

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 Vorhängeschlösser 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:



(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?

1)

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

From:
<https://wiki.qg-moessingen.de/> - QG Wiki

Permanent link:
https://wiki.qg-moessingen.de/modell_kryptobox:start?rev=1648654699

Last update: **30.03.2022 17:38**



