

Gilbert Brands

Verschlüsselungs- algorithmen

Angewandte Zahlentheorie rund
um Sicherheitsprotokolle

Inhaltsverzeichnis

1	Einleitung.....	1
2	Gruppentheorie, Primzahlen, Restklassen.....	8
2.1	Restklassenalgebra.....	9
2.2	Gruppentheorie.....	15
2.3	Primzahlen und prime Restklassen.....	24
2.4	Das Spektrum einer Restklassen-Gruppe.....	36
2.4.1	Das „potentielle“ Spektrum.....	37
2.4.2	Maximale Ordnung verschiedener Module.....	39
2.4.3	Das reale Spektrum.....	45
3	Anwendung in der Datenverschlüsselung.....	55
3.1	Einleitung.....	55
3.1.1	Rahmenbedingungen.....	55
3.1.2	Kodierung der Daten.....	57
3.1.3	Mathematische Basisoperationen symmetrischer Verfahren.....	63
3.2	Verschlüsselungsalgorithmen.....	65
3.2.1	Einwegverschlüsselung.....	65
3.2.1.1	Hash-Verfahren.....	68
3.2.1.2	Diskreter Logarithmus.....	73
3.2.2	Umkehrbare Verfahren.....	76
3.2.2.1	Symmetrische Verfahren.....	77
3.2.2.1.1	Data Encryption Standard, DES.....	77
3.2.2.1.2	Advanced Encryption Standard AES.....	82
3.2.2.2	Asymmetrische Verfahren mit öffentlichen Schlüsseln.....	87
3.2.2.2.1	RSA-Verschlüsselung.....	88
3.2.2.2.2	Algorithmen auf Basis des Diskreten Logarithmus.....	92
3.3	Sicherheitsprotokolle.....	94
3.3.1	Individueller vertraulicher Nachrichtenaustausch.....	96
3.3.2	Identitätsfeststellung der Partner (Authentifizierung).....	101
3.3.3	Elektronische Unterschriften.....	106
3.3.4	Unwiderrufbare geheime Unterschriften.....	110
3.3.5	Unterschrift durch eine Gruppe von Signatarausstellern.....	118
3.3.6	Gesicherte Anmeldeverfahren.....	130
3.3.7	Elektronisches Geld.....	139
3.4	Abschließende Betrachtungen zu Sicherheitsprotokollen.....	142
3.5	Spektrum und Sicherheit.....	144
4	Eigenschaften von Primzahlen.....	149
4.1	Primzahlhäufigkeiten.....	149
4.1.1	Der Primzahlsatz.....	149
4.1.2	Dichte und Verteilung von Primzahlen.....	158
4.2	Identifizierung von Primzahlen.....	166
4.2.1	Zufallzahlen und Pseudozufallzahlen.....	166
4.2.2	Prüfverfahren zur Feststellung der Primzahleigenschaft.....	179

VIU

4.3 Sichere Primzahlen.....	196
4.4 Parameterprüfung in Sicherheitsprotokollen.....	204
5 Faktorisierungsverfahren.....	218
5.1 Der Fermat'sche Algorithmus.....	219
5.2 Pollard's p - und $(p-1)$ -Algorithmus.....	223
5.3 Quadratisches Sieb.....	228
5.3.1 Der methodische Ansatz.....	229
5.3.2 Primzahlbasis.....	233
5.3.2.1 Elemente in der Basis.....	233
5.3.2.2 Untersuchungen zur Basisgröße.....	238
5.3.3 Quadratische Reste.....	250
5.3.3.1 Lucas-Folgen.....	250
5.3.3.2 Berechnung quadratischer Reste.....	257
5.3.4 Siebung und vollständige Faktorisierung.....	259
5.3.5 Lösung des linearen Gleichungssystems.....	266
5.4 Quadratisches Sieb für große Zahlen.....	269
5.4.1 Relationenklassen: große Restfaktoren.....	269
5.4.2 Multi-Polynomialales Sieb.....	276
6 Ein kurzer Blick auf andere Gebiete.....	282
6.1 Diskreter Logarithmus.....	282
6.2 Elliptische Funktionen.....	285
6.3 Neue Algorithmen und neue Hardware.....	291
Literaturverzeichnis.....	298
Stichwortverzeichnis.....	299