4.4 Geheime Kommunikation ohne Schlüsselaustausch

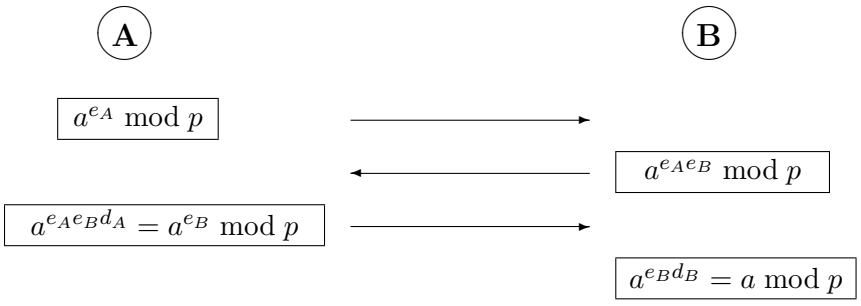
Es ist auch möglich, vertraulich zu kommunizieren, ohne vorher Schlüssel vereinbart zu haben – der Angriff durch den Mann in der Mitte ist hier aber ebenfalls möglich.

Die Idee lässt sich an einem Bild aus dem Alltagsleben verdeutlichen:

- Alice legt die Nachricht in eine Kiste und verschließt sie mit einem Vorhängeschloss, zu dem nur sie den Schlüssel hat. Sie schickt die Kiste an Bob.
- Bob kann die Kiste natürlich nicht öffnen. Statt dessen verschließt er sie mit einem weiteren Vorhängeschloss, zu dem nur er den Schlüssel hat. Er schickt die doppelt verschlossene Kiste an Alice zurück.
- Alice entfernt ihr Vorhängeschloss und schickt die nunmehr nur noch mit Bobs Schloss verschlossene Kiste wieder an Bob.
- Bob entfernt sein Schloss, öffnet die Kiste und liest die Nachricht.

Dieses kryptographische Protokoll heißt Massey-Omura-Schema oder Shamirs No-Key-Algorithmus. Es lässt sich mit Hilfe der diskreten Exponentialfunktion umsetzen; seine Sicherheit beruht auf der Komplexität des diskreten Logarithmus:

Vorgegeben ist eine öffentlich bekannte, allgemein gültige (große) Primzahl p. Alice und Bob wählen je ein Paar von Exponenten d und e mit $ed \equiv 1 \pmod{p-1}$, also $a^{de} \equiv a \pmod{p}$ für alle ganzen Zahlen $a \in \mathbb{Z}$. Jeder hält seine *beiden* Exponenten geheim. Das Protokoll, mit dem Alice nun eine Nachricht a an Bob schickt, sieht so aus:



Ein Angreifer, der diskrete Logarithmen berechnen könnte, könnte aus den erlauschten Geheimtexten $a^{e_A} \bmod p$ und $a^{e_A e_B} \bmod p$ den Exponenten e_B und daraus durch Kongruenzdivision auch d_B berechnen. Ebenso könnte er aus $a^{e_A e_B} \bmod p$ und $a^{e_A e_B d_A} = a^{e_B} \bmod p$ den Exponenten d_A und dann auch e_A berechnen.

Ein anderer Angriff ist nicht bekannt.