Kap. V:

Asymmetrische Verschlüsselungsverfahren

§ 10. Asymmetrische Verschlüsselungsverfahren und Public–Key–Systeme

Wir hatten bisher symmetrische Verschlüsselungsverfahren behandelt. Wer verschlüsseln kann, kann auch entschlüsseln und umgekehrt, d.h. aus dem Schlüssel zum Verschlüsseln läßt sich der Schlüssel zum Entschlüsseln bestimmen und umgekehrt. Damit zwei Personen $\boldsymbol{A}$ und $\boldsymbol{B}$ geheim miteinander korrespondieren können, müssen sie vorher auf irgendeine Weise einen Schüssel verabreden. Bei solch einem symmetrischen Verfahren ergeben sich zweischwerwiegende Probleme:

1) Ist die Nachricht authentisch?

2) Wie können die Schlüssel bei mehreren Teilnehmern verwaltet werden?

zu 1) Hat eine dritte Person $\boldsymbol{X}$ eine verschlüsselte Botschaft von $\boldsymbol{A}$ an $\boldsymbol{B}$ abgefangen und hat $\boldsymbol{X}$ auf irgendeine Weise den Schlüssel erfahren, so kann $\boldsymbol{X}$ den Geheimtext entschlüsseln und kennt das Geheimnis. Aber noch viel schlimmer: $\boldsymbol{X}$ kann die Nachricht abändern, verschlüsseln und im Namen von $\boldsymbol{A}$ an $\boldsymbol{B}$ schicken. $\boldsymbol{B}$ glaubt dann, dass die Nachricht von $\boldsymbol{A}$ stammt, und ahnt nicht, dass $\boldsymbol{X}$ der Absender ist.

zu 2) Wollen mehrere Teilnehmer verschlüsselte Nachrichten untereinander austauschen, so müssen vorher je zwei Teilnehmer einen Schlüssel vereinbart haben. Bei $\boldsymbol{n}$ Teilnehmern sind dafür $\frac{1}{2}\boldsymbol{n}(\boldsymbol{n}-\mathbf{1})$ Schlüssel erforderlich. Kommt noch ein weiterer Teilnehmer hinzu, so sind $\boldsymbol{n}$ weitere Schlüsselverabredungen erforderlich.

(10.1) DEF: Bei einem **asymmetrischen Verschlüsselungsverfahren** gibt es zwei verschiedene Schlüssel, und zwar einen zum Ver– und einen zum Entschlüsseln. Aus der Kenntnis eines Schlüssels darf sich der andere Schlüssel nicht herausfinden lassen.

Das Prinzip eines asymmetrischen Kryptosystems wurde im Jahre 1976 von **Whitfield Diffie** und **Martin Hellman** in ihrer Arbeit

"New Directions in Cryptography"

vorgeschlagen. Sie konnten jedoch noch keine Realisierung angeben.

(10.2) DEF: Bei einem **Public–Key–Kryptosystem** besitzt jeder Teilnehmer $\boldsymbol{A}$ ein Schlüsselpaar $(\boldsymbol{e_A}, \boldsymbol{d_A})$. Dabei ist $\boldsymbol{e_A}$ ein **öffentlicher** Schlüssel, mit dem Nachrichten **an** $\boldsymbol{A}$ verschlüsselt werden, und $\boldsymbol{d_A}$ ist ein **privater** Schlüssel, mit dem $\boldsymbol{A}$ an ihn gesandte Nachrichten entschlüsseln kann. Aus der Kenntnis von $\boldsymbol{e_A}$ darf sich $\boldsymbol{d_A}$ nicht bestimmen lassen und umgekehrt.

(10.3) BEM: **a)** Die öffentlichen Schlüssel aller Teilnehmer sind in einem Verzeichnis enthalten, das frei zugänglich ist. Daher kommt der Name **Public–Key–Verfahren**.

b) Der private Schlüssel $\boldsymbol{d_A}$ muss geheim gehalten werden. Da er sich aus $\boldsymbol{e_A}$ nicht herleiten läßt, ist $\boldsymbol{A}$ der einzige, der entschlüsseln kann.

c) Bei diesem Verfahren müssen die Teilnehmer keine gemeinsamen geheimen Schlüssel verabreden , wie dies bei einem symmetrischen Verfahren nötig ist.

(10.4) DEF: Ein Public–Key–Kryptosystem heißt ein **Signatur–Schema**, wenn sich mit Hilfe des öffentlichen Schlüssels von $\boldsymbol{A}$ einwandfrei feststellen läßt, ob eine verschlüsselte Nachricht wirklich von $\boldsymbol{A}$ kommt oder nicht.