

## 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



Die Online-Fachbuchhandlung 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	<b>Einleitung</b>	3
2	<b>Was ist Kryptografie und warum ist sie so wichtig?</b>	9
3	<b>Wie und vom wem Daten abgehört werden</b>	17
4	<b>Klassische symmetrische Verschlüsselung</b>	39
5	<b>Die Enigma und andere Verschlüsselungsmaschinen</b>	61

## Teil 2

### Moderne Kryptografie

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

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

## Teil 6

### Mehr über Kryptografie

<b>47</b>	<b>Wo Sie mehr zum Thema erfahren</b>	<b>807</b>
<b>48</b>	<b>Kryptografisches Sammelsurium</b>	<b>821</b>

## Anhang

<b>Bildnachweis</b>	<b>853</b>
<b>Literatur</b>	<b>855</b>
<b>Index</b>	<b>883</b>