Mehr über Blockchiffren

5

Eine Blockchiffre ist wesentlich mehr als nur ein Algorithmus zur Verschlüsselung. Als vielseitiger Baustein kann sie für unterschiedliche kryptografische Mechanismen eingesetzt werden. Zum einen können mit Blockchiffren eine ganze Reihe verschiedener blockorientierter Verschlüsselungsverfahren oder gar Stromchiffren konstruiert werden. Die unterschiedlichen Verschlüsselungsmöglichkeiten nennt man *Betriebsmodi* und werden in diesem Kapitel behandelt. Zum anderen können Blockchiffren auch für die Konstruktion von Hash-Funktionen, für kryptografische Checksummen (auch als Message-Authentication-Codes oder MAC bekannt) und in Schlüsselaustauschprotokollen genutzt werden, was in nachfolgenden Kapiteln beschrieben wird. Darüber hinaus finden Blockchiffren auch als Pseudozufallszahlengeneratoren (PRNG) Verwendung. Neben Betriebsmodi werden wir in diesem Kapitel zwei nützliche Techniken zur Erhöhung der Sicherheit von Blockchiffren besprechen: Key Whitening und Mehrfachverschlüsselung.

In diesem Kapitel erlernen Sie

- die wichtigsten praxisrelevanten Betriebsmodi für Blockchiffren,
- Sicherheitsfallen bei der Verwendung von Betriebsmodi,
- das Prinzip des Key Whitening,
- warum die Doppelverschlüsselung mit Blockchiffren kaum einen Sicherheitsgewinn darstellt sowie den Meet-in-the-Middle-Angriff,
- das Prinzip der Dreifachverschlüsselung.

5.1 Verschlüsselung mit Blockchiffren: Betriebsmodi

In den vorangegangenen Kapiteln wurde gezeigt, wie man mit AES, DES, 3DES und PRESENT einen Klartextblock verschlüsselt. In der Praxis möchte man jedoch fast immer mehr als einen 8 Byte oder 16 Byte großen Datenblock verschlüsseln, beispielsweise

C. Paar, J. Pelzl, *Kryptografie verständlich*, eXamen.press, DOI 10.1007/978-3-662-49297-0_5

bei der Verschlüsselung einer E-Mail oder einer Datei. Es gibt eine ganze Reihe von Verfahren, um lange Klartexte mit einer Blockchiffre zu verschlüsseln. Wir führen in diesem Kapitel die bekanntesten sogenannten Betriebsmodi ein:

- Electronic-Codebook-Modus (ECB),
- Cipher-Block-Chaining-Modus (CBC),
- Cipher-Feedback-Modus (CFB),
- Output-Feedback-Modus (OFB),
- Counter-Modus (CTR),
- Galois-Counter-Modus (GCM).

Die letzten vier Modi verwenden die Blockchiffre als Baustein, um eine Stromchiffre zu realisieren. Jeder der sechs Modi hat ein Ziel: Verschlüsselung von Daten, um damit die Vertraulichkeit des Nachrichtenaustauschs zwischen Alice und Bob zu ermöglichen. In der Praxis wird oft nicht nur Vertraulichkeit benötigt, sondern Bob möchte auch wissen, ob die Nachricht wirklich von Alice stammt, was man Authentisierung nennt. Der Galois-Counter-Modus (GCM) ist ein Betriebsmodus, der den Empfänger (Bob) überprüfen lässt, ob die Nachricht wirklich von der Person, mit der er den Schlüssel teilt, gesendet wurde (Alice). Darüber hinaus erlaubt die Authentisierung Bob, zu erkennen, ob das Chiffrat während der Übertragung verändert wurde, d. h. ob die Nachrichtenintegrität gewahrt ist. Die Themen Authentisierung und Nachrichtenintegrität werden in Kap. 10 näher diskutiert.

Für den ECB- und den CFB-Modus muss die Länge des Klartexts ein genaues Vielfaches der Blockgröße der verwendeten Chiffre sein, also z. B. im Fall von AES ein Vielfaches von 16 Byte. Hat der Klartext nicht diese Länge, muss er mit dem sogenannten Padding erweitert werden. Es gibt eine Reihe von Möglichkeiten, ein solches Padding praktisch umzusetzen. Eine Padding-Methode besteht aus dem Anhängen eines einzelnen 1-Bit gefolgt von so vielen 0-Bits, wie zum Erreichen der Blockgröße notwendig sind. Wenn der Klartext schon ein exaktes Vielfaches der Blockgröße sein sollte, wird ein Extrablock, der nur aus Paddingbits besteht, angehängt.

5.1.1 Electronic-Codebook-Modus

Der *ECB* ist der einfachste und nächstliegende Weg, Nachrichten zu verschlüsseln. Im Folgenden bezeichnet $e_k(x_i)$ die Verschlüsselung eines Klartextblocks x_i mit dem Schlüssel k, wobei $e(\cdot)$ eine beliebige Blockchiffre ist. $e_k^{-1}(y_i)$ bezeichnet die Entschlüsselung des Chiffratblocks y_i mit dem Schlüssel k. Wir nehmen an, die Blockchiffre verschlüsselt (bzw. entschlüsselt) Blöcke mit einer Länge von b Bit. Nachrichten, die länger sind, werden in b Bit große Blöcke unterteilt. Ist die Nachricht kein Vielfaches von b Bit, so muss sie vor der Verschlüsselung durch geeignetes Padding auf ein Vielfaches von b Bit aufgefüllt werden. Wie in Abb. 5.1 gezeigt, wird beim ECB-Modus jeder Block separat

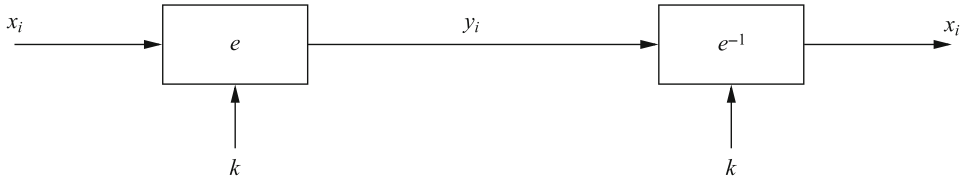

Abb. 5.1 Ver- und Entschlüsselung im Electronic-Codebook-Modus

verschlüsselt. Bei der Blockchiffre kann es sich beispielsweise um AES oder 3DES handeln.

Ver- und Entschlüsselung im ECB-Modus können formal wie folgt beschrieben werden:

Definition 5.1 (Electronic-Codebook-Modus (ECB))
Sei $e(\cdot)$ eine Blockchiffre mit Blockgröße b und seien x_i und y_i Bitblöcke der Länge b.

Verschlüsselung: $y_i = e_k(x_i), i \geq 1$
Entschlüsselung: $x_i = e_k^{-1}(y_i), i \geq 1$

Die Korrektheit des ECB-Modus lässt sich einfach zeigen, da gilt:

$$e_k^{-1}(y_i) = e_k^{-1}(e_k(x_i)) = x_i$$

Der ECB-Modus hat einige Vorteile. Es ist keine Synchronisation der Blöcke zwischen Sender und Empfänger (Alice und Bob) notwendig, d. h. wenn der Empfänger aufgrund von Übertragungsproblemen nicht alle verschlüsselten Blöcke erhält, ist es trotzdem möglich, alle empfangenen Blöcke zu dechiffrieren. Ebenso wirken sich Bitfehler, die möglicherweise auf dem Übertragungskanal in das Chiffrat eingebracht werden, nur auf den betroffenen Block, nicht aber auf die darauffolgenden Blöcke aus. Darüber hinaus können Blockchiffren im ECB-Modus parallelisiert werden. Hierbei chiffriert eine Verschlüsselungseinheit den ersten Block, eine weitere den nächsten Block etc. Die Parallelisierung, die in manchen anderen Betriebsmodi wie dem CFB-Modus nicht möglich ist, ermöglicht eine hohe Verschlüsselungsgeschwindigkeit.

Wie so oft in der Kryptografie hat der ECB-Modus allerdings auch Schwächen, die auf den ersten Blick nicht auffallen. Das Hauptproblem des ECB-Modus ist, dass er vollkommen deterministisch verschlüsselt. Das bedeutet, dass identische Klartextblöcke in identischen Chiffratblöcken resultieren, solange sich der Schlüssel nicht ändert. Der ECB-Modus kann als ein sehr großes Codebuch betrachtet werden – daher auch der Name des Modus –, das jeden Eingangsblock auf einen festen, bestimmten Ausgangswert abbildet. Das gesamte Codebuch ändert sich zwar, wenn der Schlüssel gewechselt