



6.

Auflage



Klaus Schmeh

# Kryptografie

Verfahren • Protokolle • Infrastrukturen

 X-EDITION

dpunkt.verlag



**Klaus Schmeh** ist seit 1997 als Unternehmensberater mit Schwerpunkt Kryptografie aktiv. Seit 2004 arbeitet er für die Gelsenkirchener Firma cryptovision. Nebenbei ist Klaus Schmeh ein erfolgreicher Journalist, der 15 Bücher und 150 Zeitschriftenartikel verfasst hat. Etwa die Hälfte seiner Werke beschäftigt sich mit kryptografischen Themen. Klaus Schmeh hat damit mehr zum Thema Kryptografie veröffentlicht als jede andere Person in Deutschland. Seine Stärke ist die anschauliche Vermittlung komplexer Zusammenhänge, die auch in seinen anderen Veröffentlichungen (meist zu populärwissenschaftlichen Themen) zum Tragen kommt.

### **iX-Edition**

In der *iX*-Edition erscheinen Titel, die vom dpunkt.verlag gemeinsam mit der Redaktion der Computerzeitschrift *iX* ausgewählt und konzipiert werden. Inhaltlicher Schwerpunkt dieser Reihe sind Standardthemen aus IT, Administration und Webprogrammierung.

Papier  
plus<sup>+</sup>  
PDF.

Zu diesem Buch – sowie zu vielen weiteren dpunkt.büchern – können Sie auch das entsprechende E-Book im PDF-Format herunterladen. Werden Sie dazu einfach Mitglied bei dpunkt.plus<sup>+</sup>:

[www.dpunkt.de/plus](http://www.dpunkt.de/plus)

**Klaus Schmeh**

# **Kryptografie**

**Verfahren, Protokolle, Infrastrukturen**

6., aktualisierte Auflage



**dpunkt.verlag**

Klaus Schmeh  
klaus.schmeh@dpunkt.de

Lektorat: Dr. Michael Barabas  
Copy-Editing: Annette Schwarz, Ditzingen  
Satz: Klaus Schmeh  
Herstellung: Susanne Bröckelmann  
Umschlaggestaltung: Helmut Kraus, [www.exclam.de](http://www.exclam.de)  
Druck und Bindung: Druckerei C.H. Beck

#### Bibliografische Information Der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

#### ISBN:

Print 978-3-86490-356-4  
PDF 978-3-86491-907-7  
ePub 978-3-86491-908-4  
mobi 978-3-86491-909-1

6., aktualisierte Auflage 2016  
Copyright © 2016 dpunkt.verlag GmbH  
Wiebinger Weg 17  
69123 Heidelberg

Die vorliegende Publikation ist urheberrechtlich geschützt. Alle Rechte vorbehalten. Die Verwendung der Texte und Abbildungen, auch auszugsweise, ist ohne die schriftliche Zustimmung des Verlags urheberrechtswidrig und daher strafbar. Dies gilt insbesondere für die Vervielfältigung, Übersetzung oder die Verwendung in elektronischen Systemen.

Es wird darauf hingewiesen, dass die im Buch verwendeten Soft- und Hardware-Bezeichnungen sowie Markennamen und Produktbezeichnungen der jeweiligen Firmen im Allgemeinen warenzeichen-, marken- oder patentrechtlichem Schutz unterliegen.

Alle Angaben und Programme in diesem Buch wurden mit größter Sorgfalt kontrolliert. Weder Autor noch Verlag können jedoch für Schäden haftbar gemacht werden, die in Zusammenhang mit der Verwendung dieses Buches stehen.

5 4 3 2 1 0

## Vorwort von Prof. Bernhard Esslinger

*»Cryptography is about communication in the presence of adversaries.«*

Ron Rivest, 1990

*»Transparenz. Das ist das Höchste, was man sich in einer technologisch hoch entwickelten Gesellschaft erhoffen kann. ... sonst wird man einfach nur manipuliert ...«*

Daniel Suarez in *Darknet*, 2011

*»The best that can be expected is that the degree of security be great enough to delay solutions by the enemy for such a length of time that when the solution is finally reached, the information thus obtained has lost all its value.«*

William Friedman in *Military Cryptanalysis*, 1936

*»Immer wenn man etwas konkret formuliert, wird man angreifbar, aber wenn man nicht konkret wird, ist es nicht nachvollziehbar.«*

Unbekannt

## Buch und Vorwort

Als Herr Schmech mich fragte, ob ich das Vorwort zu seinem Kryptografie-Buch schreibe, war meine erste Reaktion: »Warum ich und warum ein weiteres Buch über Kryptologie?«

Auf beide Fragen hatte Herr Schmech eine einleuchtende Antwort:

- Ich sollte das Vorwort schreiben, da er jemand suchte, der intensive theoretische, praktische und berufliche Erfahrung auf diesem Gebiet habe und diese Erfahrungen pointiert in das Vorwort einfließen ließe (ich war bei SAP CISO und Entwicklungsleiter der Sicherheitskomponenten des Systems R/3, bei der Deutschen Bank Leiter IT-Sicherheit und Chef des »Cryptography Competence Center« und bin unabhängiger Consultant für Risikomanagement, also für eine angemessene und effiziente Allokation der Ressourcen. Außerdem habe ich einen Lehrauftrag zu IT-Sicherheit und Kryptologie und leite seit über 15 Jahren ein Open-Source-Projekt, das das bisher erfolgreichste Lernprogramm zu Kryptologie erstellt).
- Sein Buch hat aufgrund mehrerer Eigenschaften ein Alleinstellungsmerkmal: Aktualität, Umfang/Vollständigkeit, Betonung der Anwendungssicht, Behandlung auch der umliegenden Felder (Geschichte, Gesellschaft, Politik, Wirtschaftsspionage, ... ) und – aufgrund seiner journalistischen Erfahrung – die gewohnt leicht verständliche Beschreibung auch komplexer Zusammenhänge.



## Kryptografie – eine spannende Angelegenheit

Kryptografie ist eine in mehrfacher Hinsicht spannende Angelegenheit:

- Für **Historiker**, weil sie schon immer Teil des strategischen und taktischen Arsenal der Mächtigen war.
- Für **Mathematiker und Informatiker**, weil sich in der Zahlentheorie und der mathematischen Kryptologie ständig neue Forschungsergebnisse ergeben (z. B. die Möglichkeiten für die Cloud durch homomorphe Verschlüsselung, generische Analysemethoden wie SAT-Solver, die Berechnung von Gröbner-Basen, sehr große Gitterreduktionen, erweiterte Grenzen bei neuen und alten Verschlüsselungsverfahren wie das Zerlegen eines gegebenen 232-stelligen Produktes in seine beiden Primzahl-Faktoren durch Kleinjung etc. im Jahre 2009 oder das Knacken eines Pairing-basierten 923-Bit-Verschlüsselungssys-

tem durch Fujitsu etc. in 2012). Und das zukünftige Quanten-Computing sorgt dafür, dass weiter intensiv an neuen Verfahren geforscht wird (z. B. haben Sicherheitsforscher um Bernstein/Lange im Zuge des europäischen Forschungsprojektes PQCRYPTO Mitte 2015 konkrete Ansätze empfohlen).

- Für **Praktiker und Sicherheitsverantwortliche**, weil es stets neue Entwicklungen gibt: Auf der Angreiferseite werden etablierte Protokolle, die man für sicher hielt, kreativ missbraucht oder mit Man-in-the-Middle-Attacken umgangen. Vor allem aber bieten normale Produkte den Angreifern jede Menge Einfallstüren: Es ist unglaublich, wie viele Fehler beim Schlüsselmanagement und in den Implementierungen gemacht werden – und das nicht nur bei »einfachen« Produkten wie Routern (die Sicherheitsfirma SEC Consult untersuchte die öffentlich zugängliche Firmware von mehr als 4000 Geräten und gab im Nov. 2015 die Schätzung ab, dass bei 9 Prozent aller SSL-Endpunkte im Netz die privaten Schlüssel bekannt sind), sondern auch bei sogenannten Marktführern wie Symantec und PeopleSoft, die beispielsweise Schlüssel fest in produktiven Executables ablegten (ist inzwischen behoben). Auch auf der Seite »der Guten« kommen neue Techniken zum Einsatz: Nutzen von virtualisierbarer Hardware oder auch Open-Source-Lösungen wie OpenXPKI, das weit über die Grundfunktionalität einer PKI hinausgeht und zusätzlich die Anpassung an eigene Geschäftsprozesse über eine Workflow-Engine ermöglicht, eine Abstraktionsebene für die praxisnahe Anbindung beliebiger Datenquellen bietet, Zertifikats-Renewal-Software (CertNanny) über Automatisierungs-APIs wie SCEP andockt, externe CAs wie SwissSign anbindet, Tracking-Systeme wie RT integriert und CA-Rollover nahezu automatisiert. OpenXPKI ist ein sehr »konservativ« (im positiven Sinne) geführtes Open-Source-Projekt, das erst nach zehnjähriger Projektlaufzeit und über fünf Jahren produktiven Einsatzes im Oktober 2015 die Version 1.0 releaste ([www.openxpki.org](http://www.openxpki.org)).
- Für **IT-Manager**, weil sich hier ganz praktisch die Fragen nach dem richtigen Umgang mit dem Risiko stellen, nach den angemessenen Maßnahmen, nach der Balance zwischen technischen und organisatorischen Maßnahmen (Anweisungen, Schulungen, Kontrolle), nach der erlangten Sicherheit, die sich aus der Wahl der richtigen Algorithmen/Protokolle, korrekter Implementierung und der Benutzerfreundlichkeit ergibt.
- Für **jedermann**. Um sich zu schützen, insbesondere nachdem man dank Snowden genauer weiß, wie die NSA die ganze Prozesskette der Sicherheit schwächte. Um zu verstehen, wie man mit Kryptografie seine Privatsphäre einigermaßen schützen kann. Dass man dazu auch selbst beitragen muss und kann – beispielsweise mit kostenloser Open-Source-Software zum Verschlüsseln seiner E-Mail (Thunderbird), durch (Let's-encrypt-)Zertifikate für seine Webseiten, durch Nutzung von VeraCrypt zur Partitionsverschlüsselung, durch Unterbinden des massenhaften anlasslosen Abhörens und, und, und.

## Kryptografie im Unternehmen

Unternehmen investieren nicht einfach in IT-Sicherheit. Stattdessen werden Risikobetrachtungen angestellt, und es wird versucht, das optimale Maßnahmenbündel zur Verringerung/Vermeidung (Mitigation) des Risikos zu finden. Dabei kann Kryptografie die richtige Maßnahme sein, sie ist es aber nicht immer. Sie ist es vor allem dann, wenn sie mit Sachverstand eingesetzt wird. Manchmal sind organisatorische Maßnahmen billiger, manchmal wirken Mitarbeiterschulungen nachhaltiger. Immer kommt es auf den richtigen Mix an. Unter den technischen Maßnahmen wirkt Kryptografie proaktiv – im Gegensatz zu reaktiven Maßnahmen wie Monitoring.

Investitionen erfolgen nicht nur aus langfristig geplanten Überlegungen, sondern vermehrt auch wenn Aufsichtsbehörden, Kreditgeber oder Börsen Auflagen erteilen (z. B. »Two-Factor Authentication« der FFIEC, Schlüsselaufbewahrung in HSMs als Forderung der MAS, Basel-2, Compliance-Forderungen, SOx).

Im Gegensatz zur Lehre an den Hochschulen und zur Arbeit der Forscher stellen sich den Anwendern primär die Fragen nach den Kosten der Umsetzung (einmalige Kosten für Entwicklung und Roll-out, laufende Kosten für Betrieb und Schlüssel-Management), zur Vermeidung von Outages und zur Akzeptanz bei den Benutzern.

## Kryptografie – typische Erscheinungen

Dabei ergeben sich im Umfeld der Kryptografie die sonst auch in der IT und im Management manchmal typischen Erscheinungen:

- Gartner-Hype-Kurven, die z. B. von PKI zuerst die Lösung aller Sicherheitsprobleme erwarteten, dann PKI »verdammten«, und nun ist PKI doch fast überall im Einsatz (Online-Banking, Webauthentisierung, SOA, Flaschenpfandsystem)
- »Angesagte« Produkte bieten für ein bestimmtes Problem eine Lösung an, aber gleichzeitig schafft ihr Einsatz neue Probleme (z. B. mathematisch sehr spannende neue Verfahren mit schönen Namen, die von Firmen mit Venture Capital vermarktet werden. Dabei ist dann die Anzahl der Mitarbeiter in den Vertriebs-, Marketing- und Rechtsabteilungen um ein Vielfaches höher als die Anzahl der kryptografischen Kompetenzträger oder der eigentlichen Softwareentwickler). Ebenso zu hinterfragen sind angesagte Begriffe wie BYOD, bei denen noch ein ganzes Bündel an Fragen ungeklärt ist: Hierbei sollten Firmen ihren Mitarbeiter eher erstklassige Smartphones (auch zur Privatbenutzung in einem abgetrennten Bereich) ausgeben, als jeden Handtyp der Mitarbeiter zuzulassen. Interessen von Herstellern und Netzwerk-Providern zielen aber eher auf den privaten Besitz ab, da dort im Gegensatz zu den Firmen keine besonderen Firmenkonditionen zu gewähren sind.

- Manager müssen verstehen lernen, dass man bei Infrastrukturen nicht nur nach den Alternativen Make or Buy fragen sollte, sondern vor allem nach der nahtlosen Integration in die eigene IT-Landschaft und welchen Einfluss man hat, dass bedarfsgerechte Neuerungen umgesetzt werden, um Kostenvorteile zu heben.
- Top-Manager, die ihre speziellen Gadgets wollen und die sie sich auch genehmigen können, obwohl die Sicherheitsarchitektur und die Interoperabilität dafür nicht ausreichend gegeben sind (was z. B. dazu führt, dass gerade wichtige E-Mails im Klartext versandt werden).
- Eine Konzentration der Anbieterfirmen und ein Marktverhalten einzelner großer IT-Security-Anbieter, das darauf abzielt, die Kunden abhängig zu machen. Nicht offengelegte Schnittstellen werden als Sicherheitsmerkmal verkauft (Security by Obscurity oder verborgene Hintertüren?). Die nächste Hardwaregeneration gibt es umsonst, dafür sind die Updates umso teurer. Ein Hersteller, der schon mit einem Produkt zum Virenschutz im Unternehmen ist, verkauft sein Data-Loss-Prevention-Produkt zum Dumpingpreis. Alles aus einer Hand kann späteres Wechseln nahezu unmöglich machen und gerade im Sicherheitsbereich der Spionage Tür und Tor öffnen.
- Es zählen Kosten und kurzfristige Gewinne, sodass beispielsweise nicht hinterfragt wird, warum eine Backup-Lösung auf amerikanischem Boden viel billiger ist als in Europa und warum die Backup-Bänder unverschlüsselt ins Bergwerk gebracht werden. Hier helfen nur staatliche Auflagen und Haftung für den Verlust von Daten. Vorbildlich und Arbeitsplätze schaffend sind die Schweizer Regelungen, die beispielsweise die Verarbeitung der Kontendaten in ihrem gesamten Lebenszyklus nur auf Schweizer Boden erlauben.
- Unternehmen, die vorausseilenden Gehorsam und unterwürfige Scheinloyalität fördern, deren Top-Manager Kritik und offene Diskussion abwürgen, gelangen schneller an den Rand der Pleite (dies zeigen die Betrugsfälle in der Finanz- und Automobilindustrie der letzten Jahre). Modernes Risikomanagement schaut sich inzwischen auch an, wie Führungskräfte mit konstruktivem Widerspruch und selbstbewussten Warnungen umgehen und ob die proklamierten Werte auch wirklich gelebt werden.
- In Arbeitsgruppen über Layout, Strategie und Businessmodelle meint jeder mitreden und sich profilieren zu können – im Gegensatz zu sehr erfolgreichen technischen Arbeitsgruppen, wo nur mitreden kann, wer über die nötige Kompetenz verfügt. Karriere-affine Kollegen und Entscheider diskutieren oft gerne bei den ersten Arbeitsgruppen mit, denn sie führen zur unternehmensinternen »Visibilität« und ignorieren die Bedeutung der zweiten.
- Technisch überlegene Standards »vergessen« den Benutzer, dem beispielsweise zugemutet wird, ein Zertifikat in den Keystore seines E-Mail-Clients zu bringen, obwohl er doch nur sicher mailen will.

- Diskussionen um rechtliche Erfordernisse, die von sehr wenigen Dogmatikern beherrscht werden, die Einfluss auf die Politik und den Gesetzgeber nehmen (z. B. im deutschen SigG/SigV) und die selbst dann an ihren teuren Empfehlungen festhalten, wenn fast keiner diese nutzt und wenn sie unserer internationalen Wettbewerbsfähigkeit im Wege stehen. Man braucht sich nicht zu wundern, wenn die Standards in den verbreiteten Produkten dann von einzelnen, schnellen Herstellern geprägt und in internationale Normungsgremien (IETF, IEEE, PKCS) eingebracht werden, die kein Verständnis für inkompatible nationale Sonderwege haben. Ebenso wenig braucht man sich dann zu wundern, dass innerhalb von pragmatisch agierenden Zusammenschlüssen (wie der European Bridge-CA oder den virtuellen Behörden-Poststellen) die Sicherheit real deutlich erhöht wird mithilfe von fortgeschrittenen Zertifikaten (die zigmillionenfach im Einsatz sind), während die akkreditiert-qualifizierten »Sonderlocken« noch nicht einmal die 100.000 erreichten. Mit solchen über die EU-Direktive hinausgehenden akkreditiert-qualifizierten Signaturen (die zudem bei der Validierung das inkompatible »Kettenmodell« verlangen) erschwert man die Verbreitung der digitalen Signatur beträchtlich. Hier zeigt sich, dass man sehr genau spezifizieren sollte, für welche Fälle man Anforderungen aufstellt: So wenig, wie man für die allermeisten der im Alltag geschlossenen Verträge einen Notar braucht, so selten muss man bei elektronischen Verträgen vom Spezialfall des Anscheinsbeweises im Prozessfall ausgehen. Es geht nicht um »richtige« oder maximale Sicherheit, sondern um eine bessere!
- Gefährlich für die kritischen Infrastrukturen sind nicht einzelne Hacker, sondern rational handelnde und oft mafiamäßig/militärisch organisierte Angreifer, die auf Gewinn aus sind und meist zuerst den leichtesten/kostengünstigsten Weg für ihre modernen Raubzüge wählen. Das »Spiel« zwischen Cyber-Kriminellen und »guten« Cyber-Nutzern und ihren Verbündeten wird nicht enden. Dabei wird die Benutzerinteraktion (ermöglicht vom Softwareentwickler, aber getragen vom Verständnis und Mitwirken des Nutzers) immer zentral und schwierig bleiben.
- Und natürlich hat alles mehrere Seiten, so dass sich sicher auch Kritiker (und berechnete Einwände) an dieser bewusst überspitzt formulierten Kritik finden ...

### **Kryptografie in der Realität**

In der Realität hat Kryptografie inzwischen fast überall Einzug gehalten: von Pay-TV über Auto-Wegfahrsperre, Handy bis in jeden Webbrowser. Fast alle großen Unternehmen betreiben eigene PKIs, mit denen ihre Mitarbeiter sichere E-Mails versenden könnten, sich sicher in WLANs anmelden können oder sicher Dateien auf outgesourceten Servern verschlüsseln könn(t)en. Softwarehersteller

wie SAP statteten ihre Software mit generischen Schnittstellen wie der GSS-API aus, so dass die Kunden die Wahl haben, die Sicherheitsfunktionen wahlweise von PKI- oder Kerberos-basierten Systemen zu nutzen.

Kryptografie erwies sich dann als sicher und erfolgreich im Einsatz in Firmen und im Internet, wenn sie

- hohe Interoperabilität gewährleistete (keine Insellösungen),
- für die Benutzer (nahezu) transparent war (kein oder kaum Mehraufwand) und
- ausgereift war.

Eine weitere Voraussetzung war, dass Expertenwissen im Voraus genutzt wird, was Geld spart und Fehler vermeidet, die im Nachhinein aufwändig zu beheben sind: Das Management von Schlüsseln für Maschinen, Dienste, Personen und Infrastrukturen muss verstanden und geplant werden. Beispielsweise machen CAs mit Modullängen von 512 Bit keinen Sinn. Hier hat Microsoft im August 2012 mit seinem Security Advisory 2661254 gute Dienste geleistet (das entsprechende Windows-Update verhindert die Verwendung von Zertifikaten mit RSA-Schlüsseln von weniger als 1024 Bit Länge durch die MS-Krypto-API). Ein anderes Beispiel: Der Lebenszyklus von Schlüsseln muss Zertifikats-Renewal und Schlüsselverlust von vornherein berücksichtigen. Insbesondere kleineren Firmen, die kostenlose PKI-Software von Microsoft oder aus dem Open-Source-Bereich oder Managed PKIs von Trustcenter wie VeriSign nutzen (und damit die rein technische Seite abdecken), ist hier zu raten, Experten-Know-how kurzfristig in der Architektur-Phase einzukaufen.

Das erforderliche Expertenwissen ist inzwischen breiter vorhanden, da viele Lehrstühle IT-Sicherheitsexperten ausgebildet haben. Sowohl für diese neuen Kollegen als auch für alle, die Fragen zu diesem Thema haben, vermittelt das Buch von Klaus Schmeh einen hervorragenden Überblick. Insbesondere gefällt mir, dass es trotz seiner Breite auf einem ganz aktuellen Stand ist und dabei genau so weit in die Tiefe geht, dass man die Verfahren verstehen und einordnen kann und dass man Produkt- und Protokoll-Entscheidungen treffen kann. Imponiert hat mir insbesondere die klare und unaufgeregte Art der Darstellung im Kapitel zum Chiffren-Design. Hier lässt sich Experten-Know-how ohne Mathe und mit klarem Urteil prima nachvollziehen.

Im ausführlichen Literaturverzeichnis finden sich alle Originalpapiere, die auch die genaue Mathematik enthalten. Zusätzlich können Sie spielerisch einzelne Verfahren mit der im Buch erwähnten freien Lernsoftware CrypTool (in den Varianten CrypTool 1, CrypTool 2 und JavaCrypTool) ausprobieren.

Und zu Recht wird in diesem Buch unter den »wichtigsten weiterführenden Büchern« Ross Anderson mit *Security Engineering* aufgeführt, denn die praktischen Probleme sind oft verschieden von denen, über die theoretisch orientierte

Experten gerne diskutieren (z. B. das Ausnutzen von Paddingfehlern statt Angriffe mit differenzieller Kryptoanalyse, das Eindringen über Passwortraten und auf Anwendungsebene, das Nutzen der menschlichen Psychologie und immer stärker auch die Ökonomie der IT-Sicherheit und der Malware-Industrie). Beide Sichtweisen sind wichtig.

Aufgrund von Snowdens Whistleblowing ist zur Erkenntnis geworden, was vorher als Vermutung von Verschwörungstheoretikern abgetan wurde: Die NSA hört nahezu jede Kommunikation anlasslos ab und archiviert diese, die Kryptoverfahren werden sowohl bei der Standardisierung als auch bei der Implementierung geschwächt. Besondere Raffinesse zeigten NSA und GCHQ bei den Advanced-Persistent-Threat-Hacks mit der Spionage-Software Regis beispielsweise gegen Belgacom. Alle Betroffenen reagieren gleich: Sie untersuchen, finden nichts, aber haben als Ergebnis das Problem angeblich im Griff.

Eine weitere Erkenntnis, zu der uns Snowden verhalf: Die Schützer des Staates tendieren zu elektronischer Überwachung – und zeigen bei ihren eigentlichen Aufgaben erstaunlich geringen Erfolg und viel internes Kommunikations-Missmanagement. Die gute Nachricht: Die Mathematik der modernen Verfahren (wie AES, RSA mit richtiger Parametrisierung und Modulen von mindestens 2048 Bit Länge, SHA2) ist nicht geknackt; die NSA ist keine Macht mit Alien-Fähigkeiten, aber eine Macht, die wirklich groß und umfassend planen und handeln kann.

Wie alt das Thema Missbrauch von Überwachung schon ist, zeigt das folgende Zitat-Duo:

*Jeder neue Angriff auf die Privatsphäre wird mit einer allgegenwärtigen Kultur der Angst gerechtfertigt.*

John Twelve Hawks (aus den Anmerkungen zum zweiten Band der Traveler-Trilogie von 2005–2009)

*Ich behaupte, dass, wer immer in diesem Augenblick zittert, schuldig ist, denn die Unschuld hat von der öffentlichen Überwachung nichts zu befürchten.»*

Maximilien de Robespierre, 1794 im französischen Nationalkonvent, als Kritik an seinen staatlich verordneten Verhaftungen und Morden laut wurde

Auch diese Themen im Umfeld der Kryptografie werden in diesem Buch aktuell behandelt. Für die Zielgruppe der Nichtmathematiker ist es daher weiterhin das Kryptografie-Standardwerk im deutschsprachigen Raum, das nicht nur bei meinen Studenten als Einstieg sehr geschätzt wird.

Ich wünsche auch der 6. Auflage alles Gute.

Bernhard Esslinger

Januar 2016

# Inhaltsübersicht

## Teil 1

### Wozu Kryptografie?

1	Einleitung	3
2	Was ist Kryptografie und warum ist sie so wichtig?	9
3	Wie und vom wem Daten abgehört werden	17
4	Klassische symmetrische Verschlüsselung	39
5	Die Enigma und andere Verschlüsselungsmaschinen	61

## Teil 2

### Moderne Kryptografie

6	Der Data Encryption Standard	85
7	Chiffren-Design	97
8	Kryptoanalyse symmetrischer Verfahren	113
9	Symmetrische Verfahren, die vor dem AES entstanden sind	123
10	Der Advanced Encryption Standard (AES)	137
11	AES-Kandidaten	151
12	Symmetrische Verfahren, die nach dem AES entstanden sind	171
13	Asymmetrische Verschlüsselung	189
14	Digitale Signaturen	215
15	Weitere asymmetrische Krypto-Verfahren	225
16	Kryptografische Hashfunktionen	241
17	Weitere kryptografische Hashfunktionen	265

18	Weitere Anwendungen kryptografischer Hashfunktionen	281
19	Kryptografische Zufallsgeneratoren	293
20	Kryptoanalyse mit Quantencomputern und Post-Quanten-Kryptografie	311
21	Stromchiffren	319

### Teil 3

## Implementierung von Kryptografie

22	Real-World-Attacks	359
23	Standardisierung in der Kryptografie	389
24	Betriebsarten und Datenformatierung	409
25	Kryptografische Protokolle	427
26	Authentifizierung	447
27	Verteilte Authentifizierung	469
28	Krypto-Hardware und Krypto-Software	483
29	Management geheimer Schlüssel	505
30	Trusted Computing und Kryptografie	517
31	Kryptografische APIs	525
32	Evaluierung und Zertifizierung	537

### Teil 4

## Public-Key-Infrastrukturen

33	Public-Key-Infrastrukturen	561
34	Digitale Zertifikate	591
35	PKI-Prozesse im Detail	607
36	Spezielle Fragen beim Betrieb einer PKI	631
37	Beispiel-PKIs	649

### Teil 5

## Kryptografische Netzwerkprotokolle

38	Kryptografie im OSI-Modell	667
39	Kryptografie in OSI-Schicht 1	679
40	Krypto-Standards für OSI-Schicht 2	689

41	IPsec (Schicht 3)	709
42	TLS und DTLS (Schicht 4)	719
43	E-Mail-Verschlüsselung- und Signierung (Schicht 7)	731
44	Weitere Krypto-Protokolle der Anwendungsschicht	747
45	Digitales Bezahlen	771
46	Noch mehr Kryptografie in der Anwendungsschicht	785

## Teil 6

### Mehr über Kryptografie

47	Wo Sie mehr zum Thema erfahren	807
48	Kryptografisches Sammelsurium	821

## Anhang

	Bildnachweis	853
	Literatur	855
	Index	883



# Inhaltsverzeichnis

## Teil 1

### Wozu Kryptografie?

<b>1</b>	<b>Einleitung</b>	<b>3</b>
1.1	Kryptografie heute. . . . .	4
1.2	Die sechste Ausgabe . . . . .	5
1.2.1	Erste Ausgabe (1998) . . . . .	5
1.2.2	Zweite Ausgabe (2001) . . . . .	5
1.2.3	Dritte Ausgabe (2007) . . . . .	5
1.2.4	Vierte Ausgabe (2009) . . . . .	6
1.2.5	Fünfte Ausgabe (2013) . . . . .	6
1.2.6	Sechste Ausgabe (2015) . . . . .	6
1.3	Mein Bedauern, meine Bitten und mein Dank . . . . .	7
<b>2</b>	<b>Was ist Kryptografie und warum ist sie so wichtig?</b>	<b>9</b>
2.1	The Name of the Game . . . . .	9
2.1.1	Die kurze Antwort . . . . .	9
2.1.2	Die lange Antwort. . . . .	9
2.2	Die Kryptografie – ein wichtiges Teilgebiet . . . . .	11
2.3	Warum ist die Kryptografie so wichtig? . . . . .	12
2.3.1	Wirtschaftsspionage . . . . .	13
2.3.2	Kommerz im Netz. . . . .	13
2.3.3	Die Privatsphäre . . . . .	13
2.3.4	Technik und Infrastrukturen . . . . .	14
2.4	Anwendungen der Kryptografie. . . . .	14
2.5	Und wer zum Teufel ist Alice? . . . . .	15

<b>3</b>	<b>Wie und vom wem Daten abgehört werden</b>	<b>17</b>
3.1	Mallory am Übertragungsmedium . . . . .	17
3.1.1	Kupferkabel . . . . .	18
3.1.2	Glasfaser . . . . .	18
3.1.3	Drahtlose Datenübertragung . . . . .	19
3.1.4	Satellit . . . . .	19
3.2	Mallory am Gerät . . . . .	19
3.2.1	Netzkomponenten . . . . .	20
3.2.2	Mitlesen und Verändern von Dateien . . . . .	20
3.3	Mallory in Computernetzen . . . . .	20
3.3.1	Telefon . . . . .	20
3.3.2	LAN . . . . .	21
3.3.3	DSL . . . . .	22
3.3.4	Mobilfunk . . . . .	22
3.3.5	WLANs . . . . .	23
3.4	Mallory im Internet . . . . .	23
3.4.1	ARP-Spoofing . . . . .	23
3.4.2	Abhörangriffe auf Router . . . . .	24
3.4.3	IP-Spoofing . . . . .	24
3.4.4	DNS-Spoofing . . . . .	25
3.4.5	Mitlesen von E-Mails . . . . .	26
3.4.6	URL-Spoofing . . . . .	27
3.4.7	Abhören von Internettelefonie . . . . .	27
3.5	Ein paar Fälle aus der Praxis . . . . .	27
3.5.1	Mitgelesene E-Mails . . . . .	28
3.5.2	Abgehörte Telefonate . . . . .	29
3.6	Ist Kryptografie gefährlich? . . . . .	30
3.6.1	Nachteile einer Krypto-Beschränkung . . . . .	32
3.6.2	Vorteile einer Krypto-Beschränkung . . . . .	33
3.6.3	Fazit . . . . .	36
<b>4</b>	<b>Klassische symmetrische Verschlüsselung</b>	<b>39</b>
4.1	Symmetrische Verschlüsselung . . . . .	39
4.1.1	Kryptografische Fachbegriffe . . . . .	41
4.1.2	Angriffe auf Verschlüsselungsverfahren . . . . .	41
4.2	Monoalphabetische Substitutionschiffren . . . . .	42
4.2.1	Caesar-Chiffre . . . . .	43
4.2.2	Freie Buchstabensubstitution . . . . .	44
4.2.3	Homophone Chiffre . . . . .	45

4.2.4	Bigramm-Substitution . . . . .	47
4.2.5	Playfair-Chiffre . . . . .	48
4.2.6	Nomenklatoren und Wörter-Codes . . . . .	49
4.3	Polyalphabetische Substitutionschiffren . . . . .	50
4.3.1	Vigenère-Chiffre . . . . .	50
4.3.2	Vernam-Chiffre . . . . .	51
4.3.3	One-Time-Pad . . . . .	52
4.4	Permutationschiffren . . . . .	53
4.4.1	Kryptoanalyse von Permutationschiffren . . . . .	54
4.4.2	Bedeutung von Permutationschiffren . . . . .	55
4.5	Berühmte ungelöste Verschlüsselungen . . . . .	56
4.5.1	Das Voynich-Manuskript . . . . .	57
4.5.2	Der Zettel des Somerton-Manns . . . . .	57
4.5.3	Das Thouless-Kryptogramm . . . . .	58
4.5.4	Weitere ungelöste Rätsel . . . . .	59
<b>5</b>	<b>Die Enigma und andere Verschlüsselungsmaschinen</b>	<b>61</b>
5.1	Verschlüsselungswerkzeuge . . . . .	62
5.2	Rotorchiffren . . . . .	65
5.2.1	Heberns Rotormaschine . . . . .	65
5.2.2	Die Enigma . . . . .	66
5.2.3	Weitere Rotor-Chiffriermaschinen . . . . .	70
5.3	Weitere Verschlüsselungsmaschinen . . . . .	71
5.3.1	Die Kryha-Maschine . . . . .	71
5.3.2	Hagelin-Maschinen . . . . .	73
5.3.3	Die Purple . . . . .	75
5.3.4	Der Geheimschreiber . . . . .	77
5.3.5	Die Lorenz-Maschine . . . . .	79
5.3.6	Schlüsselgerät 41 (Hitler-Mühle) . . . . .	80

## Teil 2

### Moderne Kryptografie

<b>6</b>	<b>Der Data Encryption Standard</b>	<b>85</b>
6.1	DES-Grundlagen . . . . .	85
6.2	Funktionsweise des DES . . . . .	88
6.2.1	Die Rundenfunktion F . . . . .	89
6.2.2	Die Schlüsselaufbereitung des DES . . . . .	90
6.2.3	Entschlüsseln mit dem DES . . . . .	91

6.3	Sicherheit des DES . . . . .	91
6.3.1	Vollständige Schlüsselsuche . . . . .	91
6.3.2	Differenzielle und lineare Kryptoanalyse . . . . .	92
6.3.3	Schwache Schlüssel. . . . .	93
6.4	Triple-DES . . . . .	94
6.4.1	Doppel-DES . . . . .	94
6.4.2	Triple-DES . . . . .	95
6.5	DES-Fazit . . . . .	96
<b>7</b>	<b>Chiffren-Design</b>	<b>97</b>
7.1	Sicherheitsüberlegungen . . . . .	98
7.1.1	Mögliche Schwachstellen . . . . .	98
7.1.2	Sicherheit gegenüber speziellen Angriffen . . . . .	100
7.1.3	Die ideale Schlüssellänge . . . . .	101
7.1.4	Hintertüren . . . . .	103
7.2	Weitere Designkriterien . . . . .	105
7.3	Aufbau symmetrischer Verschlüsselungsverfahren . . . . .	105
7.3.1	Linearität . . . . .	107
7.3.2	Konfusion und Diffusion . . . . .	108
7.3.3	Rundenprinzip . . . . .	109
7.3.4	Schlüsselaufbereitung . . . . .	111
<b>8</b>	<b>Kryptoanalyse symmetrischer Verfahren</b>	<b>113</b>
8.1	Differenzielle Kryptoanalyse . . . . .	114
8.2	Lineare Kryptoanalyse . . . . .	118
8.3	Kryptoanalyse mit Quantencomputern . . . . .	120
8.4	Weitere Kryptoanalyse-Methoden . . . . .	120
<b>9</b>	<b>Symmetrische Verfahren, die vor dem AES entstanden sind</b>	<b>123</b>
9.1	RC2 und RC5. . . . .	123
9.1.1	RC2 . . . . .	124
9.1.2	RC5 . . . . .	126
9.2	Blowfish . . . . .	128
9.2.1	Funktionsweise von Blowfish . . . . .	129
9.2.2	Schlüsselaufbereitung von Blowfish . . . . .	129
9.2.3	Bewertung von Blowfish. . . . .	130
9.3	IDEA und IDEA NXT . . . . .	131
9.4	Skipjack . . . . .	132
9.5	TEA . . . . .	133
9.6	GOST . . . . .	134
9.7	Weitere symmetrische Verfahren . . . . .	135

<b>10</b>	<b>Der Advanced Encryption Standard (AES)</b>	<b>137</b>
10.1	Funktionsweise des AES	138
10.1.1	Rundenaufbau	139
10.1.2	Entschlüsselung mit dem AES	142
10.1.3	Schlüsselaufbereitung	142
10.2	Mathematische Betrachtung des AES	144
10.3	Sicherheit des AES	145
10.3.1	AES als algebraische Formel	146
10.3.2	Quadratische Kryptoanalyse	147
10.3.3	Biclique-Kryptoanalyse	148
10.3.4	Weitere Angriffe	148
10.4	Bewertung des AES	148
<b>11</b>	<b>AES-Kandidaten</b>	<b>151</b>
11.1	Serpent	151
11.1.1	Funktionsweise von Serpent	152
11.1.2	S-Box-Design	153
11.1.3	Schlüsselaufbereitung von Serpent	154
11.1.4	Bewertung von Serpent	155
11.2	Twofish	155
11.2.1	Funktionsweise von Twofish	156
11.2.2	Bewertung von Twofish	157
11.3	RC6	157
11.3.1	Funktionsweise von RC6	158
11.3.2	Schlüsselaufbereitung von RC6	159
11.3.3	Bewertung von RC6	160
11.4	MARS	160
11.5	SAFER	162
11.5.1	Funktionsweise von SAFER+	162
11.5.2	Schlüsselaufbereitung von SAFER+	164
11.5.3	Bewertung von SAFER+	165
11.6	CAST	165
11.7	MAGENTA	166
11.8	Die restlichen AES-Kandidaten	168
11.9	Fazit	169

<b>12</b>	<b>Symmetrische Verfahren, die nach dem AES entstanden sind</b>	<b>171</b>
12.1	MISTY1, KASUMI und Camellia . . . . .	171
12.1.1	MISTY1 . . . . .	172
12.1.2	KASUMI . . . . .	173
12.1.3	Camellia . . . . .	174
12.2	Chiasmus und Libelle . . . . .	175
12.2.1	Funktionsweise von Chiasmus . . . . .	175
12.2.2	Libelle . . . . .	176
12.3	CLEFIA . . . . .	176
12.3.1	Funktionsweise von CLEFIA . . . . .	177
12.3.2	Bewertung von CLEFIA . . . . .	178
12.4	Schlanke Verschlüsselungsverfahren . . . . .	178
12.4.1	SEA . . . . .	180
12.4.2	PRESENT . . . . .	182
12.4.3	Bewertung schlanker Verfahren . . . . .	183
12.5	Tweak-Verfahren . . . . .	184
12.5.1	Beispiele . . . . .	184
12.5.2	Threefish . . . . .	185
12.5.3	Bewertung von Tweak-Verfahren. . . . .	187
12.6	Weitere symmetrische Verschlüsselungsverfahren. . . . .	187
<b>13</b>	<b>Asymmetrische Verschlüsselung</b>	<b>189</b>
13.1	Ein bisschen Mathematik . . . . .	192
13.1.1	Modulo-Rechnen . . . . .	192
13.1.2	Einwegfunktionen und Falltürfunktionen. . . . .	198
13.2	Der Diffie-Hellman-Schlüsselaustausch. . . . .	199
13.2.1	Funktionsweise von Diffie-Hellman . . . . .	200
13.2.2	MQV . . . . .	202
13.3	RSA . . . . .	204
13.3.1	Funktionsweise des RSA-Verfahrens . . . . .	204
13.3.2	Ein Beispiel. . . . .	206
13.3.3	Sicherheit des RSA-Verfahrens . . . . .	206
13.3.4	RSA und der Chinesische Restsatz . . . . .	210
13.4	Symmetrisch und asymmetrisch im Zusammenspiel . . . . .	213
13.4.1	Unterschiede zwischen symmetrisch und asymmetrisch . . .	213
13.4.2	Hybridverfahren. . . . .	214

<b>14</b>	<b>Digitale Signaturen</b>	<b>215</b>
14.1	Was ist eine digitale Signatur? . . . . .	216
14.2	RSA als Signaturverfahren. . . . .	217
14.2.1	Funktionsweise . . . . .	217
14.2.2	Sicherheit von RSA-Signaturen . . . . .	217
14.3	Signaturen auf Basis des diskreten Logarithmus . . . . .	218
14.3.1	ElGamal-Verfahren . . . . .	219
14.3.2	DSA . . . . .	220
14.3.3	Weitere DLSSs. . . . .	223
14.4	Unterschiede zwischen DLSSs und RSA. . . . .	223
14.5	Weitere Signatur-Verfahren. . . . .	224
<b>15</b>	<b>Weitere asymmetrische Krypto-Verfahren</b>	<b>225</b>
15.1	Krypto-Systeme auf Basis elliptischer Kurven . . . . .	226
15.1.1	Elliptische Kurven . . . . .	226
15.1.2	ECC-Verfahren . . . . .	228
15.1.3	Die wichtigsten ECC-Verfahren . . . . .	229
15.1.4	Beispiel-Kurven . . . . .	230
15.1.5	Montgomery- und Edwards-Kurven . . . . .	230
15.2	NTRU . . . . .	232
15.2.1	Mathematische Grundlagen . . . . .	232
15.2.2	Funktionsweise von NTRU . . . . .	232
15.2.3	Bewertung von NTRU. . . . .	234
15.3	XTR . . . . .	234
15.4	Krypto-Systeme auf Basis hyperelliptischer Kurven . . . . .	235
15.5	HFE. . . . .	235
15.5.1	Mathematische Grundlagen . . . . .	236
15.5.2	Das Verfahren. . . . .	236
15.5.3	Bewertung von HFE . . . . .	237
15.6	McEliece-Verfahren. . . . .	238
15.7	Weitere asymmetrische Verfahren . . . . .	239
<b>16</b>	<b>Kryptografische Hashfunktionen</b>	<b>241</b>
16.1	Was ist eine kryptografische Hashfunktion? . . . . .	242
16.1.1	Nichtkryptografische Hashfunktionen . . . . .	242
16.1.2	Kryptografische Hashfunktionen. . . . .	243
16.1.3	Angriffe auf kryptografische Hashfunktionen . . . . .	244
16.2	SHA-1 . . . . .	252
16.2.1	Funktionsweise von SHA-1 . . . . .	252
16.2.2	Bewertung von SHA-1. . . . .	255

16.3	SHA-2	256
16.3.1	SHA-256	256
16.3.2	SHA-224	257
16.3.3	SHA-512	258
16.3.4	SHA-384	258
16.3.5	SHA-512/224 und SHA-512/256	258
16.3.6	Bewertung von SHA-2	258
16.4	MD4	259
16.5	MD5	259
16.6	RIPEND-160	260
16.6.1	Funktionsweise von RIPEND-160	261
16.6.2	Bewertung von RIPEND-160	263
<b>17</b>	<b>Weitere kryptografische Hashfunktionen</b>	<b>265</b>
17.1	Tiger	265
17.1.1	Funktionsweise von Tiger	266
17.1.2	Bewertung von Tiger	268
17.2	WHIRLPOOL	268
17.2.1	Funktionsweise von WHIRLPOOL	269
17.2.2	Das Verschlüsselungsverfahren W	269
17.2.3	Bewertung von WHIRLPOOL	270
17.3	SHA-3 (Keccak)	271
17.3.1	Funktionsweise von Keccak	273
17.4	Hashfunktionen aus Verschlüsselungsverfahren	276
17.4.1	Variante 1	277
17.4.2	Variante 2	277
17.4.3	Variante 3 und 4	278
17.4.4	Fazit	278
17.5	Hashfunktionen aus Tweak-Verfahren	279
17.6	Weitere kryptografische Hashfunktionen	279
<b>18</b>	<b>Weitere Anwendungen kryptografischer Hashfunktionen</b>	<b>281</b>
18.1	Schlüsselabhängige Hashfunktionen	281
18.1.1	Anwendungsbereiche schlüsselabhängiger Hashfunktionen	282
18.1.2	Die wichtigsten schlüsselabhängigen Hashfunktionen	283
18.1.3	Fazit	285
18.2	Hashbäume	285
18.3	Hash-Signaturverfahren	286
18.3.1	Lamport-Diffie-Einmal-Signaturverfahren	287
18.3.2	Merkle-Signaturverfahren	287
18.3.3	Bewertung von Hash-Signaturverfahren	288

18.4	Künstliche Verzögerungen durch Hashfunktionen . . . . .	289
18.5	Weitere Anwendungen kryptografischer Hashfunktionen . . . . .	290
<b>19</b>	<b>Kryptografische Zufallsgeneratoren</b>	<b>293</b>
19.1	Zufallszahlen in der Kryptografie . . . . .	294
19.1.1	Anforderungen der Kryptografie . . . . .	294
19.1.2	Echte Zufallsgeneratoren . . . . .	295
19.1.3	Pseudozufallsgeneratoren . . . . .	296
19.1.4	Die Grauzone zwischen echt und pseudo . . . . .	297
19.1.5	Mischen von Zufallsquellen . . . . .	297
19.2	Die wichtigsten Pseudozufallsgeneratoren . . . . .	298
19.2.1	Kryptografische Hashfunktionen als Fortschaltfunktion . . .	300
19.2.2	Schlüsselabhängige Hashfunktionen als Fortschaltfunktion.	302
19.2.3	Blockchiffren als Fortschaltfunktion . . . . .	304
19.2.4	Linear rückgekoppelte Schieberegister . . . . .	304
19.2.5	Nichtlinear rückgekoppelte Schieberegister . . . . .	306
19.2.6	Zahlentheoretische Pseudozufallsgeneratoren . . . . .	307
19.3	Primzahlgeneratoren . . . . .	308
<b>20</b>	<b>Kryptoanalyse mit Quantencomputern und Post-Quanten-Kryptografie</b>	<b>311</b>
20.1	Quantenmechanik . . . . .	312
20.1.1	Superpositionen . . . . .	312
20.1.2	Verschränkungen . . . . .	313
20.2	Quantencomputer . . . . .	313
20.3	Faktorisierung mit dem Shor-Algorithmus . . . . .	315
20.4	Vollständige Schlüsselsuche mit dem Grover-Algorithmus . . . . .	315
20.5	Wie realistisch sind Quantencomputer . . . . .	316
20.6	Post-Quanten-Kryptografie . . . . .	317
<b>21</b>	<b>Stromchiffren</b>	<b>319</b>
21.1	Aufbau und Eigenschaften von Stromchiffren . . . . .	320
21.1.1	Wie eine Stromchiffre funktioniert . . . . .	321
21.1.2	Angriffe auf Stromchiffren . . . . .	322
21.1.3	Stromchiffren und Blockchiffren im Vergleich . . . . .	322
21.2	RC4 . . . . .	324
21.2.1	Funktionsweise von RC4 . . . . .	324
21.2.2	Bewertung von RC4 . . . . .	325
21.3	A5 . . . . .	327
21.3.1	Funktionsweise von A5 . . . . .	327
21.3.2	Bewertung von A5 . . . . .	328

21.4	E0 . . . . .	329
21.4.1	Funktionsweise von E0 . . . . .	329
21.4.2	Bewertung von E0 . . . . .	332
21.5	Crypto1 . . . . .	333
21.5.1	Funktionsweise von Crypto1 . . . . .	334
21.5.2	Bewertung von Crypto1 . . . . .	334
21.6	Die Verfahren des eSTREAM-Wettbewerb . . . . .	335
21.6.1	HC-128 . . . . .	336
21.6.2	Rabbit . . . . .	338
21.6.3	Salsa20 . . . . .	342
21.6.4	Sosemanuk . . . . .	344
21.6.5	Trivium . . . . .	345
21.6.6	Grain . . . . .	347
21.6.7	MICKEY . . . . .	349
21.6.8	Erkenntnisse aus dem eSTREAM-Wettbewerb . . . . .	351
21.7	Spritz . . . . .	352
21.7.1	Funktionsweise von Spritz . . . . .	352
21.7.2	Bewertung von Spritz . . . . .	353
21.8	Snow 3G . . . . .	353
21.8.1	Funktionsweise von Snow 3G . . . . .	353
21.8.2	Bewertung von Snow 3G . . . . .	355
21.9	Weitere Stromchiffren . . . . .	355

## Teil 3

### Implementierung von Kryptografie

<b>22</b>	<b>Real-World-Attacken</b>	<b>359</b>
22.1	Seitenkanalangriffe . . . . .	359
22.1.1	Zeitangriffe . . . . .	360
22.1.2	Stromangriffe . . . . .	362
22.1.3	Fehlerangriffe . . . . .	364
22.1.4	Weitere Seitenkanalangriffe . . . . .	365
22.2	Malware-Angriffe . . . . .	365
22.2.1	Malware-Angriffe auf Schlüssel und Passwörter . . . . .	366
22.2.2	Malware-Angriffe auf digitale Signaturen . . . . .	367
22.2.3	Vom Entwickler eingebaute Hintertüren . . . . .	369
22.2.4	Gegenmaßnahmen . . . . .	370
22.3	Physikalische Angriffe . . . . .	371
22.3.1	Die wichtigsten physikalischen Angriffe . . . . .	371
22.3.2	Gegenmaßnahmen . . . . .	372

22.4	Schwachstellen durch Implementierungsfehler . . . . .	374
22.4.1	Implementierungsfehler in der Praxis . . . . .	374
22.4.2	Implementierungsfehler in vielen Variationen . . . . .	376
22.4.3	Gegenmaßnahmen. . . . .	377
22.5	Insiderangriffe . . . . .	379
22.5.1	Unterschätzte Insider. . . . .	380
22.5.2	Gegenmaßnahmen. . . . .	380
22.6	Der Anwender als Schwachstelle . . . . .	381
22.6.1	Schwachstellen durch Anwenderfehler . . . . .	382
22.6.2	Gegenmaßnahmen. . . . .	384
22.7	Fazit . . . . .	388
<b>23</b>	<b>Standardisierung in der Kryptografie</b>	<b>389</b>
23.1	Standards . . . . .	389
23.1.1	Standardisierungsgremien . . . . .	390
23.1.2	Standardisierung im Internet. . . . .	391
23.2	Wissenswertes zum Thema Standards . . . . .	391
23.3	Wichtige Kryptografie-Standards. . . . .	392
23.3.1	PKCS. . . . .	392
23.3.2	IEEE P1363. . . . .	393
23.3.3	ANSI X.9 . . . . .	394
23.3.4	NSA Suite B . . . . .	395
23.4	Standards für verschlüsselte und signierte Daten . . . . .	396
23.4.1	PKCS#7. . . . .	396
23.4.2	XML Signature und XML Encryption. . . . .	398
23.4.3	Weitere Formate . . . . .	400
23.5	Standardisierungswettbewerbe . . . . .	400
23.5.1	Der DES-Wettbewerb . . . . .	401
23.5.2	Der AES-Wettbewerb . . . . .	402
23.5.3	Der SHA-3-Wettbewerb . . . . .	405
23.5.4	Weitere Wettbewerbe . . . . .	406
<b>24</b>	<b>Betriebsarten und Datenformatierung</b>	<b>409</b>
24.1	Betriebsarten von Blockchiffren. . . . .	409
24.1.1	Electronic-Codebook-Modus . . . . .	410
24.1.2	Cipher-Block-Chaining-Modus . . . . .	412
24.1.3	Output-Feedback-Modus . . . . .	413
24.1.4	Cipher-Feedback-Modus. . . . .	414
24.1.5	Counter-Modus. . . . .	415
24.1.6	Fazit . . . . .	417

24.2	Betriebsarten von Tweak-Verfahren . . . . .	418
24.3	Formaterhaltende Verschlüsselung . . . . .	419
24.4	Datenformatierung für das RSA-Verfahren. . . . .	419
24.4.1	Der PKCS#1-Standard . . . . .	420
24.4.2	Datenformatierung für die RSA-Verschlüsselung . . . . .	420
24.4.3	Datenformatierung für RSA-Signaturen . . . . .	423
24.5	Datenformatierung für DLSSs. . . . .	425
<b>25</b>	<b>Kryptografische Protokolle</b>	<b>427</b>
25.1	Protokolle. . . . .	428
25.1.1	Konzeptprotokolle . . . . .	428
25.1.2	Netzwerkprotokolle . . . . .	429
25.1.3	Eigenschaften von Netzwerkprotokollen . . . . .	430
25.2	Protokolle in der Kryptografie . . . . .	432
25.2.1	Eigenschaften kryptografischer Netzwerkprotokolle . . . . .	432
25.3	Angriffe auf kryptografische Protokolle . . . . .	434
25.3.1	Replay-Attacke. . . . .	434
25.3.2	Spoofing-Attacke . . . . .	435
25.3.3	Man-in-the-Middle-Attacke . . . . .	435
25.3.4	Hijacking-Attacke . . . . .	437
25.3.5	Known-Key-Attacken. . . . .	437
25.3.6	Verkehrsflussanalyse . . . . .	440
25.3.7	Denial-of-Service-Attacke. . . . .	441
25.3.8	Sonstige Angriffe . . . . .	442
25.4	Beispielprotokolle. . . . .	442
25.4.1	Beispielprotokoll: Messgerät sendet an PC . . . . .	442
25.4.2	Weitere Beispielprotokolle . . . . .	445
<b>26</b>	<b>Authentifizierung</b>	<b>447</b>
26.1	Authentifizierung im Überblick. . . . .	447
26.1.1	Etwas, was man weiß. . . . .	449
26.1.2	Was man hat . . . . .	450
26.1.3	Was man ist . . . . .	451
26.2	Biometrische Authentifizierung. . . . .	451
26.2.1	Grundsätzliches zur biometrischen Authentifizierung. . . . .	451
26.2.2	Biometrische Merkmale . . . . .	453
26.2.3	Fazit. . . . .	457

26.3	Authentifizierung in Computernetzen . . . . .	457
26.3.1	Passwörter. . . . .	458
26.3.2	OTP-Tokens . . . . .	461
26.3.3	Authentifizierung mit asymmetrischen Verfahren . . . . .	464
26.3.4	Biometrie in Computernetzen . . . . .	467
<b>27</b>	<b>Verteilte Authentifizierung</b>	<b>469</b>
27.1	Authentifizierungs-Synchronisation . . . . .	470
27.2	Single Sign-on . . . . .	470
27.2.1	Lokales SSO . . . . .	471
27.2.2	Ticket-SSO . . . . .	472
27.3	Kerberos . . . . .	472
27.3.1	Vereinfachtes Kerberos-Protokoll . . . . .	473
27.3.2	Vollständiges Kerberos-Protokoll . . . . .	474
27.3.3	Vor- und Nachteile von Kerberos . . . . .	476
27.4	RADIUS und andere Triple-A-Server . . . . .	477
27.4.1	Triple-A-Server . . . . .	477
27.4.2	Beispiele für Triple-A-Server . . . . .	479
27.5	SAML . . . . .	479
27.5.1	Funktionsweise von SAML . . . . .	480
27.5.2	SAML in der Praxis. . . . .	481
<b>28</b>	<b>Krypto-Hardware und Krypto-Software</b>	<b>483</b>
28.1	Krypto-Hardware oder Krypto-Software? . . . . .	483
28.1.1	Pro Software . . . . .	484
28.1.2	Pro Hardware . . . . .	485
28.1.3	Ist Hardware oder Software besser? . . . . .	485
28.2	Smartcards . . . . .	486
28.2.1	Smartcards und andere Chipkarten . . . . .	486
28.2.2	Smartcard-Formfaktoren. . . . .	488
28.2.3	Smartcards und Kryptografie . . . . .	489
28.3	Hardware-Security-Module . . . . .	493
28.4	Kryptografie in eingebetteten Systemen . . . . .	494
28.4.1	Eingebettete Systeme und Kryptografie . . . . .	495
28.4.2	Kryptografische Herausforderungen in eingebetteten Systemen. 496	
28.5	RFID und Kryptografie . . . . .	498
28.5.1	Sicherheitsprobleme beim Einsatz von EPC-Chips . . . . .	499
28.5.2	RFID und Kryptografie . . . . .	501

<b>29</b>	<b>Management geheimer Schlüssel</b>	<b>505</b>
29.1	Schlüsselgenerierung . . . . .	506
29.2	Schlüsselspeicherung . . . . .	508
29.3	Schlüsselauthentifizierung . . . . .	509
29.4	Schlüsseltransport und Schlüssel-Backup . . . . .	509
29.5	Schlüsselaufteilung . . . . .	510
29.6	Schlüsselwechsel . . . . .	511
29.7	Löschen eines Schlüssels . . . . .	512
29.8	Key Recovery . . . . .	512
29.9	Quantenkryptografie . . . . .	513
29.9.1	Quanten-Schlüsselaustausch . . . . .	513
29.9.2	Bewertung der Quantenkryptografie . . . . .	515
<b>30</b>	<b>Trusted Computing und Kryptografie</b>	<b>517</b>
30.1	Trusted Computing . . . . .	517
30.2	Trusted Computing und Kryptografie . . . . .	519
30.3	Das Trusted Platform Module . . . . .	519
30.3.1	Bestandteile des TPM . . . . .	520
30.3.2	Schlüssel . . . . .	521
30.4	Funktionen und Anwendungen des TPM . . . . .	522
30.4.1	Fazit . . . . .	523
<b>31</b>	<b>Kryptografische APIs</b>	<b>525</b>
31.1	PKCS#11 . . . . .	525
31.1.1	Aufbau . . . . .	526
31.1.2	Rollenmodell . . . . .	527
31.1.3	Prozesse . . . . .	527
31.1.4	Bewertung von PKCS#11 . . . . .	528
31.2	MS-CAPI . . . . .	529
31.2.1	Aufbau . . . . .	529
31.2.2	Rollen . . . . .	530
31.2.3	Prozesse . . . . .	530
31.2.4	Bewertung der MS-CAPI . . . . .	531
31.3	Cryptography API Next Generation (CNG) . . . . .	531
31.4	TokenD . . . . .	531
31.5	ISO/IEC 24727 . . . . .	532