# 1 Das Problem der symmetrischer Verschlüsselung

Alice und Bob arbeiten an einem streng geheimen Projekt. Da beide in verschiedenen 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 müssen deshalb verschlüsseln.
Leider hat Alice nicht ein einziges Mal Zeit, sich persönlich mit Bob zu treffen. Aus diesem Grund sendet Sie alle ihre Nachrichten 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 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 sicheren Website (https://...) 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 das Senden einer Nachricht von Alice an Bob nachzuvollziehen und selber auszuprobieren.

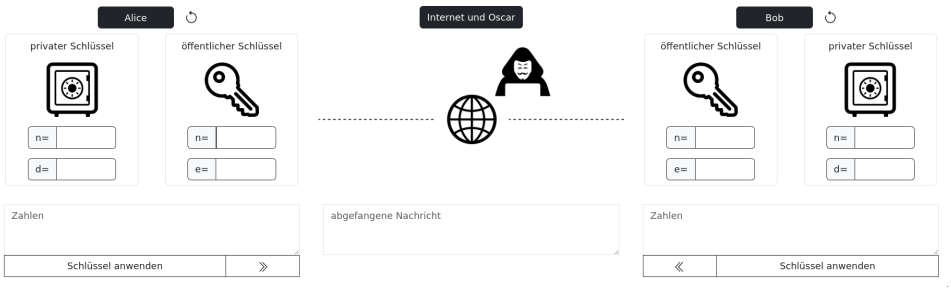
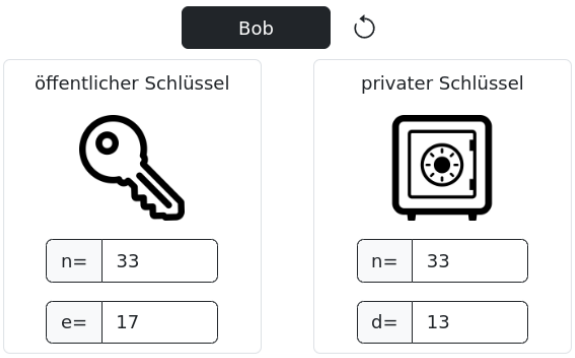



Abbildung 1: Startbildschirm beim Öffnen der Website.

## Alice sendet eine Nachricht an Bob




Bob baut sich ein Schlüsselpaar (siehe Abschnitt ...) bestehend aus einem öffentlichen und einem privaten Schlüssel.