Stromchiffren

2

Die Welt der symmetrischen Algorithmen teilt sich in die beiden Hauptfamilien der Strom- und Blockchiffren auf, wie in Abb. 2.1 dargestellt.

In diesem Kapitel erlernen Sie

- die Vor- und Nachteil von Stromchiffren,
- echte Zufallszahlengeneratoren und Pseudozufallsgeneratoren,
- eine beweisbar sichere Chiffre, das One-Time-Pad (OTP),
- lineare Schieberegister und Trivium, eine moderne Stromchiffre.

2.1 Einführung

2.1.1 Stromchiffren und Blockchiffren

In der symmetrischen Kryptografie unterscheidet man zwischen Block- und Stromchiffren. In Abb. 2.2 sind die Grundprinzipien der beiden Algorithmenfamilien dargestellt. Die Eingabe zu den Chiffren beträgt in beiden Fällen b Bit, wobei b auch die Eingangsweite der Blockchiffre ist.

Das Funktionsprinzip der beiden Chiffrenarten wird nachfolgend erläutert.

► Ein **Stromchiffre** verschlüsselt jedes Klartextbit einzeln. Dies geschieht, indem ein Bit des sog. *Schlüsselstroms* zu dem Klartextbit addiert wird. Man unterscheidet zwischen synchronen Stromchiffren, bei denen der Schlüsselstrom nur von dem eigentlichen Schlüssel abhängt, und asynchronen Stromchiffren, bei den der Schlüsselstrom zusätzlich von dem Chiffrat abhängt. Die gepunktete Linie in Abb. 2.3 ist nur bei einer asynchronen Stromchiffre gegeben. In der Praxis werden mehr synchrone als asynchrone Stromchiffren eingesetzt, und Abschn. 2.3 dieses Kapitels behandelt synchrone Chiffren. Ein Beispiel für eine asynchrone Stromchiffre ist der Cipher-Feedback-Modus in Abschn. 5.1.4.

C. Paar, J. Pelzl, *Kryptografie verständlich*, eXamen.press, DOI 10.1007/978-3-662-49297-0_2

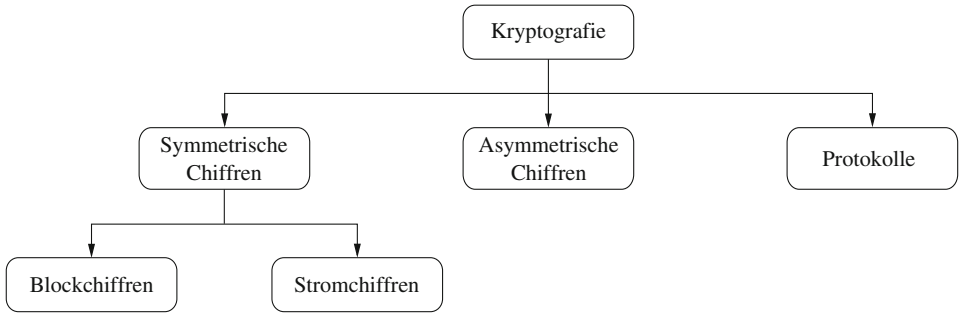

Abb. 2.1 Die Hauptgebiete der Kryptografie

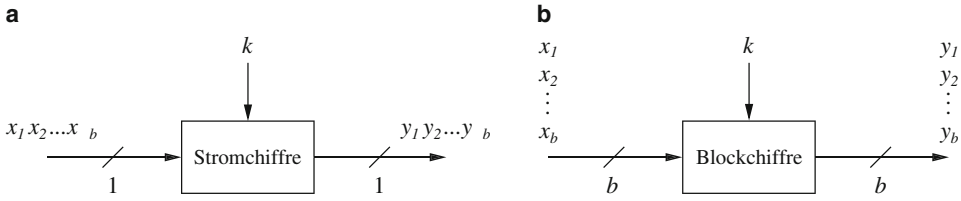

Abb. 2.2 Prinzip der Verschlüsselung von b Bit mit **a** einer Stromchiffre und **b** einer Blockchiffre

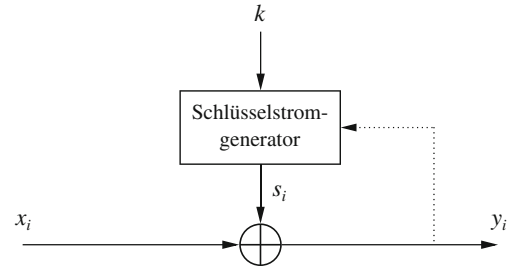

Abb. 2.3 Synchrone und asynchrone (*gepunktete Verbindung*) Stromchiffre

► Eine **Blockchiffre** verschlüsselt einen Block aus b Bit gleichzeitig mit dem gleichen Schlüssel. Hierbei beeinflusst jedes Bit die Verschlüsselung jedes anderen Bits in dem Block. Die allermeisten Blockchiffren haben entweder eine Blockbreite von 128 Bit, d. h. 16 Byte, wie der Advanced Encryption Standard (AES), oder von 64 Bit, d. h. 8 Byte, wie der Data Encryption Standard (DES) oder der 3DES-Algorithmus. Diese Chiffren werden in nachfolgenden Kapiteln eingeführt.

Dieses Kapitel gibt eine Einführung in Stromchiffren. Zunächst einige Fakten über Stromchiffren und Blockchiffren in der Praxis:

1. In vielen praktischen Anwendungen, insbesondere für Verschlüsselung im Internet, werden wesentlich häufiger Blockchiffren als Stromchiffren eingesetzt.

2. Weil Stromchiffren oft klein und schnell sind, sind sie attraktiv für Anwendungen, bei denen vergleichsweise wenig Rechenleistung zur Verfügung steht, beispielsweise Mobiltelefone oder andere eingebettete Geräte. Eine weit verbreitete Stromchiffre ist der Algorithmus A5/1, der Teil des GSM-Mobilfunkstandards ist und die eigentlichen Gesprächsdaten chiffriert. Für Datenverschlüsselung im Internet wird manchmal die Stromchiffre RC4 verwendet[1].
3. Früher galt die generelle Annahme, dass Stromchiffren effizienter als Blockchiffren sind. *Effizient* bedeutet im Fall von Software, dass die Chiffre nur wenig Taktzyklen (oder CPU-Befehle) für die Verschlüsselung eines Klartextbits benötigt. Wenn die Chiffre in Hardware realisiert wird, bedeutet effizient, dass sie mit wenigen logischen Gattern implementiert werden kann und somit nur wenig Chipfläche in Anspruch nimmt. Diese Argumente gelten heutzutage jedoch nicht mehr in dem gleichen Maß. Einige moderne Blockchiffren wie AES sind ebenfalls sehr effizient in Software. In den letzten 10 Jahren wurde zudem eine Reihe sog. *leichtgewichtiger Chiffren* („lightweight ciphers“) entwickelt, die für Hardware optimiert wurde. Die Blockchiffre PRESENT, die in Abschn. 3.7.3 behandelt wird, ist ein bekannter Vertreter einer leichtgewichtigen Chiffre.

2.1.2 Die Ver- und Entschlüsselung mit Stromchiffren

Wie eingangs erwähnt, verschlüsseln Stromchiffren die Klartextbits einzeln. Die Frage, die wir in diesem Abschnitt beantworten werden, lautet: Wie genau werden die individuellen Bits verschlüsselt? Die Antwort ist verblüffend einfach: Jedes Bit x_i wird verschlüsselt, indem ein geheimes Bit s_i des Schlüsselstroms modulo 2 aufaddiert wird.

Definition 2.1 (Ver- und Entschlüsselung mit Stromchiffren)
Der Klartext, das Chiffrat und der Schlüsselstrom bestehen aus individuellen Bits $x_i, y_i, s_i \in \{0, 1\}$.

Verschlüsselung: $y_i = e_{s_i}(x_i) \equiv x_i + s_i \bmod 2$
Entschlüsselung: $x_i = d_{s_i}(y_i) \equiv y_i + s_i \bmod 2$

Da sowohl die Ver- als auch die Entschlüsselung einfache Additionen modulo 2 sind, kann die grundsätzliche Funktionsweise einer Stromchiffre wie in Abb. 2.4 gezeigt dargestellt werden. Der Kreis mit dem Plus-Symbol steht für die Addition modulo 2.

[1] Man beachte, dass A5/1 und RC4 beide heutzutage nicht mehr als uneingeschränkt sicher gelten.