

Inhaltsverzeichnis

Vorwort.....	V
1 Ziele der Kryptographie	1
1.1 Geheimhaltung.....	1
1.2 Authentikation	2
1.3 Anonymität	3
1.4 Protokolle	4
2 Kryptologische Grundlagen	6
2.1 Verschlüsselung	6
2.2 Asymmetrische Verschlüsselung	10
2.3 Einwegfunktionen	12
2.4 Kryptographische Hashfunktionen	13
2.5 Trapdoor-Einwegfunktionen	14
2.6 Commitment und Bit-Commitment	15
2.7 Digitale Signatur	16
2.8 Der RSA-Algorithmus	19
3 Grundlegende Protokolle	23
3.1 Passwortverfahren (Festcodes)	23
3.2 Wechselcodeverfahren	25
3.3 Challenge-and-Response	26
3.4 Diffie-Hellman-Schlüsselvereinbarung	28
3.5 Das ElGamal-Verschlüsselungsverfahren	30
3.6 Das ElGamal-Signaturverfahren	31
3.7 Shamirs No-Key-Protokoll	32
3.8 Knobeln übers Telefon	34
3.9 Blinde Signaturen	36
4 Zero-Knowledge-Verfahren	39
4.1 Interaktive Beweise	39
4.2 Zero-Knowledge-Verfahren	43
4.3 Alle Probleme in NP besitzen einen Zero-Knowledge-Beweis	51
4.4 Es ist besser, zwei Verdächtige zu verhören	55
4.5 Witness Hiding	58
4.6 Nichtinteraktive Zero-Knowledge-Beweise	62
4.7 Das Random Oracle-Modell	67

5 Multiparty Computations	70
5.1 Secret Sharing Schemes	70
5.2 Wer verdient mehr?	73
5.3 Skatspielen übers Telefon	76
5.4 Secure Circuit Evaluation	79
5.5 Wie kann man sich vor einem allwissenden Orakel schützen?	83
6 Anonymität	85
6.1 Das Dining-Cryptographers-Protokoll	85
6.2 MIXe	87
6.3 Elektronische Münzen	89
6.4 Elektronische Wahlen	91
7 Vermischtes	96
7.1 Schlüsselmanagement durch Trusted Third Parties	96
7.2 Angriffe auf Protokolle	102
7.3 Oblivious Transfer	108
7.4 Quantenkryptographie	116
8 Mathematische Grundlagen	119
8.1 Natürliche Zahlen	119
8.2 Modulare Arithmetik	122
8.3 Quadratische Reste	126
8.4 Der diskrete Logarithmus	128
8.5 Isomorphie von Graphen	131
8.6 Der Zufall in der Kryptographie	133
8.7 Komplexitätstheorie	135
8.8 Große Zahlen	137
Literaturverzeichnis	139
Stichwortverzeichnis	146