1 Das Problem der symmetrischer Verschlüsselung

Alice und Bob arbeiten an einem streng geheimen Projekt. Beide sind sich aber noch nie begegnet, da sie sehr weit entfernt voneinander arbeiten. Alice und Bob müssen wichtige Nachrichten austauschen. Leider hat Alice keine Zeit sich persönlich mit Bob zu treffen. Sie wendet sich deshalb an einen zuverlässigen Mitarbeiter, der diese Aufgabe übernehmen soll. Es gibt aber ein Problem. Eine symmetrische Verschlüsselung des Nachrichtenaustauschs kommt deshalb nicht in Frage. Warum?

- ☐ Alice müsste ihrem Mitarbeiter auch erklären wie die Entschlüsselung funktioniert. Wird der Mitarbeiter von Oscar abgefangen, kennt Oscar das Geheimnis.
- ☐ Ein symmetrisches Verfahren kann leicht geknackt werden.
- ☐ Mit einem symmetrisches Verfahren ist sehr aufwendig, da es sich nur für kurze Nachrichte eignet.

Alice wendet deshalb eine asymmetrische Verschlüsselung, das RSA-Verfahren, an. Dazu schickt sie ihren Mitarbeiter ohne eine Nachricht zu Bob, der dort einen "öffentlichen Schlüssel"für Alice holt. Der "öffentliche Schlüssel"besteht aus zwei Zahlen n und e. Mit diesem Schlüssel kann Alice ihre Nachricht verschlüsseln. Sie wendet dazu eine Methode an, die auch Oscar kennt. Das Tolle an dem Verfahren ist aber, dass man die Nachricht nur dann entschlüsseln kann, wenn man auch den "privaten Schlüssel"kennt. Bei dem "privaten Schlüssel"handelt es sich um eine Zahl d, die weder Alice noch Oscar kennen. Nur der Emfänger der Nachricht, also Bob, ist im Besitz des "privaten Schlüssels".
Aus diesem Grund kann Alice ohne Gefahr ihren Mitarbeiter mit der verschlüsselten Nachricht zu Bob schicken. Bob entschlüsselt dann die Nachricht mit seinem "privaten Schlüssel".
Durch das Internet geht dieser Vorgang heutzutage natürlich unfassbar schnell. Oscar wäre in diesem Fall ein Hacker, der nur an den "öffentlichen Schlüsselünd die verschlüsselte Nachricht gelangen kann.