§12. Hybride–Verschlüsselungsverfahren

Asymmetrische Verfahren wie das RSA–Verfahren sind für das Ver– und Entschlüsseln großer Datenmengen bei weitem zu langsam. Daher versucht man, symmetrische und asymmetrische Verschlüsselungsverfahren zu kombinieren: der Klartext wird mit einem schnellen symmetrischen Verfahren verschlüsselt und der dabei verwendete Schlüssel wird mit einem asymmetrischen Verfahren verschlüsselt, d.h. das asymmetrische Verfahren wird nur zum **Schlüsselaustausch** benutzt.

(12.1) Hybride Verschlüsselung

Die Teilnehmer $\boldsymbol{A}$ und $\boldsymbol{B}$ besitzen jeweils einen öffentlichen und einen geheimen Schlüssel. $\boldsymbol{A}$ möchte eine verschlüsselte Nachricht an $\boldsymbol{B}$ schicken.

Verschlüsselung: $\boldsymbol{A}$ wählt einen (geheimen) Schlüssel $\boldsymbol{k}$ für ein symmetrisches Verschlüsselungsverfahren und verschlüsselt damit den Klartext, den er an $\boldsymbol{B}$ schicken möchte. Außerdem verschlüsselt er den Schlüssel $\boldsymbol{k}$ durch den öffentlichen Schlüssel von $\boldsymbol{B}$ zu $\boldsymbol{l}$ und schickt $\boldsymbol{l}$ ebenfalls an $\boldsymbol{B}$.

Entschlüsselung: $\boldsymbol{B}$ kann $\boldsymbol{l}$ mit seinem geheimen Schlüssel wieder zu $\boldsymbol{k}$ entschlüsseln und damit dann den symmetrisch verschlüsselten Geheimtext entschlüsseln.

(12.2) RSA–Schlüsselaustausch

$\boldsymbol{B}$ hat den öffentlichen Schlüssel $(\boldsymbol{n_B}, \boldsymbol{e_B})$.

$\boldsymbol{A}$ wählt einen Schlüssel $\boldsymbol{k} < \boldsymbol{n_B}$ und verschlüsselt damit $\boldsymbol{k}$ zu

$$\boldsymbol{k}^{\boldsymbol{e_B}} \bmod \boldsymbol{n_B} \;=:\; \boldsymbol{l}\,.$$

$\boldsymbol{A}$ schickt $\boldsymbol{l}$ an $\boldsymbol{B}$. $\boldsymbol{B}$ entschlüsselt $\boldsymbol{l}$ mit seinem geheimen Schlüssel $(\boldsymbol{n_B}, \boldsymbol{d_B})$ zu

$$\boldsymbol{l}^{\boldsymbol{d_B}} \bmod \boldsymbol{n_B} \;=\; \boldsymbol{k}\,.$$

(12.3) Diffie–Hellman–Schlüsselaustausch

Eine Primzahl $\boldsymbol{p}$ und eine natürliche Zahl $\boldsymbol{g}$ mit $\boldsymbol{g < p}$ sind (öffentlich) gegeben. Zwei Teilnehmer $\boldsymbol{A}$ und $\boldsymbol{B}$ wählen je eine Zahl $\boldsymbol{a}$ bzw. $\boldsymbol{b}$ mit $\boldsymbol{a, b < p - 1}$, die sie geheimhalten.

$\boldsymbol{A}$ schickt	$\boldsymbol{B}$ schickt
$\boldsymbol{\alpha := g^a \bmod p}$	$\boldsymbol{\beta := g^b \bmod p}$
an $\boldsymbol{B}$	an $\boldsymbol{A}$
$\boldsymbol{A}$ berechnet	$\boldsymbol{B}$ berechnet
$\boldsymbol{k := \beta^a \bmod p}$	$\boldsymbol{l := \alpha^b \bmod p}$

Beide Werte sind gleich
und können als Schlüssel für ein symmetrisches Verfahren benutzt werden.

Bei diesem Schlüsselaustausch sind beide Partner völlig gleichberechtigt bei der Bestimmung des Schlüssels, niemand gibt einen Schlüssel vor.