Inhaltsverzeichnis

Vorwort 7

Bezeichnungsweisen, Glossar 9

Klassischer Teil

Historische Chiffren und ihre Kryptoanalyse 13

Feistel-Netzwerk 18

Pseudozufallszahlen, rückgekoppelte Schieberegister 21

Entropie und Koinzidenzindex 24

Absolute Sicherheit und Unizitätsmaß 29

Visuelle Kryptographie 34

Komplexitätstheorie

Komplexitätsklassen, O-Notation 35

Einwegfunktionen 42

Hashing, Geburtstagsparadoxon 46

Effiziente Reduzierbarkeit 50

Algorithmische Zahlentheorie

Teilbarkeit, ggT, Euklid-Algorithmus 55

Primzahlen 59

Kongruenzen und Restklassen 62

Der Chinesische Restsatz und die Quadratwurzeln der 1 65

Die Euler-Funktion 69

Untergruppen und zyklische Gruppen 71

Primitivwurzeln und Diskreter Logarithmus 74

Bibliografische Informationen
http://d-nb.info/1026502497

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

Die Sätze von Euler und Fermat **76**

Pseudo-Primzahlen, Carmichael-Zahlen, Miller-Rabin-Test **78**

Quadratische Reste, Quadratwurzeln, Legendre- und Jacobi-Symbol **81**

Kryptoanalyse

Faktorisierungsalgorithmen **89**

Algorithmen für den Diskreten Logarithmus **96**

Kryptographische Protokolle

Nachrichten/Schlüssel-Austausch/Vereinbarung **99**

Public-Key-Systeme **102**

Signatur und Authentisierung **106**

Zero-Knowledge **109**

Elektronisches Bargeld **117**

Elliptische Kurven **121**

Anhang: Laufzeiten von Algorithmen **125**

Literatur **127**

Index **134**