

iX Edition

# Kryptografie

Verfahren, Protokolle, Infrastrukturen

Bearbeitet von  
Klaus Schmeh

6., aktualisierte Auflage 2016. Buch. XL, 906 S. Hardcover

ISBN 978 3 86490 356 4

Format (B x L): 16,5 x 24 cm

[Weitere Fachgebiete > EDV, Informatik > Hardwaretechnische Grundlagen > Kryptographie, Datenverschlüsselung](#)

Zu [Leseprobe](#)

schnell und portofrei erhältlich bei

The logo for beck-shop.de features the text 'beck-shop.de' in a bold, red, sans-serif font. Above the 'i' in 'shop' are three red dots of varying sizes. Below the main text, the words 'DIE FACHBUCHHANDLUNG' are written in a smaller, red, all-caps, sans-serif font.

**beck-shop.de**  
DIE FACHBUCHHANDLUNG

Die Online-Fachbuchhandlung [beck-shop.de](http://beck-shop.de) ist spezialisiert auf Fachbücher, insbesondere Recht, Steuern und Wirtschaft. Im Sortiment finden Sie alle Medien (Bücher, Zeitschriften, CDs, eBooks, etc.) aller Verlage. Ergänzt wird das Programm durch Services wie Neuerscheinungsdienst oder Zusammenstellungen von Büchern zu Sonderpreisen. Der Shop führt mehr als 8 Millionen Produkte.

# 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