Stephan Spitz | Michael Pramateftakis | Joachim Swoboda

Kryptographie und IT-Sicherheit

Stephan Spitz | Michael Pramateftakis | Joachim Swoboda

Kryptographie und IT-Sicherheit

Grundlagen und Anwendungen

2., überarbeitete Auflage

Mit 115 Abbildungen

STUDIUM

VIEWEG+
TEUBNER

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der
Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über
<<http://dnb.d-nb.de>> abrufbar.

Das in diesem Werk enthaltene Programm-Material ist mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Der Autor übernimmt infolgedessen keine Verantwortung und wird keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieses Programm-Materials oder Teilen davon entsteht.

Höchste inhaltliche und technische Qualität unserer Produkte ist unser Ziel. Bei der Produktion und Auslieferung unserer Bücher wollen wir die Umwelt schonen: Dieses Buch ist auf säurefreiem und chlorfrei gebleichtem Papier gedruckt. Die Einschweißfolie besteht aus Polyäthylen und damit aus organischen Grundstoffen, die weder bei der Herstellung noch bei der Verbrennung Schadstoffe freisetzen.

1. Auflage 2008
2., überarbeitete Auflage 2011

Alle Rechte vorbehalten
© Vieweg+Teubner Verlag | Springer Fachmedien Wiesbaden GmbH 2011

Lektorat: Christel Roß | Maren Mithöfer

Vieweg+Teubner Verlag ist eine Marke von Springer Fachmedien.
Springer Fachmedien ist Teil der Fachverlagsgruppe Springer Science+Business Media.
www.viewegteubner.de

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Umschlaggestaltung: KünkelLopka Medienentwicklung, Heidelberg
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.
Printed in Germany

ISBN 978-3-8348-1487-6

Nachruf

Diese Zeilen sind im Gedenken an Herrn Professor Swoboda, der an der TU München sowohl die Lehre als auch die Forschung auf dem Gebiet der Informationssicherheit begründete. Er bleibt uns als freundlicher und offener Kollege, sowie geschätzter und respektierter Wissenschaftler in Erinnerung, der bis kurz vor seinem Tod für die Anliegen der Studierenden und Mitarbeiter offen war.

Er starb leider viel zu früh kurz vor Veröffentlichung dieses Buchs. Seine Art komplexe Zusammenhänge einfach zu vermitteln hat unser Denken und auch dieses Buch geprägt. Durch seine engagierte Arbeit an der TU München beeinflusste er viele Generationen von Ingenieuren und trug dazu bei, dass IT-Sicherheit und Kryptographie wichtiger Bestandteile an der Universität und im industriellen Umfeld wurden.

München und Athen im Sommer 2010

Die Mitarbeiter des Lehrstuhls für Datenverarbeitung an der TU München
und Co-Autoren dieses Buchs

Vorwort

Dieses Buch entstand auf der Basis von Vorlesungen über Kryptographie und angewandte IT-Sicherheit, die seit Jahren in der Elektrotechnik und Informationstechnik (EI) der Technischen Universität München (TUM) gehalten werden, aber ebenso auf der Basis von industrieller Erfahrung auf diesem Gebiet. Wir wünschen Ihnen, verehrte Leserinnen und Leser dieses Buches, Gewinn und auch Freude.

Am Anfang des Vorhabens fragten wir uns: Wozu noch ein Buch über Kryptographie schreiben, wenn man fast alle Informationen dazu schon im Internet oder anderen Büchern findet? Wo können wir Studenten und Lesern dieses Buchs mehr bieten als Wikipedia oder existierende Literatur? Man findet zwar im Netz viele und gute Einzeldarstellungen. Ein Buch hat jedoch die Chance einer einheitlichen und ausgewogenen Darstellung. Es behandelt sowohl die Sicherheits-Technologien als auch die technischen und mathematischen Grundlagen.

Dieses Buch wurde von Ingenieuren für Ingenieure und Informatiker geschrieben. Die moderne Kryptographie benötigt diskrete Mathematik für endliche Zahlenmengen (Modulo-Arithmetik). Sie wird hier jedoch nur als Hilfsmittel in einer pragmatischen Weise benutzt, so dass man die Verfahren der Kryptographie und die darauf aufbauenden Sicherheits-Technologien verstehen kann. Beweise stehen im Hintergrund. Im Vordergrund steht das Verständnis für die Leistung kryptographischer Verfahren und deren Anwendung in der Informationstechnologie.

Kryptographie, die Verschlüsselung von Information, war lange Zeit eine Sache der Geheimdienste. Mit der Verbreitung des Internet wurde die Nutzung von Kryptographie eine Sache von jedermann: Bei Online-Banking ist sicherzustellen, dass wir PINs und TANs nicht einer vorgespiegelten Bank übermitteln (Authentizität), dass eine Überweisung nicht verändert wird (Integrität) und auch nicht abgehört werden kann (Vertraulichkeit). Bei einem Kauf über das Internet sollen die Kundendaten durch Dritte nicht beobachtbar sein.

Allgemein sind kryptographische Verfahren unverzichtbar bei der Realisierung von elektronischen Geschäftsprozessen. In Mobilfunknetzen sichern sie die Abrechnung. Kryptographische Verfahren sind eine Basis für Sicherheit im Internet und in Endgeräten oder für die Vergabe elektronischer Lizenzen.

Seit der Entwicklung des Internet wurde in den 1970er Jahren eine der wichtigsten Erfindungen seit Jahrtausenden der Kryptographie gemacht: Mit den asymmetrischen Schlüsseln, die aus einem geheimen, privaten Schlüssel und einem zugehörigen öffentlichen Schlüssel bestehen, ist es nicht mehr erforderlich, einen geheimen (symmetrischen) Schlüssel im Agentenkoffer zu übertragen. Diese Aufgabe kann heutzutage eine Verschlüsselung mit dem öffentlichen Schlüssel des Empfängers leisten.

In *Kapitel 1 „Ziele und Wege der Kryptographie“* werden Sicherheitsdienste und Sicherheitsmechanismen begrifflich eingeführt und einfache kryptographische Mechanismen anhand historischer Verfahren veranschaulicht. Was muss für die praktische Sicherheit beachtet werden und was versteht man unter perfekter Sicherheit.

Kapitel 2 „Symmetrische Chiffren“ beginnt mit endlichen Zahlenmengen und Restklassen. Es wird dabei Wert auf Anschaulichkeit gelegt und die Mathematik auf den Bedarf der Folgekapitel beschränkt. Man kann damit die Mathematik in kleinen Portionen und nahe zur Anwendung „verdauen“. Es folgen die aktuell wichtigen symmetrischen Verschlüsselungsverfahren, wie

die Blockchiffren DES, Triple-DES und AES als Nachfolger von DES sowie die Stromchiffren RC4 und A5. Ein vorgeschalteter Abschnitt über Erweiterungskörper dient nur einem tieferen Verständnis von AES und kann auch übergangen werden.

„*Hash-Funktionen*“ in Kapitel 3 erzeugen für ein Dokument einen charakteristischen Fingerabdruck, der als Hash-Wert bezeichnet wird. Hash-Funktionen sollen kollisionsresistent sein. Das heißt, es soll nicht möglich sein, unterschiedliche Dokumente mit gleichem Hash-Wert zu finden. Hash-Funktionen können mit Hilfe von Blockchiffren oder eigenständig konstruiert werden. Eine Hash-Funktion kann auch mit einem geheimen Schlüssel kombiniert werden, um damit einen „Message Authentication Code“ (MAC) auf Basis einer Hashfunktion zu bilden (HMAC).

Für „*Asymmetrische Chiffren*“ in Kapitel 4 wird das Rechnen mit Potenzen modulo n benötigt. Mit anschaulichen Beispielen wird erleichtert, diese Grundlagen zu verstehen. Die Verfahren mit asymmetrischen Schlüsseln RSA und ElGamal sind inzwischen die Klassiker für die Übertragung von symmetrischen Sitzungsschlüsseln und für die digitale Signatur. Neuere Verfahren auf der Basis von elliptischen Kurven kommen mit kürzeren Schlüsseln aus. Zu ihrem Verständnis wird in möglichst anschaulicher Weise in die erforderliche Mathematik eingeführt. „*Elliptic Curve Cryptography*“ (ECC) eignet sich besonders für Realisierungen auf Chipkarten.

„*Authentifikations-Protokolle*“ in Kapitel 5 dienen dazu, um Sicherheit über die Identität des Kommunikationspartners zu erhalten. Ein wichtiges Verfahren ist die „Challenge-Response-Authentifikation“, die eine aktuelle Antwort auf eine spezielle Frage anfordert. Für die Authentifikation werden meist asymmetrische Schlüssel in Verbindung mit Challenge-Response benutzt.

Die beiden letzten Kapitel widmen sich dem Einsatz der zuvor dargestellten kryptographischen Verfahren und Protokolle in Anwendungen, die bereits seit längerem Einzug in den elektronischen Alltag gefunden haben. Kapitel 6 „*Sicherheitsprotokolle und Schlüsselverwaltung*“ beschreibt, wie durch eine Schlüsselverwaltung der öffentliche Schlüssel einer Person verfügbar gemacht und bescheinigt wird, dass der öffentliche Schlüssel sicher zu einer bestimmten Person gehört. Diese sogenannten „Public Key Infrastrukturen“ (PKI) sind eine Grundlage für die Sicherheit im Internet. Sicherheitsprotokolle werden für drahtgebundene und für Funknetze besprochen. Gerade bei offenen Computer-Netzen spielen die in den vorherigen Kapiteln behandelten Verfahren für Authentifikation, Integrität und Vertraulichkeit eine wichtige Rolle.

Kapitel 7 „*Chipkarten und Sicherheitsmodule*“ bietet einen Einblick in deren Anwendung und Funktionsweise. Die häufigste Anwendung von Chipkarten ist die Authentisierung von Teilnehmern in Mobilfunksystemen. Mit mehreren Milliarden ausgegebenen SIM-Karten (UMTS, GSM) ist dieser Markt für Chipkarten der größte. Neuere Entwicklungen, wie Java-Chipkarten, oder ganz aktuelle Trends, wie Internet-Protokolle auf Chipkarten, werden vorgestellt. Eine weitere Anwendung der Chipkarten-Technologie liegt in dem Bereich „Trusted Computing“. Das hier eingesetzte „Trusted Platform Module“ (TPMs) ist aus technischer Sicht den Chipkarten sehr ähnlich.

Dieses Buch ist gedacht als eigenständiges Fachbuch für das Selbststudium oder als begleitende Unterlage zu einer Vorlesung. Übungsbeispiele mit Lösungen können zur weiteren Vertiefung herangezogen werden. Neben den grundlegenden kryptographischen Algorithmen, Mechanismen und Protokollen gibt das Buch Einblick in Anwendungsgebiete, wie Sicherheitsver-

fahren in Internet und Mobilfunknetzen, Betriebssysteme von Chipkarten, Trusted Computing und Public-Key-Infrastrukturen. Das Buch zielt auf eine kompakte und ausgewogene Einführung in die Kryptographie und deren aktuelle Anwendung. Dabei sind die neuesten und praktischen Erfahrungen eingeflossen, einerseits über Schlüsselverwaltung (PKI) und Sicherheitsprotokolle und andererseits über Chipkarten und Sicherheitsmodule (TPM).

Für weitergehende und spezielle Fragen bieten die angegebene Literatur und auch das Internet oft aktuelle Antworten. Zum Experimentieren mit den einzelnen Algorithmen kann das Werkzeug CrypTool (<http://www.cryptool.de/>) sehr empfohlen werden.

Wir danken Herrn Bernhard Esslinger für das umfangreiche fachliche Feedback und für das externe Vorwort. Unser Dank gilt ferner dem Vieweg-Verlag für eine vertrauensvolle Zusammenarbeit sowie Frau L. Heckmann für die redaktionelle Durchsicht des Skripts.

München und Athen, im Dezember 2007

Joachim Swoboda
Stephan Spitz
Michael Pramateftakis

Vorwort von Bernhard Esslinger

Die Autoren dieses Buches danken Herrn Bernhard Esslinger für dieses externe Vorwort. Herrn Esslinger braucht man nicht vorzustellen. Dennoch wollen die Autoren einige Worte zu seiner Einführung festhalten:

Hr. Esslinger hat intensive theoretische, praktische und berufliche Erfahrung auf dem Gebiet der IT-Sicherheit und Kryptographie. Er war Entwicklungsleiter der Sicherheitskomponenten des SAP-Systems R/3, Chief Information Security Officer (CISO) bei der SAP AG und Leiter IT-Sicherheit bei der Deutschen Bank AG. Derzeit leitet er bei der Deutschen Bank das Cryptography Competence Center, das dort weltweit für die angemessene Nutzung von Kryptographie zuständig ist. Außerdem hat Hr. Esslinger einen Lehrauftrag für IT-Sicherheit und leitet seit 10 Jahren das Open-Source-Projekt CrypTool, das das weltweit erfolgreichste Lernprogramm zum Thema Kryptologie erstellt. Hr. Esslinger schreibt dieses Vorwort als Privatperson.

Joachim Swoboda, Stephan Spitz, Michael Pramateftakis

In den letzten 10 Jahren gab es mehr und mehr Bücher zum Thema Kryptographie und IT-Sicherheit, und doch ist dies ein einzigartiges Buch, worauf ich am Ende meines Vorwortes noch eingehen möchte.

So wie die Bedeutung der EDV (oder neuer IT = Informationstechnologie) in der Gesellschaft in den letzten Jahren zunahm, so nehmen auch die Bedeutung von IT-Sicherheit und Kryptographie zu.

Unternehmen treffen ihre Entscheidungen basierend auf den Daten in ihren Computern, sie steuern Waren- und Geldströme damit, und das immer kurzfristiger. Gleichzeitig werden immer mehr Daten gesammelt, um fundiertere Entscheidungen zu treffen, besseren Service zu bieten oder vermeintlich besser Terroristen fangen zu können.

Die IT-Abhängigkeit ist den Firmen und Behörden bewusst: Regularien wie SOX (Sarbanes-Oxley Act), die sich eigentlich auf die Exaktheit der betriebswirtschaftlichen Daten beziehen, schließen inzwischen die EDV mit ein. Staaten weltweit definieren die „Kritischen Infrastrukturen“, und Behörden wie das BSI oder das NIST bieten hervorragende Maßnahmenkataloge, mit deren Hilfe man seine EDV sicher betreiben kann.

Aber auch wenn die Verfahren der Kryptographie und IT-Sicherheit eigentlich relativ gut verstanden und ausgereift sind, so werden sie doch immer wieder fehlerhaft oder nachlässig angewandt. Hierzu ein paar **Beispiele** (Namen werden nur bei schon in der Presse publizierten Fällen genannt):

- Im 4. Quartal 2007 gab es in Großbritannien drei große Skandale mit Datenverlusten bisher unbekannten Ausmaßes:
Mitte November wurde bekannt, dass der britischen Behörde HM Revenues and Customs zwei CDs beim Postversand verloren gingen, auf denen Personendatensätze mit Name,

Adresse, Geburtsdatum, nationaler Versicherungsnummer und teilweise auch Kreditkartennummer gespeichert waren (angeblich Daten von 25 Millionen Menschen, die zu Familien mit Kindergeldempfängern gehörten).

Mitte Dezember wurde bekannt, dass dem Verkehrsministeriums durch Outsourcing der Datenspeicherung an eine US-Firma eine Festplatte mit Datensätzen von drei Millionen Fahrschülern abhanden gekommen ist.

Und kurz vor Weihnachten meldete der staatliche Gesundheitsdienst, dass „Tausende Patienteninformationen“ verloren gegangen waren (laut Aufsichtsbehörde waren das allein im Osten Londons die Daten von 160.000 Kindern). Die Patientendaten von Erwachsenen und Kindern kamen neun Verwaltungszentren des britischen Nationalen Gesundheitssystems (NHS) abhanden. Wie immer hieß es auch vom britischen Gesundheitsministerium, es gebe keinen Hinweis darauf, dass sie in falsche Hände geraten seien.

Kritiker beanstandeten, dass die Regierung zu wenig für die Sicherheit sorgt, aber ständig neue Daten erhebt und speichert.

Warum brauchen untergeordnete Behörden Zugriff auf diese Datenmengen? Warum sind diese Daten beim Transfer nicht verschlüsselt? Warum werden zum Transfer CDs benutzt statt gesicherter TCP/IP-Verbindungen?

- Schlimmer noch als in UK, wo nur die Gefahr besteht, dass diese sensiblen Daten in die falschen Hände gelangen, ist ein Vorgang in Japan, der dort in der zweiten Jahreshälfte 2007 die Regierung erschütterte: Bei ungefähr einem Drittel der Rentenkonto können die Guthaben den Konten nicht korrekt zugeordnet werden. Laut Behördenangaben gingen Rentendaten von mindestens 8,5 Millionen Menschen verloren, und die Daten zu insgesamt 64 Millionen Anträgen auf Rente oder soziale Unterstützung konnten nicht mehr gefunden werden.

Wo ist die Datensicherung? Wo sind die Signaturen, die die Verbindung herstellen könnten?

- In den USA sind bis Ende 2007 in den verschiedenen Datenbanken der Geheimdienste und des Department of Homeland Security mehr als eine halbe Million Personen gespeichert, die dort fälschlicherweise aufgenommen wurden. Verfahren zur vollständigen Löschung auch rehabilitierter Personen existieren nicht oder funktionieren nicht korrekt. Trotzdem ist die Konsequenz nicht das Aufräumen und Konsolidieren, sondern: Ende 2007 meldete das FBI, dass es rund eine Milliarde USD investieren will, um bis 2013 die weltweit größte Datenbank mit biometrischen Daten zu erstellen.

Wo bleibt die alte Forderung, z.B. aus dem Datenschutz, nur notwendige Daten zu speichern, für alle Daten ein Verfallsdatum anzugeben und bei allen Daten die Nutzung nur für vorher explizit benannte Gründe zu zulassen?

- In Deutschland wurde bis Mitte 2007 bekannt, dass die Bundeswehr Daten mit Geheimdienstinformationen nicht mehr auf ihren Bändern lesen könne. Oder sollten diese Informationen nicht mehr auffindbar sein? Auf Daten, die explizit nur zur Erhebung von LkW-Maut gesammelt wurden, melden andere Behörden Ansprüche an.
- Aber auch im nichtpolitischen Bereich passieren Fehler mit manchmal schlimmen Folgen:
 - Nicht funktionierende Scanner für die Teile in einem Hochregallager führten fast zur Firmenpleite.
 - Kreditkartennummern, die verschlüsselt übertragen wurden, wurden danach in großem Stil von Webservern im Klartext abgezogen.

- Controller errechneten Kennzahlen für Managemententscheidungen mit Hilfe von Excel-Makros, obwohl nach unterschiedlichen Untersuchungen gerade die selbst erstellten Formeln in großen Excel-Tabellen immer wieder fehlerhaft sind.
- Die kompletten Kundendaten einer amerikanischen Großbank wurden regelmäßig als Backup auf Bänder gesichert, die von einer professionellen Firma zur Datensicherung und Datenspeicherung eingelagert wurden. Leider waren die Daten auf den Bändern nicht verschlüsselt, und manche Bänder gingen schon beim Transport verloren. Aber selbst bei den eingelagerten Bändern kann nicht sichergestellt werden, dass davon keine Kopien angefertigt werden.
- Bei der Einführung von Mitarbeiter-Smartcards und SecurID-Tokens wurden die Super-PINs zum Zurücksetzen der Smartcards auf CD geschickt – unverschlüsselt, ohne Schlüsselmanagement beim Kunden und ohne dass der Kunde die Super-PINs ändern konnte, so dass beim Hersteller theoretisch ebenfalls noch eine Kopie vorliegen kann, mit denen man die Kunden-Smartcards missbrauchen könnte.
- Applikationen verwenden moderne kryptografische Verfahren, aber alles basiert auf schwachen Passwörtern für Benutzer, Administratoren oder Super-User – ein Kartenhaus.
- Weil die modernen kryptografischen Verfahren inzwischen in Betriebssystemen zur Verfügung stehen, können sie leicht benutzt werden. Die Bedeutung von klar definierten Prozessen für ein gutes Schlüsselmanagement wird übersehen.
- Applikationen verwenden Protokolle, die die verwendeten Verfahren und die Mindeststandards nicht aushandeln können. Jede Umrüstung geht dadurch in die Millionen und wird entsprechend erst (zu) spät durchgeführt.

Das **Buch** bietet einen sehr breiten Überblick über den aktuellen Stand der Kryptographie und IT-Sicherheit und ist eher Praxis/Prozess-orientiert. Dazu definiert es die Ziele der IT-Sicherheit und erläutert, mit welchen kryptografischen Maßnahmen welche Ziele erreicht werden können. Es werden sowohl die Grundbegriffe der Sicherheitsmechanismen (wie beispielsweise Authentizität) als auch – wohl dosiert – die notwendigen mathematischen Grundlagen erläutert (z.B. welche Axiome der Arithmetik bei der Modulo-Operation erfüllt sind und immer wieder, warum dies von Bedeutung ist; siehe Kap. 2.1, 2.5 und 4.1). Die Algorithmen werden ausführlich genug besprochen, um sie nachvollziehen zu können.

Dabei wird der Inhalt stets mit Beispielen ergänzt: wo finden Verfahren wie z.B. AES und RSA Verwendung (z.B. Hybridverschlüsselung in dem E-Mail-Standard S/MIME oder in PGP) oder wie steht es um ihre Anwendbarkeit (z.B. Performance und Patentsituation bei Elliptischen-Kurven-Systemen). Immer wird auch der wichtige kryptoanalytische Aspekt behandelt.

Kapitel 5 (Authentifikationsprotokolle) enthält eine sehr schöne Zusammenstellung, wie die Authentisierung z.B. mit Passwort, mit Challenge-Response-Verfahren, mit digitalen Signaturen, etc. funktioniert.

Abgerundet wird das Buch mit den Kapiteln 6 und 7: Diese erläutern, wo die zuvor genannten Verfahren eine Anwendung finden. Natürlich muss hier eine Auswahl getroffen werden, welche Themen ausführlich besprochen und welche nur kurz angeschnitten werden. Darin enthalten sind aktuelle Themen, die über die einfachen Kryptoalgorithmen (kryptografische Primiti-

ve) hinausgehen: PKI, Sicherheitsprotokolle (wie Kerberos, SSL, IPsec, Protokolle zur IP-Telefonie, WLAN), Chipkarten und ihre Anwendungen (z.B. Verschlüsselung und Authentisierung in GSM-Netzen, Nutzung von SIM-Karten, TPM oder so moderne Tokens wie Internet-Smartcards, für die man keine Treiber mehr braucht, weil sie auf dem Chip selbst den nötigen TCP/IP-Stack implementieren).

Da das Buch als Zielgruppe den versierten Anwender und den Ingenieur hat, liegt der Schwerpunkt nicht auf der puren Mathematik, sondern auf der ausführlichen und klaren Vermittlung des Verständnisses der Grundlagen, der richtigen Anwendung und der korrekten und ausführlichen Darstellung der vorhandenen technischen Möglichkeiten.

Ich halte das Buch für ein schönes Nachschlagewerk und eine sehr gute Grundlage, um sich einen Überblick über das große Thema Kryptographie und IT-Sicherheit zu verschaffen. Vor allem gefiel mir die wohl dosierte Beschreibung der mathematischen Grundlagen sehr gut.

Die anwendungsbezogene Darstellung gelingt so gut, dass ich dem Buch sehr gerne eine gute Aufnahme bei den Lesern wünsche. Und wie die obigen Beispiele zeigen, ist dieses Wissen und die nötige Sensibilität für dieses Thema notwendiger denn je.

Bernhard Esslinger, Dezember 2007

Inhaltsverzeichnis

1	Ziele und Wege der Kryptographie	1
1.1	Historische Verfahren	3
1.1.1	Skytale	3
1.1.2	Caesar-Chiffre	4
1.1.3	Vigenère-Chiffre	7
1.1.4	Vernam-Chiffre	10
1.1.5	Enigma	12
1.2	Sicherheitsdienste	14
1.2.1	Vertraulichkeit	15
1.2.2	Authentizität und Integrität	15
1.2.3	Verbindlichkeit	17
1.2.4	Anonymität	17
1.2.5	Zugriffskontrolle, Autorisierung	18
1.2.6	Sicherheitsdienste im Überblick	18
1.2.7	Bedrohungen und Sicherheitsdienste	19
1.3	Sicherheitsmechanismen	21
1.3.1	Verschlüsselung als Abbildung	21
1.3.2	Symmetrische Verschlüsselung	22
1.3.3	Asymmetrische Verfahren	26
1.3.4	Digitale Signaturen	28
1.3.5	Hilfs-Funktionen	31
1.3.6	Sicherheitsprotokolle	36
1.4	Sicherheit, Angriffe und perfekte Sicherheit	37
1.4.1	IT-Sicherheit	37
1.4.2	Kryptographische Sicherheit	37
2	Symmetrische Chiffren	43
2.1	Rechnen mit endlichen Zahlenmengen und Restklassen	43
2.1.1	Arithmetik modulo n , Restklassen	44
2.1.2	Axiome für Gruppe, Ring und Körper	45
2.1.3	Multiplikativ inverse Elemente, praktische Ermittlung	49
2.1.4	Übungen	51

2.2	DES, Data Encryption Standard.....	52
2.2.1	DES, Eigenschaften	53
2.2.2	DES, Verschlüsselung und Entschlüsselung.....	54
2.2.3	Triple-DES	57
2.2.4	DES-Anwendungen	58
2.2.5	Übungen	62
2.3	IDEA, International Data Encryption Algorithm	62
2.3.1	IDEA, im Überblick	63
2.3.2	IDEA, Verschlüsselung	64
2.3.3	IDEA, Entschlüsselung.....	65
2.3.4	Übungen	67
2.4	Stromchiffren RC4 und A5	68
2.4.1	RC4.....	69
2.4.2	A5	70
2.4.3	Sicherheit von Stromchiffren.....	72
2.5	Rechnen mit Polynom-Restklassen und Erweiterungskörpern.....	72
2.5.1	Polynom-Restklassen.....	73
2.5.2	Irreduzible Polynome	75
2.5.3	Axiome für Erweiterungskörper und Beispiel	76
2.5.4	Übungen	79
2.6	AES, Advanced Encryption Standard	81
2.6.1	AES, Verschlüsselung und Entschlüsselung.....	81
2.6.2	AES, Transformationsfunktionen	83
2.6.3	Übungen	85
2.7	Betriebsarten von Block-Chiffren: ECB, CBC, CFB, OFB, CTR.....	88
2.7.1	Wozu Betriebsarten?.....	88
2.7.2	Eigenschaft der Betriebsarten.....	89
3	Hash-Funktionen.....	95
3.1	Anwendungen und Arten von Hash-Funktionen	95
3.1.1	Arten von Hash-Funktionen	96
3.1.2	Angriffe auf Hash-Funktionen.....	97
3.2	Hash-Funktionen auf Basis von Block-Chiffren	100
3.3	Eigenständige Hash-Funktionen	101

3.3.1	MD5.....	103
3.3.2	SHA-1	104
3.3.3	SHA-2.....	105
3.3.4	SHA-Nachfolger.....	106
3.4	HMAC, MAC auf Basis von Hash.....	106
3.4.1	HMAC-Algorithmus.....	107
3.4.2	Vergleich von MAC mit HMAC	108
4	Asymmetrische Chiffren.....	109
4.1	Rechnen mit Potenzen modulo n	109
4.1.1	Potenzen modulo n	110
4.1.2	Sätze von Fermat und Euler, Eulersche Φ -Funktion	111
4.1.3	Berechnung großer Potenzen.....	114
4.1.4	Diskreter Logarithmus	115
4.1.5	Quadratwurzeln in der Rechnung modulo n	116
4.1.6	Chinesischer Restsatz	118
4.1.7	Übungen	120
4.2	RSA, Rivest/Shamir/Adleman	121
4.2.1	RSA, Schlüssel, Verschlüsselung, Signaturen.....	121
4.2.2	Zur Implementierung von RSA	124
4.2.3	Sicherheit von RSA	125
4.2.4	RSA-Beschleunigung durch Chinesischen Restsatz.....	127
4.2.5	Übungen	128
4.3	Diffie-Hellman-Schlüsselvereinbarung.....	129
4.4	ElGamal-Verfahren	131
4.4.1	Schlüsselvereinbarung nach ElGamal	131
4.4.2	Digitale Signatur und Verifikation nach ElGamal.....	133
4.4.3	Effizienz des ElGamal-Verfahrens	134
4.5	Elliptische Kurven, ECC-Kryptographie	135
4.5.1	Einführung.....	135
4.5.2	Mathematische Grundlagen	136
4.5.3	Geometrische Definition der Additionsoperation auf der Kurve.....	137
4.5.4	Bestimmung algebraischer Formeln für die Addition	139
4.5.5	Elliptische Kurven im diskreten Fall	141
4.5.6	Standardisierte Kurven	143

4.5.7	Anwendung der elliptischen Kurven in Algorithmen	144
4.5.8	Ausblick.....	147
5	Authentifikations-Protokolle	149
5.1	Authentifikation mit Passwort.....	150
5.1.1	Verfahren mit Dauer-Passwort	150
5.1.2	Verfahren mit Einmal-Passwort	150
5.2	Challenge-Response-Authentifikation	152
5.3	Authentifikation mit digitalen Signaturen	153
5.4	Fiat-Shamir-Authentifikation	155
5.4.1	Vertrauenswürdige Schlüsselbank	155
5.4.2	Authentifikations-Runde	156
5.4.3	Sicherheit für die Authentifikation	158
5.4.4	Zero-Knowledge-Protokoll.....	159
5.5	Authentifikation mit symmetrischen Schlüsseln	159
5.5.1	Protokollziel	159
5.5.2	Kerberos-Protokoll	160
5.6	Angriffe auf Authentifikations-Protokolle	162
6	Sicherheitsprotokolle und Schlüsselverwaltung	165
6.1	Public Key Infrastrukturen.....	166
6.1.1	Komponenten und Prozesse in einer PKI	166
6.1.2	PKI-Standards und Gesetzgebung	171
6.2	Sicherheitsprotokolle im Internet	174
6.2.1	Das Internet und die Internet-Protokollsuite.....	174
6.2.2	Sicherheitsprotokolle in der Internet-Protokollsuite	175
6.3	Das SSL/TLS-Protokoll	177
6.3.1	Das SSL-Handshake	177
6.3.2	Sicherung über SSL-Records.....	179
6.3.3	Secure Shell, SSH.....	180
6.4	IP-Sicherheit mit IPSec.....	181
6.4.1	Internet Key Exchange	181
6.4.2	Authentication Header	185
6.4.3	Encapsulated Security Payload.....	187
6.4.4	Tunnel-Modus	188

6.4.5	Transport-Modus	189
6.5	Sicherheit bei der Echtzeit-Datenübertragung.....	190
6.5.1	SRTP und SRTCP	191
6.5.2	MIKEY	192
6.5.3	ZRTP	193
6.5.4	DTLS	193
6.6	Sicherheit in Funknetzen.....	194
6.6.1	EAP	194
6.6.2	WEP.....	196
6.6.3	WPA und WPA-2	198
7	Chipkarten und Sicherheitsmodule.....	199
7.1	Historie.....	199
7.2	Chipkarten-Technologie.....	199
7.2.1	Arten von Chipkarten	199
7.2.2	Anwendungen.....	200
7.3	Aktuelle und zukünftige Chipkarten-Architekturen.....	201
7.3.1	Sicherheit von Chipkarten	202
7.3.2	Chipkarten-Architektur nach ISO/IEC 7816	204
7.3.3	Interpreter-basierende Chipkarten-Betriebssysteme	207
7.4	Einsatz von Chipkarten	214
7.4.1	Schnittstellen zur Chipkartenintegration	214
7.5	Chipkarten-Anwendungen	223
7.5.1	Mobilfunk Chipkarten	223
7.5.2	Zukünftiger Einsatz neuer Internet-Chipkarten	233
7.6	Trusted Computing und Trusted Platform Module	234
7.6.1	Die Trusted Computing Group	234
7.6.2	Das Trusted Platform Module	235
7.6.3	Zusammenspiel der TCG Komponenten	238
7.6.4	Integritätsmessung	240
Literatur		241
Glossar		249
Deutsch-Englisch, Begriffe.....		255
Sachwortverzeichnis.....		257