# Schlüsselerzeugung

# 13

Mit den bisher eingeführten kryptografischen Mechanismen, insbesondere der symmetrischen und asymmetrischen Verschlüsselung, den digitalen Signaturen und den MAC, können grundlegende Sicherheitsziele (vgl. Abschn. 10.1.3) relativ einfach erreicht werden:

- Geheimhaltung (mit Verschlüsselungsverfahren)
- Integrität (mit MAC oder digitalen Signaturen)
- Nachrichtenauthentisierung (mit MAC oder digitalen Signaturen)
- Nichtzurückweisbarkeit (mit digitalen Signaturen)

Das Sicherheitsziel Identifikation kann ebenfalls mit kryptografischen Standardmechanismen erreicht werden.

Eine fundamentale Voraussetzung für alle Kryptoverfahren, die wir bisher behandelt haben, ist, dass die Schlüssel zwischen den beteiligten Parteien, z. B. Alice und Bob, korrekt verteilt wurden. Schlüsselerzeugung und -verteilung sind in der Praxis mit die wichtigsten, aber oft auch die schwersten Aspekte in einem Sicherheitssystem. In den vergangenen Kapiteln wurden schon einige Methoden zur Schlüsselerzeugung und zum Schlüsselaustausch vorgestellt, insbesondere die Schlüsselerzeugung nach Diffie-Hellman. In diesem Kapitel wird eine Reihe weiterer Verfahren vorgestellt, um Schlüssel sicher zwischen Parteien zu vereinbaren.

In diesem Kapitel erlernen Sie

- wie Schlüssel mit symmetrischer Kryptografie verteilt werden können,
- wie Schlüssel mit asymmetrischer Kryptografie verteilt werden können,
- wo die Schwachstellen von asymmetrischen Techniken zur Schlüsselerzeugung liegen,
- was Zertifikate sind und wie sie eingesetzt werden,
- was Public-Key Infrastrukturen (PKI) sind.



C. Paar, J. Pelzl, *Kryptografie verständlich*, eXamen.press,
DOI 10.1007/978-3-662-49297-0_13

## 13.1 Einführung

In diesem Abschnitt werden wir einige neue Begriffe, das Prinzip der Schlüsselaktualisierung und ein einfaches Schlüsselverteilungsprotokoll einführen. Das Protokoll dient als Basis für die spätere Einführung komplexerer Protokolle.

### 13.1.1 Terminologie

Unter Schlüsselverteilung versteht man den Aufbau eines gemeinsamen Geheimnisses zwischen zwei oder mehreren Parteien. Man unterscheidet zwischen Schlüsseltransport und Schlüsselvereinbarung, wie in Abb. 13.1 dargestellt. Beim Schlüsseltransport übermittelt ein Teilnehmer ein Geheimnis sicher zu einer anderen Partei. In einem Schlüsselvereinbarungsprotokoll einigen sich zwei oder mehr Teilnehmer auf ein gemeinsames Geheimnis, wobei alle Parteien an der Erzeugung des Geheimnisses mitwirken. Idealerweise sollte keiner der Teilnehmer in der Lage sein, den genauen Wert des Geheimnisses zu bestimmen.

Schlüsselverteilung ist eng verbunden mit der korrekten Erkennung von Teilnehmern. Man kann sich beispielsweise viele Angriffe vorstellen, bei denen ein Angreifer an einem Schlüsselverteilungsprotokoll teilnimmt und sich als Alice oder Bob ausgibt, um ein gemeinsames Geheimnis mit den legitimen Teilnehmern zu vereinbaren. Um solche Angriffe zu verhindern, muss sichergestellt werden, dass alle Teilnehmer die wahren Identitäten der anderen Parteien kennen.

### 13.1.2 Schlüsselaktualisierung und Schlüsselableitung

In vielen (aber nicht in allen) Sicherheitsanwendungen ist es wünschenswert, kryptografische Schlüssel zu verwenden, die nur für eine begrenzte Zeit gültig sind, beispielsweise für die Dauer einer Internetverbindung. Solche Schlüssel bezeichnet man als *Sitzungs-*

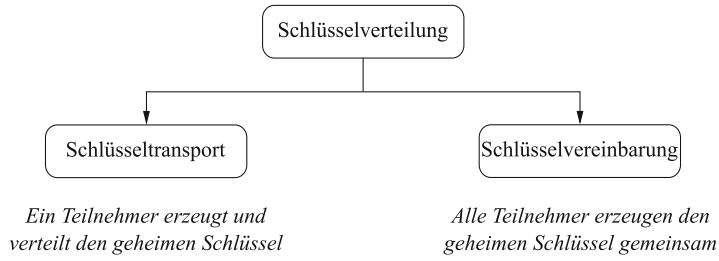


**Abb. 13.1** Klassifizierung von Schlüsselverteilungsprotokollen

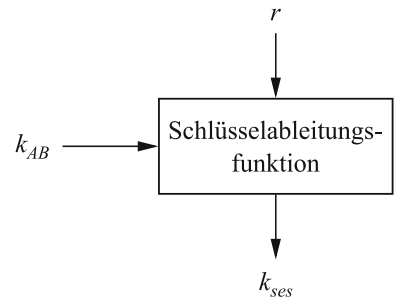


**Abb. 13.2** Das Prinzip der Schlüsselableitung

*schlüssel* („session key“) oder *temporäre Schlüssel* („ephemeral key“). Schlüssel mit einer zeitlichen Begrenzung bieten eine Reihe von Vorteilen. Zunächst ist festzustellen, dass der Schaden begrenzt wird, sollte der geheime Schlüssel bekannt werden. Auch stehen einem Angreifer weniger Chiffrate zur Verfügung, die mit einem Schlüssel erzeugt wurden. Dies erschwert manche kryptografischen Angriffe. Darüber hinaus muss ein Angreifer in den Besitz mehrerer Schlüssel kommen, wenn er lange Klartexte dechiffrieren möchte. Beispiele für Systeme, bei denen Sitzungsschlüssel sehr oft neu erzeugt werden, sind die Sprachverschlüsselung beim GSM-Mobilfunk und Videoverschlüsselung beim Satellitenfernsehen. In beiden Fällen werden innerhalb von Minuten oder manchmal sogar von Sekunden neue Schlüssel berechnet.

Die Vorteile, die die Schlüsselaktualisierung bietet, sind offensichtlich. Aber wie kann man diese realisieren? Der erste Ansatz wäre, einfach die Schlüsselverteilungsprotokolle aus diesem Kapitel immer wieder auszuführen. Wie später gezeigt wird, ist eine Schlüsselerzeugung aber auch immer mit Kosten verbunden, wobei Kosten sowohl in Form zusätzlicher Kommunikation als auch zusätzlicher Berechnungen auftreten. Besonders bei asymmetrischen Verfahren kann der Rechenaufwand sehr hoch sein.

Ein anderer Ansatz, um Schlüssel, die schon zwischen den Teilnehmern vereinbart wurden, zu aktualisieren, ist es, neue Sitzungsschlüssel *abzuleiten*. Das Grundprinzip hierbei ist, sog. Schlüsselableitungsfunktionen, wie in Abb. 13.2 dargestellt, zu verwenden. Typischerweise wird ein Parameter $r$, der nicht geheim gehalten werden muss, zusammen mit einem gemeinsamen Geheimnis $k_{AB}$ von Alice und Bob verarbeitet.

Eine wichtige Anforderung an die Schlüsselableitungsfunktion ist, dass sie eine Einwegfunktion sein muss. Hierdurch ist es einem Angreifer nicht möglich, von einem Sitzungsschlüssel, der bekannt wird, auf den Urschlüssel $k_{AB}$ zu schließen. Sollte ihm dies gelingen, könnte er alle Sitzungsschlüssel berechnen.

Eine Option zur Realisierung einer Schlüsselableitung besteht darin, dass ein Teilnehmer eine Nonce, d. h. einen numerischen Wert, der nur einmal verwendet wird, an den anderen Teilnehmer sendet. Beide Parteien verschlüsseln nun die Nonce mit dem gemeinsamen geheimen Schlüssel $k_{AB}$ und einem symmetrischen Algorithmus wie beispielsweise AES. Ein entsprechendes Protokoll ist nachfolgend dargestellt.