Message Authentication Codes (MACs)

12

MAC, die auch kryptografische Prüfsummen genannt werden, kommen in der Praxis häufig zum Einsatz. Bezüglich ihrer Sicherheitsfunktionen ähneln MAC digitalen Signaturen, da sie auch Nachrichtenintegrität und Nachrichtenauthentisierung ermöglichen. Im Gegensatz zu digitalen Signaturen sind MAC jedoch symmetrische Verfahren, die keine Nichtzurückweisbarkeit zur Verfügung stellen können. Ein Vorteil von MAC ist, dass sie wesentlich schneller sind als digitale Signaturen, da sie auf Blockchiffren oder Hash-Funktionen basieren.

In diesem Kapitel erlernen Sie

- das Prinzip von MAC,
- Sicherheitseigenschaften von MAC,
- die Realisierung von MAC mithilfe von Hash-Funktionen und Blockchiffren.

12.1 Die Grundidee von Message-Authentiation-Codes

Ähnlich wie digitale Signaturen berechnen MAC eine Prüfsumme für eine gegebene Nachricht. Der entscheidende Unterschied zwischen MAC und digitalen Signaturen ist, dass MAC einen symmetrischen Schlüssel für die Erzeugung der Prüfsumme und für die Verifikation benutzen. Die Prüfsumme ist eine Funktion des symmetrischen Schlüssels k und der Nachricht x. Im Folgenden wird die Notation

$$m = \mathrm{MAC}_k(x)$$

verwendet. Das Prinzip der MAC-Berechnung und -Verifikation ist in Abb. 12.1 dargestellt.

Typischerweise werden MAC eingesetzt, wenn Alice und Bob sicherstellen möchten, dass eine Veränderung der Nachricht x während der Übertragung erkannt wird. Um dies zu erreichen, berechnet Bob den MAC als Funktion der Nachricht und des gehei-

C. Paar, J. Pelzl, *Kryptografie verständlich*, eXamen.press,
DOI 10.1007/978-3-662-49297-0_12

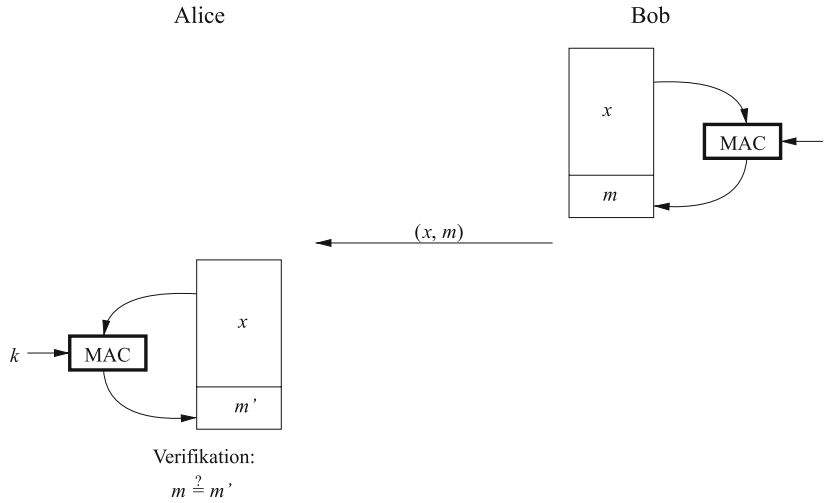

Abb. 12.1 Das Prinzip von Message-Authentication-Codes (MAC)

men Schlüssels k. Er sendet sowohl die Nachricht als auch die Prüfsumme m zu Alice. Wenn Alice die Nachricht und die Prüfsumme erhält, verifiziert sie beides. Da es sich um ein symmetrisches Verfahren handelt, braucht sie lediglich die gleichen Schritte wie Bob durchzuführen: Sie berechnet ebenfalls die Prüfsumme unter Benutzung der Nachricht und des geheimen Schlüssels.

Dem Verfahren liegt zugrunde, dass die MAC-Berechnung ein falsches Resultat liefert, wenn die Nachricht während der Übertragung verfälscht wurde. Daher stellen MAC den Sicherheitsdienst Nachrichtenintegrität zur Verfügung. Darüber hinaus weiß Alice mit Sicherheit, dass Bob tatsächlich der Sender der Nachricht war, da nur ein Besitzer des geheimen Schlüssels in der Lage ist, eine korrekte Prüfsumme zu berechnen. Ein Angreifer kann keine korrekte Prüfsumme berechnen, da er nicht über den geheimen Schlüssel verfügt. Jede bösartige oder zufällige (z. B. aufgrund eines Übertragungsfehlers) Veränderung der Nachricht wird vom Empfänger erkannt, da die Verifikation des MAC fehlschlagen wird. Somit wird auch der Sicherheitsdienst Nachrichtenauthentisierung zur Verfügung gestellt.

Wie bei Hash-Funktionen hat die Prüfsumme eine feste Länge, die unabhängig von der Länge der Nachricht ist. In der Praxis ist die Nachricht x zumeist wesentlich länger als die Prüfsumme. Die besprochenen Eigenschaften von MAC lassen sich wie folgt zusammenfassen:

Eigenschaften von Message Authentication Codes

1. **Kryptografische Prüfsumme** Ein MAC erzeugt eine kryptografisch sichere Prüfsumme für eine gegebene Nachricht.

2. **Symmetrisch** MAC basieren auf symmetrischen Schlüsseln. Sender und Empfänger müssen über einen gemeinsamen geheimen Schlüssel verfügen.
3. **Beliebige Nachrichtenlänge** MAC akzeptieren Nachrichten von beliebiger Länge.
4. **Feste Prüfsummenlänge** MAC erzeugen Prüfsummen mit einer festen Länge.
5. **Nachrichtenintegrität** Der Empfänger ist sich sicher, dass die Nachricht nicht verändert wurde.
6. **Nachrichtenauthentisierung** Der Empfänger ist sich sicher, von wem die Nachricht kommt.
7. **Keine Beweisbarkeit** Da MAC symmetrische Verfahren sind, kann mit ihnen keine Beweisbarkeit erreicht werden.

Der letzte Punkt ist besonders wichtig: MAC können keine Beweisbarkeit zur Verfügung stellen. Da die beiden Kommunikationspartner den gleichen geheimen Schlüssel besitzen, ist es nicht möglich, gegenüber einer neutralen dritten Partei, beispielsweise einem Richter, zu beweisen, ob die Nachricht und der dazugehörige MAC von Alice oder Bob stammen. Von daher bieten MAC keinen Schutz in Situationen, in denen Alice oder Bob sich potenziell unehrlich verhalten, wie in dem Beispiel zum Autokauf in Abschn. 10.1.1 diskutiert wurde. Ein symmetrischer Schlüssel ist nicht einer bestimmten Person zugeordnet, sondern zwei Teilnehmern. Von daher kann ein Richter im Fall eines Disputs nicht zwischen Alice und Bob unterscheiden.

In der Praxis gibt es zwei prinzipielle Ansätze, um MAC zu konstruieren, entweder unter Benutzung von Blockchiffren oder mithilfe von Hash-Funktionen. In den folgenden Abschnitten werden die beiden Konstruktionen vorgestellt.

12.2 MAC-Konstruktionen mit Hash-Funktionen

MAC können mit kryptografischen Hash-Funktionen, wie z.B. SHA-1, realisiert werden. Eine spezielle Konstruktion, die HMAC genannt wird, ist in den letzten zehn Jahren besonders beliebt geworden. Beispielsweise setzen sowohl das TLS-Protokoll, dessen Ausführung durch das kleine Vorhängeschloss in Webbrowsern angezeigt wird, als auch das IPsec-Protokoll die HMAC-Konstruktion ein. Ein Grund, warum sie so häufig eingesetzt wird, ist, dass HMAC unter gewissen Voraussetzungen beweisbar sicher sind.

Die Grundidee hinter allen Hash-basierten Verfahren zur Authentisierung von Nachrichten ist, dass der Schlüssel zusammen mit der Nachricht gehasht wird. Es gibt hierzu zwei naheliegende Konstruktionen. Der erste Ansatz

$$m = \mathrm{MAC}_k(x) = h(k \| x)$$