

Inhaltsverzeichnis

I	Einleitung	1
II	Anforderungen an die Bildung für die Kommunikations- und Wissensgesellschaft ..	7
1	Allgemeine Überlegungen	7
1.1	Veränderungen auf dem Weg in die Kommunikations- und Wissensgesellschaft	7
1.2	Bildung in der Kommunikations- und Wissensgesellschaft	10
2	Aspekte der Kommunikations- und Wissensgesellschaft im Spiegel der Bildungspläne gestern und heute	13
2.1	Entwicklung informatischer Inhalte am Beispiel von Baden-Württemberg	13
2.1.1	Verschiedene bildungstheoretische Ansätze der informatischen Bildung	13
2.1.2	Lehrplan von 1977	17
2.1.3	Bildungsplan von 1984	19
2.1.4	Bildungsplan von 1994	22
2.1.5	Bildungsplan von 2004	27
2.1.6	Codes in den Lehr- und Bildungsplänen von 1977 – 2004	37
2.1.7	Kryptologie in den Lehr- und Bildungsplänen von 1977 – 2004	39
2.2	Vergleich informatischer Inhalte aller Bundesländer	42
2.2.1	Kurze Charakteristik der informatischen Bildung in jedem Bundesland	42
2.2.2	Gesamtübersicht der untersuchten Kriterien	50
III	Begriffliche Grundlagen	55
1	Zum Begriff der Codierung	55
1.1	Terminologie der Codierung	55
1.2	Verwendungszwecke von Codes	58
2	Kryptologie und Steganografie	60
2.1	Terminologie der Kryptologie	60
2.2	Klassifikation kryptografischer Verfahren	64
2.3	Grundlegende Methoden der Kryptoanalyse	67
2.4	Charakterisierung der Steganografie	70

IV Bildungsrelevanz codierungstheoretischer und kryptologischer Inhalte unter besonderer Berücksichtigung der Allgemeinbildung und des genetischen Prinzips	75
1 Aus der Perspektive der Allgemeinbildung	75
1.1 Allgemeinbildung im Sinne von Klafki	75
1.2 Allgemeinbildung im Sinne von Heymann	77
2 Das genetische Prinzip	81
2.1 Allgemeine Betrachtungen	81
2.2 Das genetische Prinzip in der Mathematikdidaktik	86
3 Historische Entwicklung: Verschlüsselung und Codierungen von der Antike bis zur Moderne	95
3.1 Die Anfänge in der Antike	96
3.2 Von der römischen Antike bis zum Ende des Mittelalters	108
3.3 Von der Renaissance bis zur Moderne	111
3.4 Die Moderne	148
V Bildungsrelevanz codierungstheoretischer und kryptologischer Inhalte unter besonderer Berücksichtigung weiterer fundamentaler Ideen	157
1 Perspektive der Didaktik der Mathematik	157
1.1 Allgemeinbildender Charakter der Mathematik	157
1.2 Fundamentale Ideen der Mathematik	160
1.3 Codierung und Kryptologie im Spiegel der fundamentalen Ideen der Mathematik	175
1.3.1 Algorithmus	175
1.3.2 Funktionaler Zusammenhang	181
1.3.3 Mathematisches Modellieren	193
1.3.4 Zahl	196
1.3.5 Messen	204
1.3.6 Ordnen	209
2 Perspektive der Informatik	213
2.1 Entwicklungen der fundamentalen Ideen der Informatik	213
2.2 Codierung und Kryptologie im Spiegel der fundamentalen Ideen der Informatik	219

VI Konkrete codierungstheoretische und kryptologische Verfahren aus fachdidaktischer Perspektive	223
1 Codierverfahren	223
1.1 Gemeinsame Bezüge aller ausgewählter Verfahren zu den fundamentalen Ideen der Mathematik und Informatik	224
1.2 Blindenschrift	227
1.3 Flaggenalphabet	232
1.4 ASCII-Code	235
1.5 Strichcodes (EAN bzw. ISBN)	237
1.6 Huffman-Codierung	248
2 Kryptologische Verfahren geordnet nach Verfahrenstypen	259
2.1 Auswahl der kryptologischen Verfahren	259
2.2 Transpositionsverfahren	261
2.2.1 Skytale	261
2.2.2 Fleissner-Schablone	265
2.3 Substitutionsverfahren	279
2.3.1 Monoalphabetische Verschlüsselungen	279
2.3.2 Homophone Verschlüsselungen	284
2.3.3 Polyalphabetische Verfahren	286
2.4 Asymmetrische Verfahren	293
2.4.1 Schlüsselaustauschverfahren nach Diffie-Hellman	293
2.4.2 Verfahren nach El Gamal	298
2.4.3 RSA-Verfahren	303
VII Resümee und fachdidaktische Konsequenzen	307
Literaturverzeichnis	315
Anhang	339