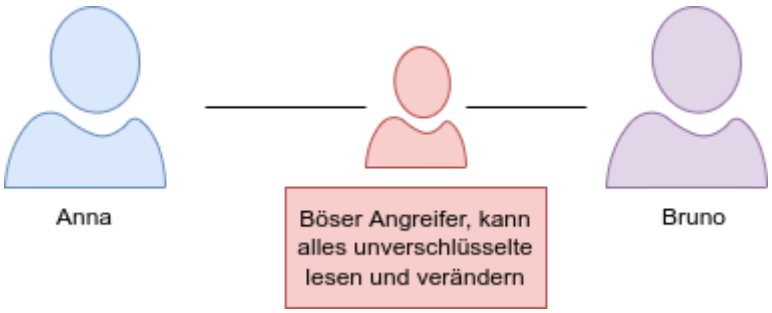
(A4)

Alice schreibt Bob eine asymmetrisch verschlüsselte Nachricht:

- Wer verschlüsselt die Nachricht mit welchem Schlüssel?
- Wer kann die Nachricht mit welchem Schlüssel entschlüsseln?
- Kann die Person, die die Nachricht verschlüsselt hat diese nach dem Verschlüsselungsvorgang lesen?

(A4)

Anna und Bruno haben sich auf Twitter kennengelernt und sich noch nie getroffen. Sie wollen auch (asymmetrisch) verschlüsselt kommunizieren.



- Was müssen Anna und Bruno haben und machen, damit das klappt?
- Auf welche Weise könnte ein Angreifer in der Phase der unverschlüsselten Kommunikation zwischen Anna und Bruno eingreifen, um am Ende deren verschlüsselte Kommunikation mitlesen zu können.
- Wie können Bruno und Anna diesen Angriff abwehren?

[1)]

Bilder und Ideen von Dietrich / Lautebach (Version: Mai 2017), Lizenz CC-BY-SA