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:

[1)]

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