Einführung in die asymmetrische Kryptografie

6

Bevor wir mehr über die Grundlagen der asymmetrischen Kryptografie lernen, erinnern wir uns, dass neben dem Begriff *asymmetrische Kryptografie* auch häufig der englische Ausdruck *Public-Key-Kryptografie* verwendet wird. Beide bezeichnen ein und die selbe Gruppe von kryptografischen Techniken und werden synonym verwendet. Im Folgenden werden wir den Begriff der asymmetrischen Kryptografie verwenden.

Wie bereits in Kap. 1 beschrieben, wird symmetrische Kryptografie schon seit mindestens 4000 Jahren verwendet. Die asymmetrische Kryptografie ist dagegen recht neu und wurde öffentlich von Whitfield Diffie, Martin Hellman und Ralph Merkle im Jahr 1976 eingeführt. 1997 wurden jedoch britische Regierungsdokumente, die nicht mehr geheim gehalten werden mussten, veröffentlicht, aus denen hervorgeht, dass die Wissenschaftler James Ellis, Clifford Cocks und Graham Williamson vom UK Government Communications Headquarters (GCHQ) das Prinzip der asymmetrischen Kryptografie schon einige Jahre früher, nämlich 1972, entdeckt und umgesetzt hatten. Es ist allerdings nicht klar, ob sich die britischen Behörden über die weitreichenden Konsequenzen der asymmetrischen Kryptografie für kommerzielle Anwendungen bewusst waren.

In diesem Kapitel erlernen Sie

- eine kurze Zusammenfassung der Geschichte der asymmetrischen Kryptografie,
- die Vor- und Nachteile der asymmetrischen Kryptografie,
- Grundlagen der Zahlentheorie, die für das Verständnis von asymmetrischen Algorithmen notwendig sind. Insbesondere wird der erweiterte euklidische Algorithmus eingeführt.

6.1 Symmetrische versus asymmetrische Kryptografie

In diesem Kapitel werden wir sehen, dass asymmetrische Algorithmen sich völlig von symmetrischen Algorithmen wie DES oder AES unterscheiden. Die meisten asymmetrischen Verfahren basieren auf zahlentheoretischen Konstruktionen, was im Gegensatz zu

C. Paar, J. Pelzl, *Kryptografie verständlich*, eXamen.press, DOI 10.1007/978-3-662-49297-0_6

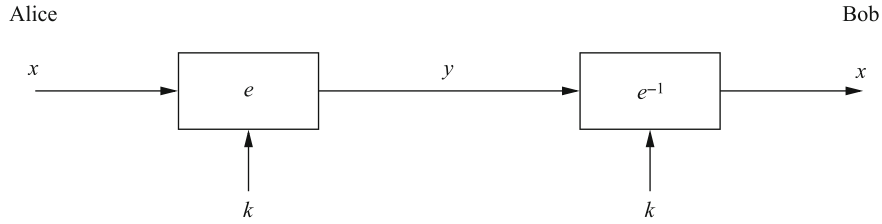

Abb. 6.1 Prinzip der symmetrischen Verschlüsselung

symmetrischen Chiffren steht, bei denen es normalerweise das Ziel ist, *keine* mathematisch einfache Beschreibung zwischen Ein- und Ausgang zu haben. Obwohl mathematische Strukturen oft für Komponenten *innerhalb* symmetrischer Chiffren genutzt werden, beispielsweise die MixColumn-Operation oder die S-Box von AES, bedeutet dies nicht, dass die gesamte Chiffre durch eine kompakte mathematische Beschreibung darstellbar ist.

6.1.1 Die Symmetrie bei der symmetrischen Kryptografie

Um das Prinzip der asymmetrischen Kryptografie besser verstehen zu können, schauen wir uns zunächst noch einmal das Prinzip der symmetrischen Verschlüsselung an (Abb. 6.1).

Solch ein System ist symmetrisch in Bezug auf folgende Eigenschaften:

1. *Derselbe geheime Schlüssel* wird für die Ver- und Entschlüsselung verwendet.
2. Die *Funktionen* zu Ver- und Entschlüsselung sind sich sehr ähnlich (im Fall von DES sind sie praktisch identisch).

Es gibt eine einfache Analogie für die symmetrische Kryptografie (Abb. 6.2) gezeigt ist. Wir nehmen einen Safe mit einem starken Schloss an. Nur Alice und Bob haben eine Kopie des Schlüssels für das Schloss. Das Verschlüsseln von Daten kann als Deponieren von Nachrichten in dem Safe interpretiert werden. Um die Nachricht wieder lesen, d. h. entschlüsseln, zu können, verwendet Bob seinen Schlüssel und öffnet den Safe.

Moderne symmetrische Algorithmen wie AES oder 3DES werden als sehr sicher angesehen, verschlüsseln sehr effizient und sind in unzähligen Anwendungen im Einsatz. Dennoch weisen alle symmetrischen Verfahren einige grundsätzliche Nachteile auf, die wir nachfolgend diskutieren.

Schlüsselaustauschproblem Der symmetrische Schlüssel muss zwischen Alice und Bob über einen sicheren Kanal ausgetauscht werden. Gleichzeitig ist der Kommunikationskanal selbst nicht sicher. Daher kann der Schlüssel nicht direkt über diese Verbindung geschickt werden, was zweifelsfrei der bequemste Weg wäre, und es wird eine andere Übertragungsform benötigt.