
Contents

1	Data Compaction	5
1.1	Entropy Coding	5
1.1.1	Discrete Sources and Their Entropy	5
1.1.2	Towards Huffman Coding	10
1.1.3	Arithmetic Coding	32
1.2	Universal Codes: The Example LZW	43
1.2.1	LZW Coding	43
1.2.2	The LZW Decoder	45
2	Cryptography	49
2.1	The Data Encryption Standard	50
2.1.1	The DES Scheme	50
2.1.2	The Cipher DES in Detail	53
2.2	The Advanced Encryption Standard: The Cipher Rijndael	60
2.2.1	Some Elementary Arithmetic	60
2.2.2	Specification of Rijndael	77
2.2.3	The Key Schedule	86
2.2.4	Decryption with Rijndael	92
2.3	The Public Key Paradigm and the Cryptosystem RSA	93
2.3.1	Encryption and Decryption via Exponentiation	93
2.3.2	The Cryptosystem RSA	97
2.4	Digital Signatures	101
2.4.1	Message Digests via SHA-1	101
2.4.2	DSA: Digital Signature Algorithm	112
2.4.3	Auxiliary Algorithms for DSA	116
2.4.4	The Signature Algorithm rDSA	122
2.4.5	ECDSA – Elliptic Curve Digital Signatures	125
3	Information Theory and Signal Theory: Sampling and Reconstruction	171
3.1	The Discrete Fourier Transform	172

VI Contents

3.1.1	Basic Properties	172
3.1.2	The Fast Fourier Transform Algorithm	183
3.2	Trigonometric Interpolation	190
3.2.1	Trigonometric Polynomials	191
3.2.2	Sampling and Reconstruction	193
3.3	The Whittaker–Shannon Theorem	198
3.3.1	Fourier Series	198
3.3.2	The Whittaker–Shannon Theorem for Elementary Periodic Functions	203
3.3.3	The (Continuous) Fourier Transform: A Sketch	209
3.3.4	The Sampling Theorem	214
4	Error Control Codes	221
4.1	The Reed–Solomon Codes	221
4.1.1	Preliminaries: Polynomial Codes	221
4.1.2	Reed–Solomon Codes	225
4.2	Convolutional Codes	239
4.2.1	Encoding: Digital Filtering in Binary Arithmetic	239
4.2.2	Decoding: The Viterbi Method	253
5	Data Reduction: Lossy Compression	267
5.1	DFT, Passband Filtering and Digital Filtering	268
5.2	The Discrete Cosine Transform	274
5.2.1	Functional Description of the DCT	275
5.2.2	The 2D DCT	293
5.2.3	The Karhunen–Loève Transform and the DCT	305
5.3	Filter Banks and Discrete Wavelet Transform	314
5.3.1	Two Channel Filter Banks	314
5.3.2	The Discrete Wavelet Transform	372
	References	435
	Index	439



<http://www.springer.com/978-3-540-33218-3>

Algorithmic Information Theory
Mathematics of Digital Information Processing
Seibt, P.
2006, VI, 443 p., Hardcover
ISBN: 978-3-540-33218-3