Literatur zur Kryptologie

(Als Beigleitmaterial zur Vorlesung kommen vor allem die unter 1.) genannten Bücher in Frage; der Rest ist eher zur Ergänzung und zur Vertiefung spezieller Themen gedacht.)

1. Allgemeine Bücher mit ähnlicher Themenauswahl wie die Vorlesung

JOHANNES BUCHMANN: Einführung in die Kryptographie, *Springer Lehrbuch,* ^{3}2004 *(Vorstellung der wichtigsten Verfahren einschließlich ihrer mathematischer Grundlagen; in deutscher Sprache die wohl beste solche Zusammenstellung.)*

JAN C.A. VAN DER LUBBE: Basic methods of cryptography, *Cambridge University Press,* 1998 *(Übersetzung eines 1994 auf Niederländisch erschienenen Buchs; trotz des Fehlens neuerer Verfahren immer noch interessant zu lesen.)*

WENBO MAO: Modern cryptography, *Prentice Hall,* 2004 *(Sehr ausführliche Zusammenstellung, behandelt sowohl die mathematischen Grundlagen als auch praktische Probleme)*

NIGEL SMART: Cryptography: An Introduction, *McGraw-Hill,* 2003 *(Mathematisch sehr fundierte Darstellung des Gesamtgebiets. Auch mathematisch kompliziertere Attacken auf RSA und Fragen der praktischen Anwendung von Kryptographie werden ausfürlich diskutiert, ebnso eine ganze Reihe von Sicherheitsmodellen.)*

DOUGLAS R. STINSON: Cryptography, Theory and Practice, *Chapman & Hall/CRC,* ^{3}2005 *(Klassisches Lehrbuch mit Schwerpunkt auf der Darstellung der Verfahren. Mathematische Grundlagen sowie Vorsichtsmaßnahmen bei der praktischen Anwendung spielen nur eine untergeordnete Rolle. Man beachte, daß die drei bisherigen Auflagen des Buchs recht verschiedene Inhalte haben.)*

DIETMAR WÄTJEN: Kryptographie – Grundlagen, Algorithmen, Protokolle, *Spektrum Akademischer Verlag,* 2004 *(Weniger ausführlich und weniger fundiert als Buchmann, aber doch eine gute Übersicht.)*

2. Weitere Darstellungen des Gesamtgebiets

AIDEN A. BRUEN, MARIO A. FORCINITO: Cryptography, Information Theory and Error-Correction. A Handbook for the 21st century, *Wiley,* 2005 *(sehr knapp gehaltener Überblick; das 21. Jahrhundert braucht mehr.)*

ALFRED J. MENEZES, PAUL C. VAN OORSCHT, SCOTT A. VANSTONE: Handbook of Applied Cryptography, *CRC Press,* 1997 *(dickes Handbuch, leider ohne Kryptosysteme mit elliptischen Kurven.)*

RICHARD A. MOLLIN: An Introduction to Cryptography, *Chapman & Hall/CRC,* 2001 *(Ziemlich elementar geschriebenes Lehrbuch mit Schwerpunkt auf asymmetrischen Verfahren. Ausführliche Darstellung der mathematischen Grundlagen.)*

MARK STAMP, RICHARD M. LOW: Applied Cryptanalysis – Breaking Ciphers in the Real Word, *Wiley,* 2007 *(Der Schwerpunkt liegt auf der Kryptanalyse symmetrischer Verfahren.)*

WADE TRAPPE, LAWRENCE C. WASHINGTON: Introduction to Cryptography with coding theory, Prentice Hall, ^{2}2005 *(Guter allgemeiner Überblick; bei spezielleren oder komplizierteren Problemen aber oft nur Verweis auf weitere Literatur)*

3. Bücher mit Schwerpunkt auf klassischer Kryptographie

HELEN FOUCHÉ GAINES: Cryptanalysis – a study of ciphers and their solution, *American Photographic Publishing,* 1939; Nachdruck by *Dover,* 1956 *(Ausführliche Behandlung klassischer Codes und ihrer Kryptanalyse)*

CIPHER A. DEVOURS, LOUIS KRUH: Machine Cryptography and Modern Cryptanalysis, *Artech House,* 1985 *(Behandelt nur Rotormaschinen und deren Kryptanalyse)*

DAVID KAHN: The Codebreakers, *Scribner,* ^{2}1996 *(In erster Linie historisch, aber viele Kryptologen haben aus der Erstauflage von 1967 die Grundlagen ihres Handwerks gelernt. Die Neuauflage unterscheidet sich von dieser nur durch ein neues Vorwort und einen kurzen Anhang über asymmetrische Kryptographie.)*

ALAN G. KOHNHEIM: Cryptography: A primer, *Wiley,* 1981 *(Ein Klassiker mit fundierter mathematischer Behandlung der wichtigsten klassischen Verfahren sowie auch des DES. Statistische Methoden der Kryptanalyse werden ausführlich dargestellt; ein kurzes Kapitel beschäftigt sich mit asymmetrischer Kryptographie.)*

4. Bücher mit Schwerpunkt auf asymmetrischen Verfahren

RICHARD CRANDALL, CARL POMERANCE: Prime numbers – A Computational Perspective, *Springer,* 2001 *(Ausführliche und mathematisch fundierte Behandlung der zahlentheoretischen Algorithmen, die (nicht nur) asymmetrischen Kryptoverfahren und den Angriffen darauf zugrunde liegen.)*

SAMUEL S. WAGSTAFF: Cryptanalysis of Number Theoretic Ciphers, *Chapman & Hall/CRC,* 2003 *(Als Lehrbuch der Kryptologie konzipiert mit deutlichem Schwerpunkt auf asymmetrischen Verfahren. Mathematisch nicht so weit gehend wie Crandell/Pomerance.)*

5. Spezialliteratur zu DES und AES

ELI BIHAM, ADI SHAMIR: Differential Cryptanalysis of the Data Encryption Standard, *Springer,* 1993 *(Differentielle Kryptanalyse ist ein in der offenen Literatur erstmals von den Autoren vorgestellten Angriffsverfahrens, das sich gegen jede Art von modernen symmetrischen Kryptoverfahren einsetzen läßt und gegen das diese resistent sein müssen. Im Buch wird die Anwendung auf DES detailiert untersucht.)*

ELECTRONIC FRONTIER FOUNDATION: Cracking DES, *O'Reilly,* 1998 *(Beschreibung einer Maschine, die mit Hilfe speziell entwickelter ASICs durch systematisches Probieren DES-Schlüssel in wenigen Stunden finden kann.)*

JOAN DAEMEN, VINCENT RIJMEN: The design of Rijndael. AES – The Advanced Encryption Standard, *Springer,* 2002 *(Beschreibung des DES-Nachfolgers AES und seiner Design-Prinzipien durch die beiden Entwickler des Algorithmus)*

CARLOS CID, SEAN MURPHY, MATHEW ROBSCHAW: Algebraic Aspects of the Advanced Encryption Standard, *Springer,* 2006 *(Neben der Beschreibung von AES behandelt dieses Buch vor allem eine Übersetzung seiner Kryptanalyse in die Lösung eines nichtlinearen Gleichungssystems.)*

6. Literatur über Quantenkryptographie und Quantencomputer

DAGMAR BRUSS: Quanteninformation, *Fischer,* 2003 *(gut lesbares Taschenbuch, das fast alles im Rahmen dieser Vorlesung wichtige enthält)*

MIKA HIRVENSALO: Quantum Computing, *Springer,* 2001 *(Darstellung der Unterschiede zwischen dem Rechnen mit klassischen und mit Quantencomputern, ausführliche Darstellung der Faktorisierung sowie der ungeordneten Suche mit Quantencomputern, kurzer Abriß der Quantenmechanik.)*

YORICK HARDY, WILLI-HANS STEEB: Classical and Quantum Computing – with C++ and Java Simulations, *Birkhäuser,* 2001 *(Hier geht es vor allem darum, einen Quantencomputer auf einem klassischen Computer zu simulieren – was natürlich nur mit erheblichen Geschwindigkeitsverlusten möglich ist. Insbesondere werden auch für die Kryptographie wichtige Algorithmen implementiert und simuliert.)*

PHILLIP KAYE, RAYMOND LAFLAMME, MICHELE MOSCA: An introduction to quantum computing, *Oxford University Press,* 2007 *(Behandelt Grundsätzliches über die unterschiedlichen Logikelemente für klassische und Quantencomputer sowie die die wichtigsten bekannten Algorithmen, bei denen Quantencomputer deutlich schneller sind als klassische, außerdem gibt es Kapitel über fehlerkorrigierende Quantencodes und Teleportation.)*

A.YU. KITAEV, A.H. SHEN, M.N. VYALYI: Classical and Quantum Computation, *American Mathematical Society,* 2002 *(Ausführliche Darstellung des grundlegenden Aufbaus von Quantencomputern und der Komplexität von Quantenalgorithmen.)*

SUSAN LOEPP, WILLIAM K. WOOTTERS: Protecting Information. From Classical Error Correction to Quantum Cryptography, *Cambridge University Press,* 2006 *(Enthält auch eine kurze Darstellung klassischer und aktuell gängiger Verfahren, beschäftigt sich aber hauptsächlich mit Quantenkryptographie und fehlerkorrigierenden Quantencodes.)*

ARTHUR O. PITTENGER: An Introduction to Quantum Computing Algorithms, *Birkhäuser,* 2000 *(Kurze Beschreibung der prinzipiellen Funktion von Quantencomputern, Darstellung der wichtigsten Algorithmen sowie des Einsatzes von fehlerkorrigierenden Codes zur Stabilisierung des Rechengangs von Quantencomputern.)*

7. Bücher über Kryptosysteme mit elliptischen Kurven

IAN BLAKE, GADIEL SEROUSSI, NIGEL SMART: Elliptic Curves in Cryptography, *Cambridge University Press,* 1999 *(Setzt Grundkenntnisse der Kryptographie voraus und verweist auch für viele Resultate über elliptische Kurven auf die Literatur. Hauptziel ist die Beschreibung von Algorithmen sowohl zur Verschlüsselung mit elliptischen Kurven als auch zum Angriff auf solche Kryptoverfahren.)*

IAN BLAKE, GADIEL SEROUSSI, NIGEL SMART [HRSG.]: Advances in Elliptic Curves Cryptography, *Cambridge University Press,* 2005 *(Fortsetzung des obigen Buchs mit einer Reihe von seit dessen Erscheinen aktuell gewordenen Einzelthemen.)*

HENRI COHEN, GERHARD FREY mit ROBERTO AVANZI, CRISTOPHE DOCHE, TANJA LANGE, KIM NGUYEN, FREDERIK VERCAUTEREN: Handbook of Elliptic and Hyperelliptic Curve Cryptography, *Chapman & Hall/CRC,* 2006 *(Sehr ausführliche Darstellung aller gängiger Verfahren und Attacken)*

ANDREAS ENGE: Hyperelliptic Cryptosystems – Efficency and Subexponential Attacks, *Books on Demand,* 2000 *(Untersuchung der Sicherheit und Effizienz von Kryptoverfahren auf der Basis hyperelliptischer Kurven, insbesondere in Abhängigkeit vom Geschlecht der Kurve.)*

DARREL HANKERSON, ALFRED MENEZES, SCOTT VANSTONE: Guide to Elliptic Curve Cryptography, *Springer,* 2004 *(Darstellung der Kryptographie mit elliptischen Kurven vor allem unter dem Gesichtspunkt des praktischen Einsatzes. Auf Kryptanalyse wird nicht eingegangen.)*

MICHAEL ROSING: Implementing Elliptic Curve Cryptography, *Manning,* 1999 *(Konkrete Implementierung in C)*

8. Bücher mit Schwerpunkt auf dem Umgang mit Kryptographie

STEVE BURNETT, STEPHEN PAINE: Kryptographie – RSA Security's Official Guide, *mitp-Verlag,* 2001 *(Hier geht es vor allem um das Umfeld für den sicheren Einsatz von Kryptoverfahren sowie um eine Darstellungen der wichtigsten dazu entwickelten Protokolle.)*

NIELS FERGUSON, BRUCE SCHNEIER: Practical Cryptography, *Wiley,* 2003 *(Diskutiert Kriterien für die praktische Auswahl von Kryptoverfahren, die Wahl sicherer Schlüssel und den Aufbau einer Infrastruktur für kryptographische Kommunikation.)*

ERIC RESCORLA: SSL and TLS – Designing and Building Secure Systems, *Addison Wesley,* 2001 *(Beschreibung der Protokolle für sichere Internetverbindungen)*

MICHAEL WELSCHENBACH: Kryptographie in C und C++, *Springer,* 1998 *(Implementierung einer Langzahlarithmetik sowie der für die Kryptologie wichtigsten zahlentheoretischen Algorithmen)*