1

Einladung zur Kryptokomplexität

Über dieses Buch

Dieses Buch führt in zwei Gebiete ein, *Komplexitätstheorie* und *Kryptologie*, die eng miteinander verwandt sind, sich aber recht unabhängig voneinander entwickelt haben. Neben anderen Gebieten wie etwa der Zahlentheorie verwendet die moderne Kryptologie die mathematisch strengen Konzepte und Methoden der Komplexitätstheorie. Umgekehrt ist die aktuelle Forschung in der Komplexitätstheorie oft durch Fragen und Probleme motiviert, die in der Kryptologie auftreten. Das vorliegende Buch trägt diesem Trend Rechnung, und sein Gegenstand könnte daher treffend als „*Kryptokomplexität*“ bezeichnet werden, eine Art Symbiose dieser beiden Gebiete.

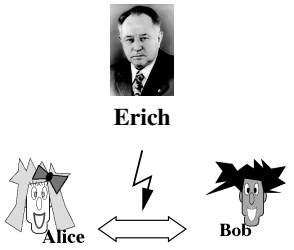

Abb. 1.1. Ein typisches kryptographisches Szenario

Abbildung 1.1 zeigt ein typisches Szenario der Kryptographie. Alice und Bob (deren Design von Crépeau entworfen wurde) möchten Nachrichten über einen unsicheren Kanal austauschen – etwa über eine öffentliche Telefonleitung oder über das Internet –, der von Erich abgehört wird. Deshalb verschlüsselt Alice ihre Nachricht an Bob so, dass Bob sie leicht entschlüsseln kann, Erich jedoch nicht. Kryptographie

ist die Kunst und Wissenschaft vom Entwurf sicherer Kryptosysteme. Alice und Bob verwenden Kryptosysteme und kryptographische Techniken, um ihre privaten Daten zu schützen und geheim zu halten, um ihre Nachrichten digital zu signieren, so dass ihre Unterschriften nicht gefälscht werden können, zum Zwecke der Authentikation, für den Schutz von Urheberrechten, zur sicheren Nutzung von Computer-Netzwerken und um in sicherer Weise über das Internet Informationen zu tauschen und Geschäfte zu machen.

Ihr Gegenspieler Erich ist ärgerlich, weil er zwar ihre Nachrichten empfangen und abhören, aber keinen Vorteil daraus schlagen kann. Sein Ziel ist die nicht authorisierte Entschlüsselung ihrer Schlüsseltexte, er möchte sich ihre Schlüssel aneignen, um ihr Kryptosystem zu knacken. Kryptoanalyse ist die Kunst und Wissenschaft des Brechens von Kryptosystemen. Kryptologie umfasst beide Gebiete, die Kryptographie und die Kryptoanalyse.

Kryptographie und Kryptoanalyse führen seit Urzeiten einen immerwährenden Krieg gegeneinander. Als unsere Vorfahren zu denken und zu sprechen und zu schreiben lernten, wollten sie ihre Gedanken und Nachrichten nicht nur übermitteln, sondern auch gegen den Zugriff unauthorisierter Empfänger schützen, d.h., sie wollten sie geheim halten. So ist verbürgt, dass bereits Julius Cäsar, Alleinherrscher von Rom und Diktator auf Lebenszeit, von einem einfachen (und leicht zu brechenden) Kryptosystem Gebrauch machte.

Schlacht um Schlacht wird seither zwischen diesen beiden widerstreitenden Welten geschlagen: Sobald die Kryptographen ein neues Kryptosystem entworfen haben, geben die Kryptoanalytiker keine Ruhe, bevor sie es nicht gebrochen haben, woraufhin bessere Kryptosysteme entwickelt werden, und so fort. Die Frontlinie verläuft dabei nicht zwischen Ländern, sie teilt nicht nur Familien, sondern sie spaltet Personen: Oft sind Kryptographen gleichzeitig Kryptoanalytiker und umgekehrt.

Die Ausdrücke „Krieg“ und „Schlacht“ sind hier durchaus wörtlich zu nehmen. Während des Zweiten Weltkriegs war der Kampf der alliierten Codebrecher gegen die berüchtigte Verschlüsselungsmaschine *Enigma* der Deutschen Wehrmacht eine Sache von Leben und Tod. Die *Enigma*, einst für unbedingt sicher gehalten, wurde schließlich von den britischen Codebrechern in Bletchley Park gebrochen, unter anderem unterstützt durch die vorherige Arbeit polnischer Mathematiker und durch die Mithilfe eines deutschen Doppelspions. Die Leistung dieser Kryptoanalytiker war entscheidend – wenn nicht für den Krieg, so doch für eine Reihe von Schlachten, besonders für die großen Seeschlachten und die Zerstörung der deutschen U-Boot-Flotte. Ausführlich erzählen Singh [Sin99] und Bauer [Bau00a, Bau00b] die aufregende Geschichte dieses Kampfes zwischen deutschen Kryptographen und alliierten Kryptoanalytikern. Der Erfolg, die *Enigma* gebrochen zu haben, wird unter anderen Alan Turing zugeschrieben. Seine Brillanz als Kryptoanalytiker wird womöglich nur durch seine genialen, fundamentalen Leistungen in der Theoretischen Informatik noch übertroffen. Indem er die nach ihm benannte Turingmaschine erfand, legte er das Fundament der Berechenbarkeitstheorie, die als die Mutter der Komplexitätstheorie gilt.

Dass effiziente Algorithmen nützliche Anwendungen in der Praxis haben, ist offensichtlich. Im Gegensatz dazu versucht man in der Komplexitätstheorie zu zeigen,

dass bestimmte Probleme nicht effizient lösbar sind. Sie stellt die Mittel und Methoden zur Verfügung, mit denen Probleme hinsichtlich der ihnen innewohnenden Komplexität klassifiziert werden können. Ebenso liefert sie nützliche Werkzeuge und Techniken, um die relative Komplexität zweier gegebener Probleme mittels Reduktionen zu vergleichen.

In kryptographischen Anwendungen jedoch bedeutet Ineffizienz Sicherheit: Die Sicherheit der heute verwendeten Kryptosysteme beruht auf der Annahme, dass bestimmte Probleme nicht effizient gelöst werden können. Das Problem, ein Kryptosystem zu brechen, kann mittels Reduktionen auf geeignete Probleme zurückgeführt werden, die allgemein als „störrisch“ gelten, also widerspenstig in dem Sinn, dass sie sich einer effizienten Lösbarkeit widersetzen. Die Kryptographie erfordert und benutzt demnach die Berechnungswiderspenstigkeit von Problemen. Kurz gesagt benötigt die Kryptographie komplexitätstheoretische Begriffe, Modelle, Methoden und Ergebnisse, und dadurch motiviert sie diese. Insbesondere sind die Begriffe der Einwegfunktion, des interaktiven Beweissystems und des Zero-Knowledge-Protokolls sowohl in der Kryptologie als auch in der Komplexitätstheorie zentral, was die gegenseitige Durchdringung dieser beiden Gebiete demonstriert. Dieses Buch behandelt die Kryptologie und die Komplexitätstheorie gleichermaßen, mit einem besonderen Augenmerk auf ihre gegenseitige Beziehung.

Wie benutzt man dieses Buch?

Dieses Lehrbuch beruht auf den Vorlesungen des Autors, die an der Heinrich-Heine-Universität Düsseldorf und an der Friedrich-Schiller-Universität Jena seit 1996 gehalten wurden. Vorwiegend für Diplom- und Masterstudierende in Informatik, Mathematik und den Ingenieurwissenschaften geschrieben, ist es ebenso eine nützliche Quelle für Forscher, Dozenten und Praktiker, die in diesen Gebieten arbeiten.

Dieses Buch kann in mehr als einer Weise in der Lehre eingesetzt werden. Einerseits ist es für Einführungsveranstaltungen in Kryptologie aus komplexitätstheoretischer Sicht geeignet. Andererseits kann es für Einführungsveranstaltungen in Komplexitätstheorie verwendet werden, die besonderen Wert auf mögliche Anwendungen in der Kryptologie legen. In beiderlei Hinsicht gibt es einen umfassenden, aktuellen, forschungsorientierten Überblick über den aktuellen Stand in diesen beiden Gebieten, wobei ihr Zusammenhang betont und ein einheitlicher Zugang gewählt wird.

Am besten jedoch ist dieses Buch für eine Folge von zusammenhängenden Kursen geeignet, die in diese beiden Gebiete gemeinsam einführen und etwa in einem Modul oder mehreren Modulen zusammengefasst sind. Beispielsweise wird das in diesem Buch enthaltene Material seit einigen Jahren vom Autor in Düsseldorf in einer Reihe von sechs einsemestrigen Vorlesungen (zu je zwei Semesterwochenstunden, ergänzt um Übungen und Seminare) präsentiert, die insgesamt in einem Zeitraum von zwei Jahren gehalten werden und wobei je zwei Vorlesungen zu einem Modul kombiniert werden können. Je eines der Kapitel 3 bis 8 macht den Inhalt einer solchen Vorlesung aus, wobei die jeweils nötigen Grundlagen aus Kapitel 2 nach Bedarf ergänzt werden. Als vorteilhaft hat es sich dabei erwiesen, dass die

einzelnen Kapitel relativ unabhängig voneinander sind, so dass die Studierenden wirklich flexibel je zwei Vorlesungen zu einem Modul ihrer Wahl zusammenstellen können. Wenn nötig, können sie sich noch fehlenden Stoff aus anderen Kapiteln bzw. Vorlesungen mit Hilfe des Buches im Selbststudium leicht aneignen. Die starke Nachfrage nach diesen Veranstaltungen und der positive Zuspruch seitens der Studierenden, sowohl im persönlichen Gespräch als auch in anonymen Befragungen, lassen den Schluss zu, dass dieser Zugang, der sich auf die gegenseitige Verflechtung von Komplexitätstheorie und Kryptologie konzentriert, für die Studierenden nutzbringender ist, als wenn beide Gebiete separat und unabhängig unterrichtet würden. Natürlich können und sollten die in diesem Buch behandelten Themen um aktuelle Forschungsergebnisse der Originalliteratur und anderes interessantes Material erweitert werden. Detaillierte Beschreibungen der Veranstaltungen in Düsseldorf findet man unter `http://ccc.cs.uni-duesseldorf.de/~rothe/vorlesungen`.

Viel Sorgfalt wurde der Motivation und Erklärung der präsentierten Begriffe und Resultate gewidmet. Zahlreiche Beispiele, Abbildungen und Tabellen sollen den Text zugänglich, verständlich, leicht lesbar und hoffentlich hin und wieder auch unterhaltsam machen. Gelegentlich wird daher ein Begriff oder Satz, bevor er abstrakt, formal und mathematisch präsentiert wird, zunächst mittels einer kleinen Geschichte (einer „*Story*“) eingeführt und anhand von mehr oder weniger alltäglichen Beispielen erläutert. Dieses Buch zu lesen, ist jedoch kein reines Vergnügen. Es ist auch harte Arbeit: Jedes Kapitel bietet dem Leser eine Reihe von Übungen und Problemen an, einige mit Hinweisen für mögliche Lösungen oder mit Verweisen auf die Originalliteratur. Der Schwierigkeitsgrad der Übungen bewegt sich in einem recht großen Bereich; es gibt ziemlich leichte Übungen und es gibt schwere. Viele der Probleme sind überaus große Herausforderungen. Einige von ihnen beschreiben erst kürzlich gelöste Forschungsfragen, die manchmal tiefe Einsichten oder clevere Ideen erfordern. Selbst wenn sich diese als zu schwierig erweisen sollten, lohnt es sich, eine eigene Lösung zu versuchen.

Dank der umfassenden Bibliographie (mit 550 Einträgen) und dem Sach- und Autorenverzeichnis (mit 1569 Hauptstichwörtern und 995 Nebeneinträgen und Querverweisen) ist dieses Buch auch für Wissenschaftler von Wert, die in der Komplexitätstheorie oder Kryptologie arbeiten. Es bahnt sich seinen Weg von den grundlegenden Anfängen bis hin zu den Fronten der aktuellen Forschung in ausgewählten Themen dieser beiden Gebiete, wobei Wert auf einen einheitlichen Zugang gelegt wird. Jedes Kapitel schließt mit einer Zusammenfassung, die die historische Entwicklung der zuvor dargelegten Begriffe und Resultate beschreibt, verwandte Begriffe und Ideen erklärt und umfassende, detaillierte bibliographische Anmerkungen macht.

Das Sach- und Autorenverzeichnis enthält eine Fülle von Stichwörtern und Querverweisen, denn ein Lehrbuch ist nur so nützlich wie sein Index. [1] Jedes Stichwort kann mehrere Einträge haben, einen fettgedruckten Haupteintrag, der auf die Defi-

[1] Angenommen, man sucht nach jedem Vorkommen des Ausdrucks *Baby-Klonen* in diesem Buch. Oder man interessiert sich für ein spezielles Werkzeug, etwa eine *Kettensäge* oder eine *Turingmaschine*. Oder man möchte alles wissen, was dieses Buch über *Polygamie*, den

nition des entsprechenden Begriffs verweist, und eine Anzahl weiterer Einträge, die auf Sätze verweisen, in denen dieser Begriff vorkommt. Ein Lehrbuch ohne Index, oder mit einem dürftigen oder schlampig erstellten Index, ist dem Leser kaum eine größere Hilfe als eine Bibliothek ohne Katalog, in der alle Bücher unsortiert auf einen Haufen geworfen wurden. Man steht dann vielleicht vor diesem gewaltigen Bücherberg und weiß, dass man alles Wissen und alle Weisheit des Universums darin finden könnte, und doch findet man die ganz spezielle Information nicht, die man so verzweifelt sucht. Diese Erkenntnis wurde eloquent von Borges [Bor89] in seiner Kurzgeschichte „Die Bibliothek von Babel“ geschildert. Übrigens findet man wirklich jedes in Fußnote 1 erwähnte Stichwort im Sach- und Autorenverzeichnis. Sehen Sie mal nach.

Zugegeben, dieses Buch fokussiert scharf auf Theorie. Praktische Aspekte des *Security Engineering*, wozu etwa der Entwurf sicherer Public-Key-Infrastrukturen gehört, findet man hier nicht. Empfehlenswerte Referenzen für dieses Thema sind z.B. Buchmann [Buc01b] und Schneier [Sch96].

Während der Arbeit an der englischen Originalversion dieses Buches, 2003 und 2004, entwickelte eine Gruppe Düsseldorfer Studierender ein System, das eine Reihe von Kryptosystemen implementiert, welche auch hier behandelt werden. Danken möchte ich an dieser Stelle besonders Tobias Riege, der dieses Praktikum leitete, und auch Yves Jerschow, Claudia Lindner, Tim Schlüter, David Schneider, Andreas Stelzer, Philipp Stöcker, Alexander Tchernin, Pavel Tenenbaum, Oleg Umanski, Oliver Wollermann und Isabel Wolters. Den Quellcode in Java erhält man von `http://ccc.cs.uni-duesseldorf.de/~riege/praktikum`.

Überblick über die Buchkapitel

Kapitel 2 führt knapp in die Gebiete der Informatik und Mathematik ein, die für die in diesem Buch behandelten Themen der Komplexitätstheorie und Kryptologie relevant sind. Die verwendeten Begriffe werden so einfach wie möglich erklärt, aber auch mit der nötigen mathematischen Strenge. Insbesondere werden elementare Grundlagen der Algorithmik, der Theorie der formalen Sprachen, der Berechenbarkeitstheorie, der Logik, Algebra, Zahlentheorie, Graphentheorie und Wahrscheinlichkeitstheorie bereitgestellt. Obwohl jedes dieser Gebiete von Grund auf eingeführt und nicht viel an mathematischen Vorkenntnissen vom Leser verlangt wird, kann es hilfreich sein, wenn man mit den Grundlagen der Mathematik und Informatik bereits ein wenig vertraut ist.

In den Kapiteln 3 und 4 werden die Grundlagen der Komplexitätstheorie und Kryptologie gelegt, und ihre historische Entwicklung wird kurz skizziert. In Kapitel 3 werden die Komplexitätsmaße Zeit und Raum und die entsprechenden Komplexitätsklassen im traditionellen Worst-Case-Modell definiert. (Das Average-Case-Komplexitätsmodell wird hier nicht behandelt; für dieses Modell enthalten z.B. die

Zauberer *Merlin*, den *Einen Ring*, den *Heiligen Gral* oder *DNA-Tests* zu sagen hat. Oder man möchte alles über seine *Dogmen* erfahren.

exzellenten Arbeiten von Goldreich [Gol97a] und Wang [Wan97] viele nützliche Referenzen.) Grundlegende Eigenschaften der Worst-Case-Komplexität werden studiert, einschließlich der linearen Raumkompression und Beschleunigung sowie der Hierarchiesätze für Zeit und Raum. Die Beziehungen der wichtigsten Komplexitätsklassen zwischen logarithmischem und polynomialem Raum werden erkundet. Am namhaftesten unter diesen sind die Klassen P und NP, deterministische und nichtdeterministische polynomiale Zeit.

P kann man sich als eine Komplexitätsklasse vorstellen, die den intuitiven Begriff der effizienten Berechnung einfängt, wohingegen die härtesten Probleme in NP, die NP-vollständigen Probleme nämlich, als widerspenstig gelten, falls $P \neq NP$. Die P-versus-NP-Frage besteht darin, ob diese beiden Klassen verschieden sind oder nicht. Sie ist eine der wichtigsten offenen Fragen in der theoretischen Informatik, und sie hat die Komplexitätstheoretiker seit inzwischen mehr als dreißig Jahren geärgert. Falls $P \neq NP$ gilt, dann kann kein NP-vollständiges Problem effiziente (d.h. polynomialzeit-berechenbare) Algorithmen haben. Gilt jedoch $P = NP$, dann sind alle NP-Probleme in Polynomialzeit lösbar, und insbesondere können dann die meisten der derzeit verwendeten Kryptosysteme gebrochen werden.

Besondere Aufmerksamkeit wird in Kapitel 3 den komplexitätsbeschränkten Reduzierbarkeiten gewidmet, wie etwa der polynomialzeit-beschränkten Many-one-Reduzierbarkeit, und den darauf beruhenden Begriffen der Härte und Vollständigkeit. Reduzierbarkeiten sind mächtige, nützliche Werkzeuge für den Vergleich der Komplexität zweier gegebener Probleme, und Vollständigkeit erfasst die härtesten Probleme einer gegebenen Komplexitätsklasse bezüglich einer gegebenen Reduzierbarkeit. Insbesondere werden die vollständigen Probleme in den Klassen NL (nichtdeterministischer logarithmischer Raum) und NP intensiv untersucht, und sehr viele spezifische Beispiele natürlicher vollständiger Probleme in diesen Klassen werden angegeben. Dazu gehören auch verschiedene Varianten des Erfüllbarkeitsproblems, welches fragt, ob eine gegebene boolesche Formel erfüllbar ist. Die Liste der Probleme, deren NP-Vollständigkeit in diesem Kapitel gezeigt wird, enthält mehrere Graphenprobleme, wie etwa das Dreifärbbarkeitsproblem für Graphen, und auch bestimmte Varianten des Rucksack-Problems. In Kapitel 8 wird später ein Kryptosystem vorgestellt, das auf solch einem Rucksack-Problem beruht.

Es gibt Probleme in NP, die vermutlich weder NP-vollständig sind noch effiziente Algorithmen haben. Ein solches Beispiel ist das Graphisomorphie-Problem, das in Kapitel 2 eingeführt und in den Kapiteln 3, 6 und 8 tiefgründiger untersucht wird. Ein weiteres Beispiel eines Problems, das in nichtdeterministischer Polynomialzeit gelöst werden kann, von dem man aber nicht weiß, ob es in deterministischer Polynomialzeit lösbar ist, ist das Faktorisierungsproblem, das in Kapitel 7 gründlich untersucht wird. Die Sicherheit vieler Kryptosysteme, einschließlich des berühmten RSA-Systems, beruht auf der vermuteten Härte des Faktorisierungsproblems.

Kapitel 3 führt auch eine interessante Komplexitätsklasse ein, der vollständige Probleme vermutlich fehlen: UP, „Unambiguous Polynomial Time“, enthält genau die NP-Probleme, deren Instanzen nie mehr als eine Lösung haben. Die Komplexitätsklasse UP ist unter anderem nützlich für die Charakterisierung der Existenz bestimmter Typen von Einwegfunktionen im Worst-Case-Modell. Eine Funktion ist

eine Einwegfunktion, falls sie „leicht“ zu berechnen, aber „schwer“ zu invertieren ist. In der Komplexitätstheorie stehen solche Funktionen in einem engen Zusammenhang zur Isomorphie-Vermutung von Berman und Hartmanis. Einwegfunktionen (in einem adäquaten Komplexitätsmodell) sind auch in der Kryptographie wichtig; solche Funktionen werden in Kapitel 8 diskutiert.

Kapitel 4 führt die Grundbegriffe der Kryptologie ein, wie etwa symmetrische (alias *private-key*) und asymmetrische (alias *public-key*) Kryptosysteme. Dieses Kapitel stellt einige klassische symmetrische Kryptosysteme vor, einschließlich der Substitutions-, der affinen und der Permutationschiffre, der affin linearen Blockchiffren, der Stromchiffren, der Vigenère- und der Hill-Chiffre. Kryptoanalytische Angriffe auf diese Kryptosysteme werden anhand von Beispielen präsentiert. Außerdem wird der Begriff der perfekten Geheimhaltung für Kryptosysteme eingeführt, der auf dem Entropiebegriff im Sinne der Informations- und Codierungstheorie von Shannon [Sha49] beruht. Schließlich wird Shannons Resultat vorgestellt, das notwendige und hinreichende Bedingungen dafür angibt, dass ein Kryptosystem perfekte Geheimhaltung erreicht.

Kapitel 5 wendet sich wieder der Komplexitätstheorie zu und führt Hierarchien ein, die auf NP beruhen, einschließlich der booleschen Hierarchie über NP und der Polynomialzeit-Hierarchie. Im Zusammenhang damit werden verschiedene polynomialzeit-beschränkte Turing-Reduzierbarkeiten definiert. Diese Hierarchien enthalten beide NP als ihre erste Stufe und sind sehr nützlich für die Klassifizierung von Problemen, die vermutlich härter als NP-vollständige Probleme sind. Zu den Beispielen für Probleme, die in den höheren Stufen der booleschen Hierarchie vollständig sind, zählen „exakte“ Varianten von NP-vollständigen Optimierungsproblemen, Facettenprobleme und kritische Graphenprobleme. Zu den Beispielen für Probleme, die in den höheren Stufen der Polynomialzeit-Hierarchie vollständig sind, gehören bestimmte Varianten von NP-vollständigen Problemen, die durch eine beschränkte Anzahl von alternierenden längenbeschränkten Quantoren dargestellt werden können. Beispielsweise gehören dazu solche Probleme, die das Erfüllbarkeitsproblem verallgemeinern, indem sie nach dem Wahrheitsgehalt von quantifizierten booleschen Formeln mit einer beschränkten Anzahl von alternierenden existenziellen und universellen Quantoren fragen.

Im Zusammenhang damit wird in Kapitel 5 der Begriff der alternierenden Turingmaschine eingeführt, und die Klassen P und PSPACE werden bezüglich solcher Maschinen charakterisiert: Deterministische Polynomialzeit ist gleich alternierendem logarithmischem Raum, und deterministischer polynomialer Raum ist gleich alternierender Polynomialzeit. Das erstgenannte Resultat zeigt, dass alternierende Turingmaschinen ein vernünftiges Modell der Parallelberechnung sind, denn sie erfüllen das Kriterium von Cook, nach welchem parallele Zeit (in etwa) dasselbe ist wie sequenzieller (d.h. deterministischer) Raum. Aus dem letztgenannten Resultat folgt insbesondere, dass das Problem der quantifizierten booleschen Formeln mit unbeschränkter Anzahl von alternierenden längenbeschränkten Quantoren vollständig für PSPACE ist.

Es gibt einen bemerkenswerten Zusammenhang zwischen der Polynomialzeit-Hierarchie und der booleschen Hierarchie über NP: Wenn die boolesche Hierarchie

auf eine endliche Stufe kollabiert, so kollabiert auch die Polynomialzeit-Hierarchie. Weiter führt Kapitel 5 die Frage-Hierarchien über NP mit einer beschränkten Anzahl von Fragen sowie die Low- und die High-Hierarchie in NP ein. Die Low-Hierarchie kann als ein Maßstab verwendet werden, um die Komplexität solcher NP-Probleme zu messen, die vermutlich weder in P liegen noch NP-vollständig sind.

Kapitel 6 befasst sich mit randomisierten Algorithmen und probabilistischen Komplexitätsklassen. Insbesondere wird ein randomisierter Algorithmus für das NP-vollständige Erfüllbarkeitsproblem vorgestellt und analysiert, der zwar immer noch nur in Exponentialzeit läuft, aber schneller als der naive deterministische Algorithmus für dieses Problem ist. Außerdem werden Monte-Carlo- und Las-Vegas-Algorithmen und die probabilistischen Komplexitätsklassen PP („Probabilistic Polynomial Time"), RP („Random Polynomial Time"), ZPP („Zero-error Probabilistic Polynomial Time") und BPP („Bounded-error Probabilistic Polynomial Time") in Kapitel 6 eingeführt und gründlich untersucht. Indem man den Fehler eines solchen randomisierten Algorithmus „von ein halb weg beschränkt", ist es möglich, eine sehr nützliche Technik zur Wahrscheinlichkeitsverstärkung anzuwenden, mittels derer man eine Fehlerwahrscheinlichkeit der Berechnung erreichen kann, die exponentiell klein in der Eingabegröße ist. Eine so kleine Fehlerwahrscheinlichkeit kann in den meisten praktischen Anwendungen (nahezu) unbeschadet vernachlässigt werden, besonders wenn man bedenkt, dass schon die Wahrscheinlichkeit eines Hardware-Fehlers größer sein kann. Wieder haben einige probabilistische Komplexitätsklassen (z.B. PP) vollständige Probleme, wohingegen andere (z.B. BPP) höchstwahrscheinlich keine vollständigen Probleme besitzen.

In Kapitel 6 werden außerdem die von Babai und Moran eingeführten Arthur-Merlin-Spiele studiert, welche man als „interaktive Beweissysteme mit öffentlichen Münzwürfen" auffassen kann. Auch sie definieren eine Hierarchie von Komplexitätsklassen mittels alternierender längenbeschränkter Quantoren. Die Hauptergebnisse über die Arthur-Merlin-Hierarchie in Kapitel 6 sind erstens, dass diese Hierarchie auf eine endliche (nämlich die zweite) Stufe kollabiert, und zweitens, dass das Graphisomorphie-Problem in der zweiten Stufe dieser Hierarchie enthalten ist. Daraus folgt, dass das Graphisomorphie-Problem auch in der zweiten Stufe der Low-Hierarchie liegt und somit vermutlich nicht NP-vollständig ist.

Kapitel 7 stellt das RSA-Kryptosystem vor, das erste im öffentlichen Bereich entwickelte Public-Key-Kryptosystem, das auch heute noch in der Praxis weitverbreitet und in Gebrauch ist. Das RSA-Schema für digitale Signaturen, welches auf dem RSA-Kryptosystem beruht, wird ebenfalls präsentiert. Ein Protokoll für digitale Signaturen ermöglicht es Alice, ihre Nachrichten an Bob so zu unterschreiben, dass Bob verifizieren kann, dass tatsächlich sie die Senderin war, und ohne dass Erich Alice' Signatur fälschen kann. Des Weiteren werden zahlreiche kryptoanalytische Angriffe auf das RSA-System inspiziert und gründlich diskutiert, und für jeden solchen Angriff auf RSA werden mögliche und zweckmäßige Gegenmaßnahmen vorgeschlagen.

Im Zusammenhang mit dem RSA-System werden in Kapitel 7 das Faktorisierungsproblem und das Primzahl-Problem intensiv untersucht. Einerseits hängt die Sicherheit von RSA wesentlich von der vermuteten Härte des Faktorisierens großer

ganzer Zahlen ab. Andererseits erfordern sowohl das RSA-Kryptosystem als auch das RSA-Schema für digitale Signaturen, wie auch viele andere Kryptosysteme und Protokolle, die effiziente Erzeugung großer Primzahlen. Die Komplexität der prominentesten Faktorisierungsmethoden, zu denen z.B. das quadratische Sieb gehört, wird in Kapitel 7 diskutiert. Anzumerken ist, dass es für das Faktorisierungsproblem derzeit weder einen effizienten Algorithmus noch einen mathematisch strengen Beweis seiner Härte gibt.

Außerdem werden in Kapitel 7 eine Reihe von effizienten, in der Praxis verwendeten Primzahltests vorgestellt, einschließlich des Fermat-Tests, des Miller–Rabin-Tests und des Solovay–Strassen-Tests. Bei diesen handelt es sich um randomisierte Algorithmen, und einige von ihnen sind vom Monte-Carlo-Typ. Ein kürzlich erzieltes Resultat, nach dem das Primzahlproblem sogar in deterministischer Polynomialzeit gelöst werden kann, wird ebenfalls diskutiert.

Kapitel 8 inspiziert weitere wichtige Public-Key-Kryptosysteme und kryptographische Protokolle, einschließlich des Diffie–Hellman-Protokolls für den Tausch geheimer Schlüssel und des ElGamal-Protokolls für digitale Signaturen. Das letztere Protokoll ist, mit geeigneten Modifizierungen, als der Digital Signature Standard der Vereinigten Staaten übernommen worden. Im Zusammenhang mit diesen Protokollen wird auch das Problem des diskreten Logarithmus in diesem Kapitel sorgfältig studiert. Die Sicherheit vieler wichtiger Protokolle, wie z.B. der beiden eben erwähnten, beruht auf der vermuteten Härte dieses Problems.

Indem wir uns dann dem in den vorherigen Kapiteln studierten Graphisomorphie-Problem und dem Begriff der Arthur-Merlin-Spiele wieder zuwenden, wird in Kapitel 8 der Begriff des Zero-Knowledge-Protokolls eingeführt, der für die kryptographische Aufgabe der Authentikation wichtig ist.

Es hat in der Vergangenheit Versuche gegeben, Kryptosysteme zu entwerfen, deren Sicherheit auf NP-harten Problemen beruht, insbesondere auf Varianten des Rucksack-Problems. Einige dieser Kryptosysteme wurden gebrochen, wohingegen andere noch immer intakt sind (also nach wie vor als sicher gelten). Ein solches Kryptosystem wird in Kapitel 8 vorgestellt und kritisch diskutiert. Im Zusammenhang damit wird der Begriff der Falltür-Einwegfunktion (*trapdoor one-way function*) diskutiert, der in der Public-Key-Kryptographie sehr wichtig ist. Schließlich werden in diesem Kapitel Protokolle für den Tausch geheimer Schlüssel und für digitale Signaturen vorgestellt, die auf assoziativen, stark nichtinvertierbaren Einwegfunktionen (im Worst-Case-Modell) beruhen.

Selbstverständlich gibt es noch viele weitere interessante Themen und Resultate in der Komplexitätstheorie und Kryptologie, auf die in diesem Buch zwar nicht eingegangen werden kann, für die aber ein paar empfehlenswerte Referenzen gegeben werden. Beispielsweise wird das Thema der Approximation und der Nichtapproximierbarkeit, welches sowohl von theoretischer als auch von praktischer Bedeutung ist, hier nicht angesprochen; siehe z.B. Ausiello et al. [ACG+03], Vazirani [Vaz03] und das umfassende, stets aktuell gehaltene Kompendium von NP-Optimierungsproblemen, herausgegeben von Crescenzi, Kann, Halldórsson, Karpinski und Woeginger: `http://www.nada.kth.se/~viggo/problemlist`.

Für eine Vielzahl weiterer wichtiger Themen der Komplexitätstheorie sei auf die folgenden Bücher verwiesen: Balcázar, Díaz und Gabarró [BDG95, BDG90], Bovet und Crescenzi [BC93], Du und Ko [DK00], Garey und Johnson [GJ79], L. Hemaspaandra und Ogihara [HO02], Papadimitriou [Pap95], Reischuk [Rei90], Vollmer [Vol99], Wagner und Wechsung [WW86, Wec00] und Wegener [Weg87, Weg03], sowie auf die Sammelwerke, die herausgegeben wurden von Selman und L. Hemaspaandra [Sel90, HS97] und von Ambos-Spies, Homer und Schöning [AHS93].

Das Rechnen mit so genannten Quantencomputern wird hier nicht behandelt; Berthiaume [Ber97] führt in dieses faszinierende neue Gebiet ein, das über die Grenzen der klassischen Berechenbarkeits- und Komplexitätstheorie hinausgeht und auf den quantenmechanischen Prinzipien der Physik gründet. Einen verständlichen Einstieg in das verwandte Gebiet der Quantenkryptographie, welches sich gleichermaßen von der hier präsentierten klassischen Kryptographie beträchtlich unterscheidet, geben z.B. Bruß, Erdélyi, T. Meyer, Riege und Rothe [BEM+07] sowie Gisin, Ribordy, Tittel und Zbinden [GRTZ02]. Für andere Themen der Kryptologie, die hier nicht behandelt werden, sei beispielsweise verwiesen auf Goldreich [Gol99, Gol01], Luby [Lub96], Micciancio und Goldwasser [MG02], Salomaa [Sal96], Schneier [Sch96], Stinson [Sti05] und Welsh [Wel98].

http://www.springer.com/978-3-540-79744-9

Komplexitätstheorie und Kryptologie
Eine Einführung in Kryptokomplexität
Rothe, J.
2008, XI, 535 S., Hardcover
ISBN: 978-3-540-79744-9