
Literatur

1. Advanced Encryption Standard, <http://csrc.nist.gov/encryption/aes/>
2. M. Agrawal, N. Kayal, N. Saxena, Primes is in P, <http://www.cse.iitk.ac.in/news/primality.html>
3. A. Aho, J. Hopcroft, J. Ullman, *The Design and Analysis of Computer Algorithms* (Addison-Wesley, Reading, Massachusetts, 1974)
4. E. Bach, J. Shallit, *Algorithmic Number Theory* (MIT Press, Cambridge, Massachusetts and London, England, 1996)
5. F. Bauer, *Entzifferte Geheimnisse* (Springer, Berlin, 1995)
6. F. Bauer, *Decrypted Secrets* (Springer, Berlin, 2000)
7. M. Bellare, P. Rogaway, The exact security of digital signatures: How to sign with RSA and Rabin, in *Advances in Cryptology – EUROCRYPT '96* (Springer, 1996), S. 399–416
8. M. Bellare, P. Rogaway, Optimal asymmetric encryption – how to encrypt with RSA, in *Advances in Cryptology – EUROCRYPT '94* (Springer, 1996), S. 92–111
9. M. Bellare, R. Canetti, H. Krawczyk, Keying hash functions for message authentication, in *Advances in Cryptology – CRYPTO '96*, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18–22, 1996, S. 1–15
10. D.J. Bernstein, J. Buchmann, E. Dahmen (Hrsg.), *Post-Quantum Cryptography* (Springer, 2008)
11. D.J. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, L. Papachristodoulou, M. Schneider, P. Schwabe, Z. Wilcox-O’Hearn, SPHINCS: practical stateless hash-based signatures, in *Advances in Cryptology – EUROCRYPT 2015*, 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26–30, 2015, Proceedings, Part I, S. 368–397
12. A. Beutelspacher, J. Schwenk, K.-D. Wolfenstetter, *Moderne Verfahren der Kryptographie* (Vieweg, 1998)
13. E. Biham, A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard* (Springer, New York, 1993)
14. I.F. Blake, G. Seroussi, N.P. Smart, *Elliptic Curves in Cryptography* (Cambridge University Press, Cambridge, England, 1999)
15. D. Bleichenbacher, Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS#1, in *Advances in Cryptology – CRYPTO '98*, 1998, S. 1–12
16. D. Boneh, The decision Diffie-Hellman problem, in *ANTS III, Lecture Notes in Computer Science*, Bd. 1423, (Springer, Berlin, 1998), S. 48–63

17. D. Boneh, G. Durfee, Cryptanalysis of RSA with private keys d less than $N^{0.292}$, IEEE Transact. Inf. Theory **46**(4), 1339–1349 (2000)
18. J. Buchmann, Faktorisierung großer Zahlen. Spektrum Wiss. **9**, 80–88 (1996)
19. J. Buchmann, S. Paulus, A one way function based on ideal arithmetic in number fields, in *Advances in Cryptology – CRYPTO '97, Lecture Notes in Computer Science*, Bd. 1294, hrsg. von B. Kaliski (Springer, Berlin, 1997), S. 385–394
20. J. Buchmann, H.C. Williams, Quadratic fields and cryptography, in *Number Theory and Cryptography, London Mathematical Society Lecture Note Series*, Bd. 154, hrsg. von J.H. Loxton (Cambridge University Press, Cambridge, England, 1990), S. 9–25
21. J.A. Buchmann, E.G. Karatsiolis, A. Wiesmaier, *Introduction to Public Key Infrastructures* (Springer, 2013)
22. T.H. Cormen, C.E. Leiserson, R.L. Rivest, *Introduction to Algorithms* (MIT Press, Cambridge, Massachudetts, 1990)
23. R. Cramer, V. Shoup, Signature schemes based on the strong rsa assumption. ACM Transact. Inf. Syst. Theory **3**, 161–185 (2000)
24. N.G. de Bruijn, On the number of integers $\leq x$ and free of prime factors $> y$. Indag. Math. **38**, 239–247 (1966)
25. W. Diffie, M.E. Hellman, New directions in cryptography. IEEE-IT **IT-22**, 644–654 (1976)
26. Discrete Logarithm Records, https://en.wikipedia.org/wiki/Discrete_logarithm_records#Integers_modulo_p
27. Factoring records, <http://www.crypto-world.com/FactorRecords.html>
28. A. Fiat, M. Naor, Rigorous time/space trade offs for inverting functions, in *23rd ACM Symp. on Theory of Computing (STOC)* (ACM Press, 1991), S. 534–541
29. A. Fiat, A. Shamir, How to prove yourself: practical solutions to identification and signature problems, in *Advances in Cryptology – CRYPTO '86, Lecture Notes in Computer Science*, Bd. 263, hrsg. von A.M. Odlyzko (Springer, 1986), S. 186–194
30. FIPS 186-4, Digital Signature Standard (DSS). Federal Information Processing Standards Publication 186-4, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, 2013.
31. O. Goldreich, *Modern Cryptography, Probabilistic Proofs and Pseudorandomness* (Springer, New York, 1999)
32. S. Goldwasser, S. Micali, Probabilistic encryption. J. Comput. Syst. Sci. **28**, 270–299 (1984)
33. D.M. Gordon, A survey of fast exponentiation methods. J. Algorithms **27**, 129–146 (1998)
34. M. Hellman, A cryptanalytic time-memory trade-off. IEEE Transact. Inf. Theory **26**(4), 401–406 (1980)
35. P. Horster, *Kryptologie* (Bibliographisches Institut, 1987)
36. ISO/IEC 9796, Information technology – Security techniques – Digital signature scheme giving message recovery (International Organization for Standardization, Geneva, Switzerland, 1991)
37. D. Kahn, *The codebreakers* (Macmillan Publishing Company, 1967)
38. L.R. Knudsen, Contemporary block ciphers, in *Lectures on Data Security, LNCS*, Bd. 1561, hrsg. von I. Damgard (Springer-Verlag, New York, 1999), S. 105–126

39. D.E. Knuth, *The art of computer programming. Volume 2: Seminumerical algorithms* (Addison-Wesley, Reading, Massachusetts, 1981)
40. N. Koblitz, *A Course in Number Theory and Cryptography* (Springer, 1994)
41. L. Lamport, Constructing digital signatures from a one way function. Technical Report SRI-CSL-98, SRI International Computer Science Laboratory, 1979
42. A.K. Lenstra, H.W. Lenstra, Jr., Algorithms in number theory, in *Handbook of Theoretical Computer Science, Volume A, Algorithms and Complexity*, Kap. 12, hrsg. von J. van Leeuwen (Elsevier, Amsterdam, 1990)
43. A.K. Lenstra, H.W. Lenstra Jr., Algorithms in number theory, in *Handbook of Theoretical Computer Science. Volume A. Algorithms and Complexity*, Kap. 12, hrsg. von J. van Leeuwen (Elsevier, 1990), S. 673–715
44. A.K. Lenstra, H.W. Lenstra Jr. (Hrsg.), The Development of the Number Field Sieve, in *Lecture Notes in Math* (Springer, Berlin, 1993)
45. H.W. Lenstra, Jr., C. Pomerance, A rigorous time bound for factoring integers. *J. AMS* **5**, 483–516 (1992)
46. H.R. Lewis, C.H. Papadimitriou, *Elements of the Theory of Computation* (Prentice-Hall, Englewood Cliffs, NJ, 1981)
47. LiDIA, www.informatik.tu-darmstadt.de/TI/Welcome-Software.html
48. A. Menezes, *Elliptic Curve Public Key Cryptosystems* (Kluwer Academic Publishers, Dordrecht, 1993)
49. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography* (CRC Press, Boca Raton, Florida, 1997)
50. R.C. Merkle, A certified digital signature, in *CRYPTO '89: Proceedings on Advances in Cryptology, Lecture Notes in Computer Science*, Bd. 435 (Springer, 1989), S. 218–238
51. K. Meyberg, *Algebra Teil 1* (Carl Hanser, 1980)
52. K. Meyberg, *Algebra Teil 2* (Carl Hanser, 1980)
53. B. Möller, Improved techniques for fast exponentiation, in *Proceedings of ICISC 2002* (Springer, 2003)
54. E. Oeljeklaus, R. Remmert, *Lineare Algebra I* (Springer, Berlin, 1974)
55. J. Overbey, W. Traves, J. Wojdylo, On the key space of the hill cipher. *Cryptologia* **29**, 59–72 (2005)
56. PKCS#1, www.rsasecurity.com/rsalabs/pkcs/pkcs-1/index.html
57. D. Pointcheval, J. Stern, Security arguments for digital signatures and blind signatures. *J. Cryptol.* **13**, 361–396 (2000)
58. H. Riesel, *Prime Numbers and Computer Methods for Factorization* (Birkhäuser, Boston, 1994)
59. R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **21**, 120–126 (1978)
60. R. Rompel, One-way functions are necessary and sufficient for secure signatures, in *22nd ACM Symp. on Theory of Computing (STOC)*, 1990, S. 387–394
61. M. Rosing, *Implementing Elliptic Curve Cryptography* (Manning, 1999)
62. J. Rosser, L. Schoenfeld, Approximate formulas for some functions of prime numbers. *Illinois J. Math.* **6**, 64–94 (1962)

63. R.A. Rueppel, *Analysis and Design of Stream Ciphers* (Springer, Berlin, 1986)
64. O. Schirokauer, D. Weber, T. Denny, Discrete logarithms: the effectiveness of the index calculus method, in *ANTS II, Lecture Notes in Computer Science*, Bd. 1122, hrsg. von H. Cohen (Springer, Berlin, 1996)
65. B. Schneier, *Applied Cryptography*, 2. Aufl. (Wiley, New York, 1996)
66. C.P. Schnorr, Efficient signature generation by smart cards, in *Advances in Cryptology – CRYPTO '89*, Lecture Notes in Computer Science (Springer, 1991), S. 161–174
67. A. Shamir, How to share a secret. *Commun. ACM* **22**, 612–613 (1979)
68. C.E. Shannon, Communication theory of secrecy systems. *Bell Sys. Tech. J.* **28**, 656–715 (1949)
69. P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **26**, 1484–1509 (1997)
70. V. Shoup, OAEP reconsidered, in *Advances in Cryptology – CRYPTO 2001* (Springer, 2001), S. 239–259
71. D. Stinson, *Cryptography* (CRC Press, Boca Raton, Florida, 1995)
72. D. Stinson, *Cryptography, Theory and Practice*, 2. Aufl. (CRC Press, Boca Raton, Florida, 2002)
73. Yearly report on algorithms and key sizes, ICT-2007-216676 ECRYPT II, 2012

Sachverzeichnis

$\text{GF}(p^n)$, 64

Ω -Notation, 20

\mathbb{P} , 10

\mathbb{Z}_m , 83

$\lfloor \alpha \rfloor$, 2

$\overset{\$}{\leftarrow}$, 74

A

abelsch, 40

adaptiv, 129, 251

AddRoundKey, 146

Adjunkte, 107

affin linear, 108

affine Chiffre, 103

Algorithmus, 17

 deterministisch, 18

 polynomiell, 21

 probabilistisch, 18

 zustandsbehaftet, 18

Alphabet, 82

Angreifer

 aktiv, 80

 passiv, 80

Angriff

 Chosen-Ciphertext, 81

 Chosen-Message, 251

 Chosen-Plaintext, 80

 Known-Message, 251

 Known-Plaintext, 80

 Low-Exponent, 175

 No-Message, 250

anomale Kurve, 282

Archivierung, 300

assoziativ, 40

Authentisierungspfad, 266

Authentizität, 233, 245

Average-Case-Laufzeit, 22

B

Babysteps, 218

Berechnungsproblem, 22

(t, ε) -schwer, 23

 asymptotisch schwer, 24

 unlösbar, 23

beschränkt

 nach oben, 2

 nach unten, 2

Beweiser, 285

bijektiv, 49

binäre Länge, 7

Binärentwicklung, 6

Bit-Komplexität, 20

Bit-Operation, 20

Bitpermutation, 84

Blockchiffre, 85

 affin linear, 109

Blocklänge, 85

C

CA, 299

Caesar-Chiffre, 75

Carmichael-Zahl, 158

CBC-Mode, 90

CCA-Sicherheit, 131

CDH, 190

Certificate Revocation List, 302

Certification Authority, 299

CFB-Mode, 94

Challenge-Response-Verfahren, 287

Charakteristik, 64

Chiffre

 linear, 109

Chiffretext, 73

Chiffretextraum, 73, 167
Chinesischer Restsatz, 56
Chosen-Ciphertext-Angriff, 81
Chosen-Ciphertext-Sicherheit, 131, 186
Chosen-Message-Angriff, 251, 273
Chosen-Plaintext-Angriff, 80
Chosen-Plaintext-Sicherheit, 129, 184
Cipher, 146
Cipherblock-Chaining-Mode, 90
Cipher-Feedback-Mode, 94
Ciphertext-Only-Angriff, 79
Completeness, 288
Counter-Mode, 99
CPA-Sicherheit, 129, 184
CRL, 302
CTR-Mode, 99

D

Darstellungsproblem, 298
DDH, 190
Determinante, 106
differentielle Kryptoanalyse, 114
Diffie-Hellman-Problem, 190
 computational, 190
 decisional, 190
Diffie-Hellman-Schlüsselaustausch, 188
Diffie-Hellman-Tripel, 190
Diffusion, 111
digitale Signatur, 246
direktes Produkt, 57
diskreter Logarithmus, 188, 217
Diskriminante, 280
Division mit Rest, 5, 61, 62
DL-Problem, 217
Dreifach-Verschlüsselung, 86
DSA-Signatur, 261

E

ECB-Mode, 87
Eingabelänge, 20
Einheit, 42
Einheitengruppe, 42
Einmalpaßwort, 287
Einselement, 42
Einwegeigenschaft, 273
Einwegfunktion, 234
Electronic-Codebook-Mode, 87
elektronische Signatur, 246
Elementarereignis, 12
ElGamal

 Signatur, 257
 Verschlüsselung, 195
elliptische Kurve, 280
 anomale, 282
 supersinguläre, 282
endlicher Körper, 279
Entschlüsselungsalgorithmus, 73, 168
Enumerationsverfahren, 218
Ereignis, 13
 unabhängig, 14
Erfolgswahrscheinlichkeit, 19
Ergebnis, 12
Ergebnismenge, 12
Erwartungswert, 15
Erzeuger, 48
Eulersche φ -Funktion, 46
Eulersches Kriterium, 68
existentielle Fälschung, 243
exklusives Oder, 90
Experiment, 128

F

Faktorbasis, 228
Fälschung
 existentielle, 250
 selektive, 250
Feige-Fiat-Shamir-Protokoll, 290
Feistel-Chiffre, 135
Fermat-Test, 157
Fermat-Zahlen, 12
Fiat-Shamir-Identifikationsverfahren, 288
Funktion
 affin linear, 108
 linear, 108

G

g-adische Darstellung, 5
g-adische Entwicklung, 6
ganze Zahlen, 1
ganzzahlige Linearkombination, 8
gcd, 7
Geburtsangriff, 236
gemeinsamer Teiler, 7
Giantsteps, 219
glatte Zahlen, 209, 228
Gleichverteilung, 13
Grad, 60
größter gemeinsamer Teiler, 7
Gruppe, 41
 abelsch, 41

kommutativ, 41
zyklisch, 48
Gruppenordnung, 42

H

Halbgruppe, 40
Hashfunktion, 234
Hexadezimalentwicklung, 6
Hill-Chiffre, 110
HMAC, 242
Homorphismus, 58
Hybridverfahren, 166

I

Identifikation, 285
IND-CCA, 131, 186
IND-CPA, 184
Index einer Untergruppe, 50
Induktionsschritt, 3
Induktionsverankerung, 3
initiale Permutation, 137
Initialisierungsvektor, 91
injektiv, 49
Integrität, 75, 233, 235, 245
Inverses, 41
invertierbar, 41, 42
Isomorphismus, 58

K

Key
 private, 166
 public, 166
Klartext, 73, 167
Klartextraum, 73, 167
Known-Message-Angriff, 251
Known-Plaintext-Angriff, 80
Kollision, 235
kollisionsresistent, 235
 schwach, 235
 stark, 235
kommutativ, 40
Kompressionsfunktion, 234
Konfusion, 111
Kongruenz, 37
Konkatenation, 83
Körper, 43
Kryptosystem
 linear, 109
 Private-Key, 77
 Public-Key, 77, 167

symmetrisch, 73
Kürzungsregeln, 41

L

Lamport-Diffie-Einmal-Signaturverfahren, 247
Las-Vegas-Algorithmus, 18
Laufzeit, 20
 exponentiell, 21
 linear, 21
 quadratisch, 21
 quasi-linear, 21
 subexponentiell, 21
LD-OTS, 247
leere Folge, 83
Leitkoeffizient, 60
lineare Rekursion, 102
Low-Exponent-Angriff, 175

M

MAC, 241
MAC-Erzeugungsalgorithmus, 242
MAC-Raum, 241
Man-In-The-Middle-Attacke, 194
Matrix, 105
Mehrfachverschlüsselung, 86
Merkle-Hashbaum, 265
Merkle-Signaturverfahren, 264
Message-Authentication-Code, 241
Miller-Rabin-Test, 159
MixColumns, 146
Monoid, 41
Monom, 60
Monte-Carlo-Algorithmus, 18
Münzwurf, 18

N

Nachricht, 241, 246
Nachrichtenerweiterung, 197
Nachrichtenraum, 241, 246
natürliche Zahlen, 1
Nenner, 2
neutrales Element, 41
No-Message-Angriff, 250
No-Message-Modell, 276
Non-Malleability, 186
Nullstelle, 60
Nullteiler, 42

O

OAEP, 179

OFB-Mode, 96
 O-Notation, 20
 Orakel, 126
 Ordnung
 einer Gruppe, 42
 eines Gruppenelementes, 47
 OTP, 123
 Output-Feedback-Mode, 96

P

perfekt geheim, 121
 Permutation, 84
 Permutationschiffre, 86, 110
 persönliche Sicherheitsumgebung, 297
 Phishing-Angriff, 233
 PKCS# 1, 179
 PKI, 297
 Polynom, 59, 60
 irreduzibel, 64
 reduzibel, 64
 Potenz, 2
 Potenzgesetze, 40
 Potenzmenge, 13
 prime Restklasse, 44
 prime Restklassengruppe, 45
 Primfaktorzerlegung, 11
 Primitivwurzel, 67
 Primkörper, 64
 Primteiler, 10
 Primzahl, 10
 Probedivision, 156, 162
 Produkt, 1
 PSE, 297
 Software, 298
 Pseudoprimzahl, 158
 Public Key Infrastruktur, 297

Q

quadratische Form, 283
 quadratischer Nichtrest, 68
 quadratischer Rest, 68
 Quadratwurzeln mod p , 71
 Quotient, 2, 5, 62

R

Rabin
 Signatur, 256
 Verschlüsselung, 180
 Random-Oracle-Modell, 187, 272
 Redundanzfunktion, 254

reduziert, 5
 Registrierung, 299
 Relation, 229
 Rest, 5, 62
 absolut kleinster, 38
 kleinster nicht negativer, 38
 kleinster positiver, 38
 mod m , 38
 Restklasse, 38
 Restklassenring, 42
 Rijndael, 146
 Ring, 42
 kommutativ, 42
 nullteilerfrei, 42
 RSA
 Signatur, 251
 Verschlüsselung, 168
 RSA-Annahme, 187, 272
 stark, 273
 RSA-Modul, 169, 252
 RSA-OAEP, 179
 RSA-Problem, 187, 272
 RSA-PSS, 272
 rückgekoppeltes Schieberegister, 101
 Rückkopplungsfunktion, 102

S

Satz von Lagrange, 49
 S-Box, 147
 Schieberegister
 linear rückgekoppelt, 102
 rückgekoppelt, 101
 Schlüssel, 73
 öffentlicher, 167, 246
 öffentlicher, 166
 privater, 166, 167, 246
 Schlüsselerzeugung, 299
 Schlüsselerzeugungsalgorithmus, 73, 167, 246
 Schlüsselraum, 73, 167, 241, 246
 Schlüsseltext, 73, 167
 Schlüsseltextraum, 167
 Schranke
 obere, 2
 untere, 2
 schwach kollisionsresistent, 235
 schwacher DES-Schlüssel, 144
 Secret Sharing, 293
 semantische Sicherheit, 125, 186
 ShiftRows, 146

Sicherheit

- Chosen-Ciphertext, 131, 186
- Chosen-Plaintext, 129, 184
- semantische, 124, 125, 184, 186

Sicherheitslevel, 127**Sicherheitsreduktion, 187, 272****Sieb des Eratosthenes, 36****Signatur, 245, 246**

- aus Public-Key-Verfahren, 256
- DSA, 261
- ElGamal, 257
- gültig, 246
- mit Nachrichtengewinnung, 253
- Rabin, 256
- RSA, 251
- ungültig, 246

Signaturraum, 246**Signieralgorithmus, 246****Signierschlüssel, 246****simultane Kongruenz, 55****Sondness, 288****state, 146****String, 83****Stromchiffre, 100**

- asynchron, 101
- binär additiv, 100
- selbstsynchronisierend, 101
- synchron, 100

subexponentiell, 211**Substitutionschiffre, 85****Summe, 1****supersinguläre Kurve, 282****surjektiv, 49****T****teilbar, 43****Teilbarkeit, 4, 43****Teiler, 4, 43**

- gemeinsamer, 7
- größter gemeinsamer, 7

time-memory trade-off, 112**TLS, 286****Transkript, 289****Transport Layer Security, 286****Transposition, 117****Trapdoor-Permutation, 180****Triple DES, 135****Triple Encryption, 86****Turing-Maschine, 18****U****universelle Verifizierbarkeit, 245****Untergruppe, 48****V****Vandermonde Matrix, 294****Verifikationsalgorithmus, 242, 246****Verifikationsschlüssel, 246****Verifizierer, 285****Verknüpfung, 39****vernachlässigbar, 23****Vernam-One-Time-Pad, 123****Verschiebungsschiffre, 75****Verschlüsselung, 73****asymmetrisch, 76****DES, 135****ElGamal, 195****homomorphe, 201****hybrid, 76****kontextabhängig, 90****Private-Key, 77****Public-Key, 77****Rabin, 180****randomisiert, 198****RSA, 168****symmetrisch, 73****Triple DES, 135****Verschlüsselungsalgorithmus, 73, 167****Verschlüsselungsfunktion, 74****Verschlüsselungsmodus, 87****Verschlüsselungsverfahren****linear, 109****Public-Key, 167****Vertraulichkeit, 74****Vertretersystem, 38****Verzeichnisdienst, 301****Vielfaches, 4, 43****volles Restsystem, 38****vollständige Induktion, 3****vollständige Suche, 76, 79****Vorteil, 128, 130****Vorwärtssicherheit, 269****W****Wahrscheinlichkeit, 13****Wahrscheinlichkeitsverteilung, 13****Wahrscheinlichkeit****bedingte, 14****Worst-Case-Laufzeit, 20****Wort, 83**

Wörterbuchangriff, [286](#)

Z

Zahl

ganze, [1](#)

natürlich, [1](#)

rationale, [1](#)

reelle, [1](#)

Zähler, [2](#)

Zero-Knowledge-Beweise, [288](#)

Zero-Knowledge-Property, [289](#)

Zero-Knowledge-Protokoll

perfekt, [290](#)

Zertifikat, [300](#)

Zertifikatskette, [303](#)

Zertifizierung, [300](#)

Zertifizierungsstelle, [299](#)

Zeuge, [159](#)

Zirkuläre Shifts, [85](#)

Zufallsvariable, [15](#)

zusammengesetzt, [10](#)

Zustand, [18](#)