

1	Ziele der Kryptographie	1
1.1	Geheimhaltung	1
1.2	Authentifikation	2
1.3	Anonymität	4
1.4	Protokolle	5
	Literatur	6
2	Kryptologische Grundlagen	7
2.1	Symmetrische Verschlüsselung	7
2.2	Asymmetrische Verschlüsselung	12
2.3	Einwegfunktionen	14
2.4	Kryptographische Hashfunktionen	16
2.5	Message Authentication Codes	17
2.6	Authenticated Encryption	18
2.7	Trapdoor-Einwegfunktionen	18
2.8	Commitment und Bit-Commitment	19
2.9	Digitale Signatur	21
2.10	Der RSA-Algorithmus	23
	Literatur	30
3	Grundlegende Protokolle	33
3.1	Passwortverfahren (Festcodes)	34
3.2	Wechselcodeverfahren	35
3.3	Challenge-and-Response	38

3.4	Diffie-Hellman-Schlüsselvereinbarung	39
3.5	Das ElGamal-Verschlüsselungsverfahren	42
3.6	Das ElGamal-Signaturverfahren	43
3.7	Shamirs No-Key-Protokoll	45
3.8	Knobeln übers Telefon	48
3.9	Blinde Signaturen	50
	Literatur	52
4	Zero-Knowledge-Verfahren	55
4.1	Interaktive Beweise	55
4.2	Zero-Knowledge-Verfahren	61
4.3	Alle Probleme in NP besitzen einen Zero-Knowledge-Beweis	71
4.4	Es ist besser, zwei Verdächtige zu verhören	75
4.5	Witness Hiding	79
4.6	Honest Verifier Zero-Knowledge	84
4.7	Die Fiat-Shamir-Heuristik	88
	Literatur	90
5	Multiparty Computations	93
5.1	Secret Sharing Schemes	93
5.2	Wer verdient mehr?	97
5.3	Skatspielen übers Telefon	100
5.4	Secure Circuit Evaluation	104
5.5	Wie kann man sich vor einem allwissenden Orakel schützen?	109
5.6	Homomorphe Verschlüsselung	110
	Literatur	113
6	Anonymität	115
6.1	Das Dining-Cryptographers-Protokoll	115
6.2	MIXe	119
6.3	Elektronische Münzen	121
6.4	Elektronische Wahlen	123
6.5	Das Tor-Netzwerk	128
	Literatur	130
7	Vermischtes	133
7.1	Schlüsselmanagement durch Trusted Third Parties	133
7.2	Angriffe auf Protokolle	141

7.3	Oblivious Transfer	146
7.4	Quantenkryptographie	156
7.5	Blockchains und Kryptowährungen	160
	Literatur	164
8	Pairing-basierte Kryptosysteme	167
8.1	Elliptische Kurven in der Kryptographie	167
8.2	Die Gap-DH-Annahme	169
8.3	Bilineare Abbildungen	171
8.4	Neue Signaturverfahren	172
8.5	Identitätsbasierte Kryptographie	173
8.6	Generischer Einsatz von bilinearen Abbildungen	174
	Literatur	174
9	Mathematische Grundlagen	175
9.1	Natürliche Zahlen	175
9.2	Modulare Arithmetik	179
9.3	Quadratische Reste	184
9.4	Der diskrete Logarithmus	187
9.5	Isomorphie von Graphen	191
9.6	Der Zufall in der Kryptographie	193
9.7	Komplexitätstheorie	195
9.8	Große Zahlen	198
	Literatur	199
	Stichwortverzeichnis	201