Der Data Encryption Standard und Alternativen 3

Der *Data Encryption Standard (DES)* war über 30 Jahre die bei Weitem verbreitetste Blockchiffre. Auch wenn DES selbst aufgrund des zu kleinen Schlüsselraums heute als unsicher gilt, kann man mit einer dreifachen DES-Verschlüsselung eine sehr sichere Chiffre bauen. Dieser *3DES* oder auch *Triple-DES* genannte Algorithmus wird in Abschn. 3.7.2 behandelt und in vielen modernen Anwendungen eingesetzt. Das Verstehen von DES ist aus heutiger Sicht auch wichtig, da es sich um den am besten untersuchten symmetrischen Algorithmus handelt, dessen Design viele aktuelle Chiffren beeinflusst hat.

In diesem Kapitel erlernen Sie

- den Entwurfprozess des DES, der sehr hilfreich für das Verständnis von technischen Details, aber auch der politischen Hintergründe bei der Entstehung der modernen Kryptografie ist,
- die grundlegenden Operationen, aus denen Blockchiffren aufgebaut sind; hierzu gehören die Konzepte der Konfusion und Diffusion,
- die interne Struktur des DES mit Feistel-Netzwerk, S-Box und Schlüsselfahrplan,
- die Sicherheitseinschätzung des DES,
- die Alternativen zum DES, u. a. 3DES und die Lightweight-Chiffre PRESENT.

3.1 Einführung zum DES

1972 unternahm das amerikanische National Bureau of Standards (NBS), das heute *National Institute of Standards and Technology (NIST)* heißt, einen Schritt, der aus damaliger Sicht revolutionär war: Das NBS initiierte eine Ausschreibung, um ein Verschlüsselungsverfahren in den USA zu standardisieren. Das Ziel war es, eine einzelne sichere Chiffre zu finden, die in zahlreichen Anwendungen eingesetzt werden kann. Bis zu diesem Punkt

C. Paar, J. Pelzl, *Kryptografie verständlich*, eXamen.press, DOI 10.1007/978-3-662-49297-0_3

hatten Regierungen weltweit die Kryptografie und insbesondere die Kryptanalyse als für so kritisch für die nationale Sicherheit gehalten, dass diese schlichtweg geheim gehalten wurden. Indes war Anfang der 1970er-Jahre der Bedarf für Verschlüsselung im kommerziellen Bereich, insbesondere im Bankwesen, so pressierend geworden, dass man diesen nicht ohne Auswirkung auf die Gesamtwirtschaft ignorieren konnte.

Das NBS erhielt 1974 den vielversprechendsten Algorithmenvorschlag von einem Team von Kryptografen von IBM. Der von IBM eingereichte Algorithmus basierte auf der Chiffre *Lucifer*. Lucifer war eine von Horst Feistel in den 1960er-Jahren entwickelte Familie von Chiffren und auch eine der ersten Blockchiffren, die für digitale Daten entworfen worden war. Lucifer ist eine sog. Feistel-Chiffre, die Blöcke von 64 Bit mit einem 128-Bit-Schlüssel chiffriert. Um die Sicherheit des eingereichten Algorithmus zu untersuchen, hatte das NBS um die Hilfe der *National Security Agency (NSA)* ersucht, die zu diesem Zeitpunkt noch nicht einmal ihre Existenz zugegeben hatte[1]. Es scheint sicher zu sein, dass die NSA auf Änderungen der Chiffre gedrungen hatte. Die veränderte Chiffre wurde Data Encryption Standard (DES) genannt. Eine der Änderungen war eine Härtung von DES gegen die sog. differenzielle Kryptanalyse, eine mächtige Angriffsmethode, die bis 1990 nicht öffentlich bekannt war. Bis heute ist nicht klar, ob das Wissen über die differenzielle Kryptanalyse von dem IBM-Team selbst entwickelt worden war oder ob die NSA hier einen starken Einfluss gehabt hatte. Die NSA überzeugte IBM auch, die Lucifer-Schlüssellänge von 128 auf 56 Bit zu reduzieren, was die Chiffre wesentlich schwächer gegen Brute-Force-Angriffe macht.

Die Beteiligung der NSA hatte in manchen Kreisen auch zu Besorgnis geführt, da man befürchtete, dass der Einbau einer geheimen Hintertür der wahre Grund für die Modifikationen des DES war. Die Sorge war, dass DES eine mathematische Eigenschaft besaß, mithilfe derer die NSA den DES brechen konnte. Ein anderer wesentlicher Kritikpunkt war die Reduktion der Schlüssellänge. Es wurde gemutmaßt, dass die NSA dazu in der Lage sei, einen Schlüsselraum von 2^{56} zu durchsuchen und damit DES durch Brute-Force-Angriff zu brechen. In den darauffolgenden Jahrzehnten stellten sich die meisten dieser Sorgen als gegenstandslos heraus. In Abschn. 3.5 werden die tatsächlichen und vermeintlichen Schwächen des DES weiter diskutiert.

Trotz aller Kritik veröffentlichte die NBS 1977 die modifizierte Chiffre als den *Data Encryption Standard (FIPS PUB 46)*. Obwohl die Chiffre in dem Standard bis auf die unterste Bit-Ebene spezifiziert ist, wurden die Hintergründe, warum die einzelnen Komponenten der Chiffre genau so gewählt worden waren (man spricht hier von den sog. Designkriterien), nie veröffentlicht. Dies betraf insbesondere die S-Boxen, die das Herzstück des DES sind.

Mit der rapiden Verbreitung von PC Anfang der 1980er-Jahre und der öffentlichen Verfügbarkeit aller Spezifikationen des DES wurde es einfacher, die innere Struktur der Chif-

[1] Ein gängiger Witz damals war, dass NSA die Abkürzung für „no such agency“ sei.

fre zu analysieren. Während dieser Zeit unterzogen auch mehr und mehr Wissenschaftler DES einer genauen Prüfung. Dennoch wurden bis 1990 keine wesentlichen Schwachstellen festgestellt. Ursprünglich war DES nur für 10 Jahre – bis 1987 – als Standard festgeschrieben worden. Durch die weite Verbreitung von DES und da zum damaligen Zeitpunkt keine ernsthaften Schwachstellen bekannt waren, verlängerte das NIST den DES-Standard bis 1999, als DES letztlich vom *Advanced Encryption Standard (AES)* abgelöst wurde.

3.1.1 Konfusion und Diffusion

Bevor wir uns der detaillierten Betrachtung von DES widmen, ist es aufschlussreich, sich die grundlegenden Operationen anzuschauen, mit denen man eine starke Verschlüsselung erreicht. Dem Begründer der modernen Informationstheorie, Claude Shannon, zufolge gibt es zwei grundlegende Operationen, mit denen starke Chiffren realisiert werden können:

1. **Konfusion** ist eine Verschlüsselungsoperation, die die Beziehung zwischen Schlüssel und Chiffrat verschleiert. Substitutionstabellen sind heutzutage das gängigste Element, um Konfusion zu erreichen. Sie finden sich sich sowohl im DES als auch im AES.
2. **Diffusion** ist eine Verschlüsselungsoperation, bei der der Einfluss eines Klartextsymbols auf zahlreiche Chiffratsymbole gestreut wird, um statistische Eigenschaften des Klartexts zu verbergen. Ein einfaches Beispiel, um Diffusion zu erreichen, ist die Bitpermutation, die von DES verwendet wird. AES benutzt eine komplexere Diffusionsfunktion, die MixColumn-Operation.

Chiffren wie beispielsweise die im Zweiten Weltkrieg eingesetzte Enigma oder die Schiebechiffre (vgl. Abschn. 1.4.3), die lediglich Konfusion verwenden, sind nicht sicher. Gleiches gilt für Chiffren, die nur Diffusion durchführen. Dennoch kann durch ein Hintereinanderschalten beider Operationen eine starke Chiffre gebildet werden. Die Idee der Hintereinanderschaltung („concatenation“) von Verschlüsselungsoperationen wurde auch von Shannon vorgeschlagen. Solche Algorithmen werden auch *Produktchiffren* genannt. Alle heutigen Blockchiffren sind Produktchiffren, da sie aus sich wiederholenden Runden bestehen (vgl. Abb. 3.1), die die Eingangsdaten sukzessiv verschlüsseln.

Moderne Blockchiffren besitzen hervorragende Diffusionseigenschaften. Auf Ebene der Chiffre bedeutet dies, dass die Änderung eines Bits im Klartext die Änderung von *durchschnittlich* der Hälfte aller Ausgabebits zur Folge hat. Das heißt, dass zwei Chiffrate, deren Klartexte sich in nur einem Bit unterscheiden, statistisch vollkommen unabhängig sind. Wenn man sich mit Blockchiffren beschäftigt, ist diese Verwürfelungseigenschaft sehr wichtig. Das folgende einfache Beispiel zeigt dieses Verhalten.

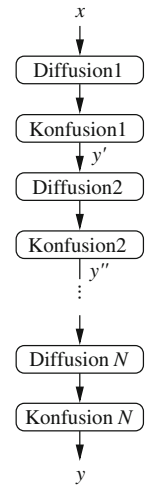

Abb. 3.1 Prinzip einer N-Runden-Produktchiffre, bei der in jeder Runde eine Konfusions- und eine Diffusionsoperation durchgeführt wird

Abb. 3.2 Prinzip der Diffusion einer Blockchiffre

Beispiel 3.1 Angenommen wir haben eine extrem kleine Blockchiffre mit einer Blockgröße von 8 Bit. Die Verschlüsselung zweier Klartexte x_1 und x_2, die sich nur in einem einzigen Bit unterscheiden, sollte ein Chiffrat ergeben wie in Abb. 3.2 gezeigt, d. h. etwa die Hälfte der Ausgangsbits sollten sich ändern.

Anmerkung: Moderne Blockchiffren haben eine Eingangsgröße von 64 oder 128 Bit und zeigen das oben skizzierte Verhalten im Fall eines veränderten Eingangsbits.

3.2 Übersicht über den DES-Algorithmus

DES ist ein Algorithmus, der Blöcke von 64 Bit mit einem 56-Bit-Schlüssel chiffriert (Abb. 3.3). DES ist eine symmetrische Chiffre, d. h. es wird derselbe Schlüssel für die Ver- und Entschlüsselung verwendet. DES, wie alle modernen Blockchiffren, ist ein iterativer Algorithmus. Für jeden Klartextblock wird die Verschlüsselung in 16 Runden durchgeführt, die alle identische Operationen ausführen. Abb. 3.4 zeigt die Rundenstruktur des DES. In jeder Runde wird ein anderer Rundenschlüssel verwendet. Die Rundenschlüssel k_i werden von dem Hauptschlüssel k abgeleitet.

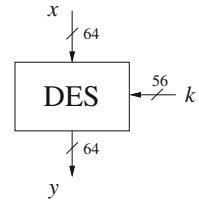

Abb. 3.3 Ein- und Ausgangsparameter der DES-Blockchiffre