



Stichwortverzeichnis

Wolfgang Ertel

Angewandte Kryptographie

ISBN (Buch): 978-3-446-42756-3

ISBN (E-Book): 978-3-446-43196-6

Weitere Informationen oder Bestellungen unter

<http://www.hanser-fachbuch.de/978-3-446-42756-3>

sowie im Buchhandel.

Index

Symbole

⊕ 52, 174

⊗ 175

φ -Funktion, Eulersche 167

A

Additional-Decryption-Key 126

ADK 126, 130

Adleman, Leonard 79

Advanced-Encryption-Standard 68

AES 68, 99, 108, 113, 127, 136

Affine Chiffre 35

Algorithmus, randomisierter 179

Alice 25

Alphabet 21

Anderson, Ross 75

Angriff 26

Angriff mit gekauften Schlüssel 26

Angriff mit Gewalt 26

ANSI 60

approximate entropy 181

Arithmetik, modulare 159

asymmetrischer Algorithmus 22

AusweisApp-Software 135

Authentifikation 22, 100

Authentifikation, biometrische 114

Authentifizierung 22

Authentizität 91, 113

B

Babbage, Charles 40

BBS-Generator 181

Benutzerauthentifikation 100, 102, 112

berechenbar 98

Berechnungskomplexität 27

Betriebsmodi von Blockchiffren 74

Bigramme 36

Biham, Eli 75

binary symmetric source 179

Biometrische Verfahren 114

Bit-Commitment 141

blenden 88

Bletchley Park 48

blinde Signatur 141

blinde Signatur 16, 107

Blockchiffre 22, 59

Blowfish 75, 131

Bob 25

Bombe 49

Brute-Force-Angriff 26, 28, 48

BSI 110, 134

BSS 179

Bundesamt für Sicherheit in der
Informationstechnik 110, 134

C

CA 119, 125, 133

CBC 74

CBC-Modus 74, 113

Certification Authority 119, 125

CESG 77

Challenge-and-Response 102, 112, 132, 135

Chaum, David 15

Chiffretext 21

Chiffriermaschine 31, 45

Chinesischer Restsatz 81

Chipkarte 88, 103, 109, 115, 157

Chosen-Ciphertext-Angriff 26, 87

Chosen-Plaintext-Angriff 26

cipher block chaining 74

ciphertext 21

Ciphertext-Only-Angriff 26

Clipper-Chip 151

CMRK 126

COCOM 153

Codebuch 49

Colossus 49

Coppersmith, Don 75

Corporate-Message-Recovery-Key 126
CRYPTO 103

D

Daemen, Joan 69
Data-Encryption-Standard 59, 60
Datenkomplexität 27
decryption 21
DES 59, 113, 127, 132
DES40 132
differential power analysis 88
differentielle Kryptanalyse 67, 73
Diffie, Whitfield 91
Diffie-Hellman-Algorithmus 77, 91, 92, 94, 132, 136
Diffusion 59
Digicash 15
Digital Signature Algorithm 106, 124
Digital Signature Standard 107
digitale Signatur 97
Ding, Yan Zong 55
diskreter Logarithmus 92, 93
Divisionsrest 159
DPA 88
DSA 106, 124, 127, 131, 136
DSS 107

E

E-Mail signieren 108
E-Commerce 145
eBay 149
ECB 74
ECB-Modus 74
ECHELON 151
echte Zufallszahl 180
EES 151
EFF 60
Eingangsp permutation 61
Einweg-Hash-Funktion 74, 98, 99, 102, 132
Einwegfunktion 97, 98
electronic codebook 74
Electronic Commerce 15
Electronic Frontier Foundation 60
Electronic-Wallet 147
elektronische Münze 15
elektronische Signatur 111
elektronische Signatur, fortgeschrittene 111
elektronische Signatur, qualifizierte 112
elektronische Unterschrift 97
elektronisches Bargeld 24, 107, 139
ElGamal 77, 106, 127
ElGamal-Algorithmus 93

Elliptische Kurven, Kryptographie mit 93, 136
Emacs 124
encryption 21
Enigma 45
Entschlüsselung 21
Escrowed Encryption Standard 151
ETH 75
Euklidischer Algorithmus, erweiterter 35, 167
Eulersche φ -Funktion 167
Eve 79

F

FAR 114
Feistel, Horst 59
Feistel-Chiffre 59, 75
Fermatscher Satz 163
Fingerabdruck, kryptographischer 98
fingerprint 117, 119
Firewall 125
Fortezza 132
Friedman, William 43
Friedman-Test 40, 43
FRR 114
ftp 132

G

Galoiskörper 94
Galoistheorie 98
Geburts tagsangriff 100, 200
Geheimdienste 151
geheimer Schlüssel 24, 108
Geheimtext 21
Geldkarte 146
 $GF(2^8)$ 70, 75, 174
 $GF(2^n)$ 94
globale Deduktion 26
GNU Privacy Assistant 128
GNU Privacy Projekt 127
Gnu-Privacy-Guard 127
GnuPG 87, 127
GnuPP 127
GPA 128
Gruppe 94

H

Hammingabstand 66
Hash-Wert 98, 132
Hellman, Martin 91
Herausfordern und Antworten 102
Homophone Chiffre 37
HTTP-Verbindungen 132
hybride Verschlüsselung 123

I

IDEA 75, 131, 132
IDS 125
IETF 131
Inflation 147
Informationsdeduktion 26
Initialisierungsvektor 75
injektiv 21
Injektivität 21
Integrität 22, 113
Internet Engineering Task Force 131
Internet Mail Consortium 131
Internet-Pakete 133
intrusion detection system 125
IP 133
IP Security 133
IP-Tunneling 132
IPSec 133
ISO-Schichtenmodell 132
ITAR 153

K

Kasiski, Friedrich 40
Kasiski-Test 40
Kerkhoffs-Prinzip 23, 48, 147, 179
key-recovery 151
Key-Server 117
KISS 181
Klíma, Vlastimil 129
Klartext 21
klassische Chiffren 31
Known-Plaintext-Angriff 26, 49, 68
Knudsen, Lars 75
Knuth, Don 179
Kocher, Paul 87
Koinzidenzindex 43
Kolmogorov-Komplexität 180, 185
Konfusion 59
Kongruenz 159
Kryptanalyse 21, 40
Kryptographie 21
kryptographischer Algorithmus 15, 22
kryptographisches Protokoll 15, 24
Kryptologie 21
Kryptosystem 22
kubische Gleichung 103

L

Lai, Xuejia 75
Lawineneffekt 66
LDAP 121
LFSR 182

Lightweight Directory Access Protocol 121
linear feedback shift register 182
lineare Komplexität 185
lineare Kryptanalyse 73
linearer Kongruenzgenerator 181
lineares Schieberegister mit Rückkopplung 182
lokale Deduktion 26
LUCIFER 59

M

MAC 74, 113, 152
Macro-Payment 145
mailcrypt 124
Mallory 90
Man-in-the-Middle 90, 117
Man-in-the-Middle-Angriff 90
MARS 69, 75
Massey, James 75
Mauborgne, J. 52
Maurer, Ueli 56
MD4 99
MD5 99, 127, 132
Meet-in-the-Middle-Angriff 68, 76
message digest 99
Message-Authentication-Code 74, 113
Micro-Payment 15, 139, 145
Miller 172
modulare Arithmetik 31, 159
modulo 159
Mondex-System 147
monoalphabetisch 31
monoalphabetische Chiffre 31, 36
MPI-Format 130
multi-precision integer 130
Multimedia-Dokumente 97
Multiplikative Chiffre 33

N

Nachricht 21
National Institute of Standards and Technology 60
National Security Agency 60
Neumann, John von 185
Neumann-Filter 185
NFS 82
NIST 60, 99, 106, 151
nPA → Personalausweis, neuer
NSA 60, 77, 99, 106, 151
number field sieve 82

O

On-Card Matching 115

One-Time-Pad 52, 58, 73, 182, 184
 Online-Banking 97
 OpenPGP-Standard 127, 129, 131

P

padding 75
 passphrase 108, 132
 Passwort 108
 Passwortverschlüsselung 100
 PayPal 149
 Peggy 103
 Periodendauer 183
 Personalausweis, neuer 109, 121, 134
 Personalisierung 119
 PGP 87, 107, 111, 117, 120, 123
 PIN-Code 109, 115, 135
 PKCS 130
 PKI 117, 134
 plaintext 21
 Point-of-Sale-Händlerterminal 150
 polyalphabetisch 31
 Polyalphabetische Chiffre 37
 POSH 150
 Prüfsumme 113
 pretty good privacy 123
 PRNG 179
 Probabilistische Verschlüsselung 87
 Protokoll, kryptographisches 24
 pseudo random number generator 179
 Pseudozufallszahlengenerator 55, 74, 179, 181
 public key 24
 public key cryptography system 130
 Public-Key-Infrastruktur 91, 117, 130, 134
 Public-Key-Kryptographie 24, 77, 97
 Public-Key-System 120

Q

Quantenkryptographie 91
 Quantenschlüsseltausch 91

R

Rabin, Michael 55, 172
 RC2 75, 132
 RC4 132
 RC5 75
 RC6 69, 75
 real random number generator 180
 Reflektor 45
 relativ prim 167
 Replay-Angriff 102, 113
 Rest 159
 RFID Chip 134

Rijmen, Vincent 69
 Rijndael 69, 94
 RIPE-MD 99
 RIPEMD160 127
 Ritter, Terry 7
 Rivest, Ron 79, 151
 ROC-Kurve 114
 root-CA 120
 Rosa, Tomáš 129
 RRNG 180
 RSA 106, 127, 131, 132
 RSA-Algorithmus 77, 79, 94, 108, 170
 RSA-Algorithmus, Korrektheit 81
 RSA-Algorithmus, Sicherheit 82
 Rucksack-Algorithmus 77
 Runden 61

S

S-Box 75
 S-Box-Transformation 64
 S/MIME 117, 130
 Scherbius, Arthur 45
 Schieberegister 182
 Schlüssel 21, 23
 Schlüssel, öffentlicher 24
 Schlüssel, geheimer 24, 108
 Schlüssel, schwacher 64
 Schlüsselraum 29
 Schlüsselring 126
 Schlüsseltausch 89
 Schlüsseltauschproblem 24, 77
 Schlüsselwort 38
 Schlüsselwortlänge 40, 43
 Schlusspermutation 61
 Schneier, Bruce 60, 75
 schwacher Schlüssel 64
 Schwellenwertproblem, (m, n) 140, 143
 secret key 24
 Secret-Splitting 139, 143
 Secret-Splitting-Protokoll 141
 Secure Electronic Transactions 148
 secure shell 131
 Secure socket layer 132
 Secure-Hash-Algorithm 99
 Secure-Hash-Standard 102
 seed 179, 181
 Seed-Zahl 181
 Seiteneffekt 157
 Seiteneffekt, Angriff 87
 selbstinverse Abbildung 47
 Serpent 69, 75
 SET 145, 148

SHA 99, 102
SHA-1 99, 127, 132
Shamir, Adi 79
Shannon, Claude 59
SHS 102
sicherer Algorithmus 27
Sicherheitsschlüssel 27
Sieb des Eratosthenes 82
Signatur, blinde 107
Signatur, digitale 97
Signaturgesetz 97, 109, 135
simple power analysis 88
Speicherplatzbedarf 27
Spionage 49
Spruchschlüssel 50
SSH 131, 137
SSL 120, 132, 150
starke Kryptographie 23, 115
statistische Analyse 32
Steckbrett 45
Steganographie 21, 152
Stromchiffre 22, 52, 74, 184
Substitutionschiffre 31
symmetrischer Algorithmus 22

T

Tartaglia, Niccolò 103
Tauschchiffre 35
TCP/IP-Port 132
teilerfremd 167
thermisches Rauschen 54
TIGER/192 127
timing-attack 87
Transport Layer Security 132
Transpositionschiffre 31
Trent 89
Triple-DES 61, 68, 131, 132
Trojanerangriff 115, 157
Trojanisches Pferd (Angriff) 115, 157
Trustcenter 89, 117, 118, 125
Trustcenter, akkreditiertes 112
Tunneln 132
Turing 52
Turing, Alan 48
TWOFISH 127
Twofish 69, 75

U

U-Boot 48

uneingeschränkt sicherer Algorithmus 27
Unterschrift, elektronische 97

V

Verbindlichkeit 22
verborgene Parameter 180
Vernam, G. 52
Verschiebechiffre 31, 32
Verschlüsselung 21
Victor 103
Vigenère-Chiffre 38
Vigenère, Blaise de 38
Viren 120
virtual private networking 125, 133
Vollständiges Aufbrechen 26
von-Neumann-Rechner 54
VPN 125, 133

W

Wörterbuchangriff 100
wahrscheinliche Wörter, Methode 49
Walze 45
Walzenlage 50
Wassenaar Abkommen 153
Web-Browser 132
Web-of-Trust 120, 126
white card 146

X

X.509 130

Z

Zahlentheorie 159
Zahlkörpersieb 82, 89
Zeitstempel 119
zentralen Kreditausschuss 146
Zero-Knowledge-Beweis 103, 104, 113
Zero-Knowledge-Protokoll 102, 103
Zertifikat 118, 130
Zertifikatshierarchie 119
Zertifizierung 118
Zimmermann, Phil 123
ZKA 146
zufällig 179
Zufallsbitfolge, echte 53
Zufallszahl 179
Zustand 70
Zyklus 50