
Inhaltsverzeichnis

1	Einleitung	1
1.1	Ziele der Kryptographie	5
1.2	Einfache Kryptosysteme	7
1.2.1	Die Cäsar-Chiffre	7
1.2.2	Die Vigenère-Chiffre	9
	Aufgaben	13
2	Theorie der Kryptosysteme	15
2.1	Was ist Information?	15
2.2	Absolute Sicherheit	21
	Aufgaben	23
3	Angriff und Verteidigung	25
3.1	Anwendung der Informationstheorie	25
3.2	Abweichungen von der Gleichverteilung	27
3.3	Pseudozufallszahlen	31
3.4	Mehrfache Verschlüsselung	34
3.4.1	Der Friedman-Angriff	38
	Aufgaben	42
4	Geteilte Geheimnisse	45
4.1	Kombinatorik	48
4.2	Codierungstheorie	60
4.3	Optimierung	74
	Aufgaben	83
5	Täuschen und Verbergen	85
5.1	Die Geschichte der Steganographie	85
5.2	Moderne Verfahren der Steganographie	86
5.3	Visuelle Kryptographie und Steganographie	89
	Aufgaben	99

6	Von Betrügern und anderen unangenehmen Zeitgenossen ..	101
6.1	Betrüger	101
6.2	... und Störer	104
6.3	Betrugssichere Systeme.....	105
	Aufgaben	109
7	Von Graustufen und Farben	111
7.1	Darf's auch etwas Farbe sein?	111
7.2	Farbmodelle	113
7.3	Farbige visuelle Kryptographie	116
	Aufgaben	124
	Lösungen	129
	Materialien zum Buch	159
	Literaturverzeichnis	163
	Sachverzeichnis	165