8.11 Signaturen, Hashfunktionen und die Praxis

Verschlüsselung schützt die Vertraulichkeit. Für Integrität und Authentizität kommen zwei weitere Bausteine hinzu.

Hashfunktionen berechnen aus einer beliebig langen Nachricht einen kurzen Wert fester Länge, den Fingerabdruck. Sie sind Einwegfunktionen: Aus dem Hashwert lässt sich die Nachricht nicht zurückgewinnen, und es soll praktisch unmöglich sein, zwei Nachrichten mit gleichem Hashwert zu finden (*Kollision*). Ändert sich ein einziges Bit der Nachricht, ändert sich der Hashwert vollständig. Aktuell ist SHA-256; ältere Verfahren wie MD5 und SHA-1 sind gebrochen – für sie lassen sich Kollisionen gezielt erzeugen – und dürfen für Sicherheitszwecke nicht mehr verwendet werden.

> LK
>
> Alles Weitere in diesem Abschnitt — digitale Signatur, Zertifikate und hybride Verfahren — steht nur im LK-Lehrplan („erläutern die Idee der digitalen Signatur anhand des RSA-Verfahrens", „erläutern die Idee hybrider Verschlüsselungsverfahren"). Die Hashfunktion oben gehört dagegen zum Schutzziel *Integrität* und damit in beide Kurse.

Digitale Signaturen drehen die asymmetrische Idee um. Der Absender verschlüsselt den Hashwert seiner Nachricht mit seinem *privaten* Schlüssel. Jeder kann diesen Wert mit dem *öffentlichen* Schlüssel prüfen und mit dem selbst berechneten Hashwert vergleichen. Stimmen beide überein, stammt die Nachricht vom Besitzer des privaten Schlüssels und wurde nicht verändert – Authentizität und Integrität in einem Schritt.

Offen bleibt: Woher weiß ich, dass ein öffentlicher Schlüssel wirklich zu der Person gehört, die draufsteht? Diese Lücke schließen **Zertifikate**. Eine Zertifizierungsstelle bestätigt mit ihrer eigenen Signatur die Zuordnung von Schlüssel und Inhaber. Ihr Zertifikat ist wiederum signiert – bis hinauf zu Wurzelzertifikaten, die im Betriebssystem und im Browser hinterlegt sind.

Hybride Verfahren verbinden schließlich beide Welten, denn asymmetrische Verfahren sind um Größenordnungen langsamer als symmetrische. Beim Aufruf einer Webseite über HTTPS läuft deshalb Folgendes ab:

1. Der Server sendet sein Zertifikat mit dem öffentlichen Schlüssel.
2. Der Browser prüft die Signaturkette bis zu einem Wurzelzertifikat.
3. Beide handeln asymmetrisch einen gemeinsamen, zufälligen Sitzungsschlüssel aus.
4. Die eigentlichen Daten werden symmetrisch mit diesem Sitzungsschlüssel verschlüsselt (AES).
5. Nach der Sitzung wird der Schlüssel verworfen.

Merke

Asymmetrisch wird der Schlüssel ausgetauscht, symmetrisch werden die Daten verschlüsselt. Das Schloss im Browser bedeutet genau das – und nicht, dass die Seite vertrauenswürdig ist.

Arbeitsauftrag 11

42. Erklären Sie, warum beim Signieren der Hashwert und nicht die ganze Nachricht verschlüsselt wird.
43. Ein Angreifer findet zwei verschiedene Verträge mit identischem MD5-Hashwert. Beschreiben Sie, welchen Schaden er damit anrichten kann.
44. Rufen Sie im Browser das Zertifikat einer beliebigen Webseite auf. Notieren Sie Aussteller, Gültigkeitsdauer und Schlüssellänge und ordnen Sie die Angaben diesem Kapitel zu.
45. Begründen Sie, warum das Schloss-Symbol nichts über die Seriosität des Anbieters aussagt.