Einführung in die Kryptografie und Datensicherheit

1

In diesem Kapitel werden Grundbegriffe der modernen Kryptografie eingeführt. Unter anderem werden wichtige Fachausdrücke und der Unterschied zwischen öffentlich bekannten und proprietären, d. h. geheim gehaltenen, Chiffren besprochen. Ebenso werden die Grundlagen der modularen Arithmetik eingeführt, die von zentraler Bedeutung für die asymmetrische Kryptografie sind.

In diesem Kapitel erlernen Sie

- die Grundregeln der Kryptografie,
- Schlüssellängen für kurz-, mittel- und langfristige Sicherheit,
- die unterschiedlichen Angriffsmöglichkeiten gegen Chiffren,
- einige historische Chiffren; hierbei wird auch die modulare Arithmetik eingeführt, die in der modernen Kryptografie eine wichtige Rolle spielt,
- Gründe, warum man nur öffentliche und gut untersuchte Chiffren einsetzen sollte.

1.1 Überblick über die Kryptografie (und dieses Buch)

Wenn das Wort *Kryptografie* fällt, denkt man schnell an E-Mail-Verschlüsselung, Internetsicherheit, Kryptowährungen à la Bitcoin oder auch Codebrechen im Zweiten Weltkrieg wie den Angriff auf die berühmte Enigma-Chiffriermaschine, die in Abb. 1.1 zu sehen ist.

Es erscheint offensichtlich, dass Kryptografie zwangsläufig mit moderner elektronischer Datenübertragung verbunden ist. Dem ist allerdings nicht so: Frühe Formen der Kryptografie sind schon seit etwa 2000 v. Chr. bekannt, als in Ägypten neben den Standard-Hieroglyphen auch „geheime“ Varianten eingesetzt wurden. Seitdem wurde in den letzten 4000 Jahren Kryptografie in vielen, vielleicht sogar in den meisten Kulturen mit Schrift eingesetzt. Prominente Beispiele sind die sog. *Scytale* (Abb. 1.2) oder die Cäsar-Chiffre im antiken Rom, über die wir in diesem Kapitel noch mehr lernen werden.

C. Paar, J. Pelzl, *Kryptografie verständlich*, eXamen.press, DOI 10.1007/978-3-662-49297-0_1

Abb. 1.1 Die Enigma-Chiffriermaschine (Abdruck mit Erlaubnis des Deutschen Museums in München)

In diesem Buch werden allerdings fast ausschließlich moderne kryptografische Verfahren sowie deren Einsatz in der modernen IT-Sicherheit behandelt.

In Abb. 1.3 ist das Gebiet der Kryptologie mit seinen Untergebieten dargestellt. Zunächst fällt auf, dass der Oberbegriff *Kryptologie* lautet und nicht *Kryptografie*. Die Kryptologie zerfällt in zwei große Themenbereiche:

► Die **Kryptografie** beschäftigt sich mit der *Absicherung* von Daten, z. B. der Verschlüsselung von Nachrichten.

► Die **Kryptanalyse** beschäftigt sich mit dem *Brechen* von Kryptosystemen. Es erscheint zunächst überraschend, dass das Brechen von Codes eine wissenschaftliche Disziplin ist; unsere Annahme wäre eher, dass dies Kriminellen oder Geheimdiensten vorbehalten sei. Es ist aber tatsächlich so, dass die meisten Kryptanalysten heutzutage Wissenschaftler sind. Die Kryptanalyse ist von zentraler Bedeutung für die moderne

Abb. 1.2 Verschlüsselung mit der Scytale im antiken Sparta

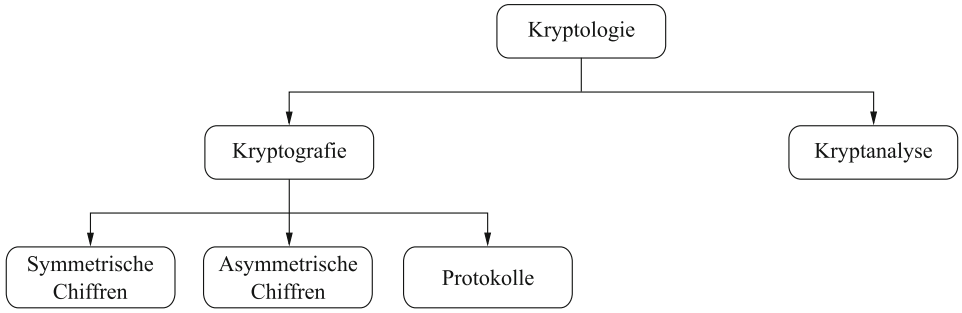

Abb. 1.3 Die Kryptologie und ihre Untergebiete

Kryptografie. Ohne sie wäre es unmöglich einzuschätzen, ob kryptografische Algorithmen sicher sind oder nicht. Dieser wichtige Aspekt wird in Abschn. 1.3 näher diskutiert.

Da die Kryptanalyse der Hauptansatz ist, mit der die Sicherheit von Kryptoverfahren nachgewiesen wird, ist sie fester Bestandteil der Kryptologie. Nichtsdestotrotz liegt der Fokus dieses Buchs auf der Krypto**grafie**. In diesem Buch werden die meisten Kryptoalgorithmen mit praktischer Relevanz im Detail erklärt. Es werden nur Algorithmen betrachtet, die schon seit vielen Jahren intensiv von Kryptanalysten untersucht und bei denen keine Schwachstellen gefunden wurden. Die meisten Kryptoverfahren, die behandelt werden, sind schon seit einigen Jahrzehnten ungebrochen. Obwohl in dem Buch nur vereinzelt Techniken zum Brechen von Codes behandelt werden, werden für alle Kryptoverfahren Sicherheitseinschätzungen basierend auf den jüngsten kryptanalytischen Ergebnissen beschrieben, beispielsweise der Faktorisierungsrekord für Angriffe gegen das RSA-Verschlüsselungsverfahren.

Wir betrachten jetzt die Teilgebiete der Kryptografie, die in Abb. 1.3 dargestellt sind:

► **Symmetrische Algorithmen** sind die bekannteste und auch intuitivste Form der Kryptografie. Zwei Parteien besitzen eine Chiffre zum Ver- und Entschlüsseln und haben sich auf einen gemeinsamen geheimen Schlüssel geeinigt. Die gesamte Kryptografie von der Antike bis in das Jahr 1976 folgte diesem Ansatz. Symmetrische Algorithmen sind fester Bestandteil nahezu jedes heutigen Kryptosystems. Sie werden insbesondere für die eigentliche Verschlüsselung von Daten und zum Integritätsschutz, d. h. Schutz gegen Veränderungen, eingesetzt.

► **Asymmetrische (oder Public-Key-) Algorithmen** Im Jahr 1976 wurde von Whitfield Diffie, Martin Hellman und Ralph Merkle eine gänzlich neue Art der Kryptografie eingeführt. Bei der asymmetrischen Kryptografie besitzt ein Teilnehmer einen geheimen Schlüssel, ähnlich der symmetrischen Kryptografie. Der Teilnehmer hat aber auch einen öffentlichen Schlüssel, der nicht geheim, sondern allgemein bekannt ist. Mit asymmetrischen Algorithmen können Dienste wie das digitale Signieren von Daten oder der Aus-

tausch von geheimen Schlüsseln über unsichere Kanäle realisiert werden. Darüber hinaus kann man sie auch für die klassische Nachrichtenverschlüsselung benutzen.

► **Kryptografische Protokolle** Grob gesagt werden mit Kryptoprotokollen Anwendungen basierend auf kryptografischen Algorithmen konstruiert. Hierbei kommen sowohl symmetrische als auch asymmetrische Algorithmen zum Einsatz. Ein Beispiel ist das Transport-Layer-Security(TLS)-Protokoll (auch als SSL bekannt), das von jedem Webbrowser verwendet wird.

Genau genommen gibt es noch eine dritte Algorithmenfamilie, die von Hash-Funktionen gebildet wird, die in Kap. 11 eingeführt werden. Da Hash-Funktionen aber viele Ähnlichkeiten mit symmetrischen Chiffren aufweisen, werden sie oft zusammen mit diesen gruppiert.

In der Mehrzahl von kryptografischen Anwendungen in der Praxis kommen sowohl symmetrische als auch asymmetrische Algorithmen (und oft auch Hash-Funktionen) zum Einsatz. Man spricht in diesem Zusammenhang manchmal von *Hybridsystemen*. Der Grund dafür, dass beide Algorithmenfamilien zum Einsatz kommen, ist, dass beide Arten von Chiffren ihre spezifischen Vorteile haben.

Der Fokus dieses Buchs liegt auf symmetrischen und asymmetrischen Algorithmen sowie auf Hash-Funktionen. Darüber hinaus werden auch die Grundlagen von Sicherheitsprotokollen eingeführt, insbesondere Protokolle zur Schlüsselvereinbarung. Ebenso wird besprochen, welche sog. Sicherheitsdienste mit Protokollen realisiert werden können, z. B. Vertraulichkeit, Integrität oder Authentisierung von Nachrichten.

1.2 Symmetrische Kryptografie

In diesem Abschnitt werden die Grundlagen symmetrischer Chiffren eingeführt und ein historisches Verschlüsselungsverfahren vorgestellt, die Substitutionschiffre. Anhand der Substitutionschiffre werden die beiden grundlegenden Angriffsverfahren, die vollständige Schlüsselsuche und die analytischen Attacken, eingeführt.

1.2.1 Grundlagen

Das Prinzip der symmetrischen Kryptografie kann man anhand eines naheliegenden Beispiels gut veranschaulichen. Wie in Abb. 1.4 dargestellt, möchten zwei Benutzer, die in der Literatur gerne Alice und Bob genannt werden, über einen *unsicheren Kanal* kommunizieren. Der leicht abstrakte Begriff „Kanal“ bezeichnet lediglich die Kommunikationsstrecke, z. B. das Internet, eine Luftstrecke im Fall von WLAN oder Mobilfunk oder jedes andere Medium, über das sich digitale Daten übertragen lassen. Aus kryptografischer Sicht wird die Situation durch den Gegenspieler Oskar interessant, der Zugriff auf den Kanal hat und