1 Das Problem der symmetrischer Verschlüsselung

Alice und Bob arbeiten an einem streng geheimen Projekt. Da beide in verschiednen Städten wohnen, sind sie sich noch nie begegnet. Alice und Bob müssen nun aber wichtige Nachrichten austauschen. Beide haben Angst, dass Oscar versuchen könnte ihre Nachrichten abzufangen. Sie verschlüsseln deshalb ihre Nachrichten.
Leider hat Alice keine Zeit sich persönlich mit Bob zu treffen. Sie sendet ihre Nachrichten deshalb mit der Post. Eine symmetrische Verschlüsselung der Nachrichten ist dabei keine gute Idee. Warum?

- ☐ Alice müsste Bob einmal das Entschlüsselungsverfahren mitteilen. Wird der Postbote dabei von Oscar abgefangen, kann Oscar alle weiteren Nachrichten entschlüsseln.
- ☐ Alle symmetrischen Verfahren sind einfach zu knacken.
- ☐ Da sich symmetrische Verfahren nur für sehr kurze Nachrichten eignen, müssen die beiden viel zu viele Nachrichten hin und her schicken.

Alice wendet deshalb eine asymmetrische Verschlüsselung, das RSA-Verfahren, an. Das RSA-Verfahren wird in vielen Bereichen des alltäglichen Lebens verwendet. Davon wissen aber nur die wenigsten. Es kommt zum Einsatz bei

- Apps zum Chatten (Telegram, Threema, usw.),
- jedem Öffnen einer Website im Internet,
- Bankgeschäften oder
- der Fernwartung von Computern.

In diesem Kapiel wollen wir uns nur den Ablauf anschauen. Wie und warum das Ganze funktioniert und absolut sicher ist, erfährst du in den nächsten Abschnitten.
Öffne die Website

https://mx3030.github.io/rsa/

und versuche die nachfolgende Erklärung nachzuvollziehen und selber auszuprobieren.

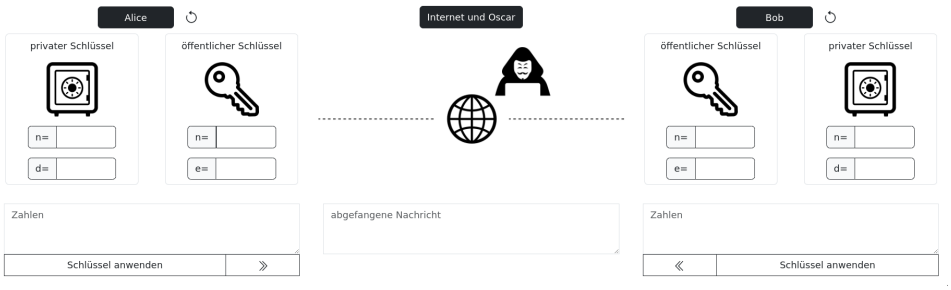

Abbildung 1: alice2bob.png