

Contents

1	Signals and Systems — 1
1.1	Communication System — 1
1.2	Data and Signals — 3
1.2.1	Representation of Signals — 7
1.2.2	Harmonic Analysis of Periodic Signals — 11
1.2.3	Harmonic Analysis of Aperiodic Signals — 20
1.2.4	Correlation and Convolution — 22
1.2.4.1	Correlation of Periodic Signals — 23
1.2.4.2	Convolution of Periodic Signals — 26
1.2.4.3	Correlation of Aperiodic Signals — 28
1.2.4.4	Convolution of Aperiodic Signals — 29
1.2.5	Bandwidth and Filtering — 31
1.3	Discretization — 32
1.4	Compressive Sensing — 36
1.4.1	Background — 36
1.4.2	Compressive Sensing Model — 39
1.4.3	Conditions for Signal (Sparse) Recovery in Compressive Sensing — 39
1.5	Discrete and Digital Signals — 41
1.5.1	Discrete Signals — 41
1.5.1.1	Finite Impulse Response — 43
1.5.1.2	Infinite Impulse Response — 44
1.5.2	Digital Signals — 46
1.6	Discrete and Fast Fourier Transform — 47
1.6.1	Discrete Fourier Transform (DFT) — 47
1.6.2	Spectrum Forming and Window Functions — 48
1.6.3	Fast Fourier Transform (FFT) — 51
2	Typical Communications Signals — 57
2.1	Speech — 57
2.1.1	Production and Modelling — 57
2.1.2	Speech Channel Bandwidth and Power of Speech Signal — 60
2.1.3	Current Values of Speech Signal — 63
2.1.4	Coding and Compression — 64
2.2	Audio — 69
2.2.1	Sound and Human Auditory System — 70
2.2.2	Audio Systems — 73
2.2.3	Digital Audio Systems — 76
2.2.3.1	Audio Coding — 77
2.2.4	Audio in transmission systems — 79

2.2.4.1	File Formats and Metadata —	79
2.2.4.2	Digital Broadcasting, Network and File Transfer —	80
2.3	Image —	81
2.3.1	Digital Image Processing System —	82
2.3.2	Digital Image Processing Operations and Methods —	83
2.3.2.1	Image Representation and Modelling —	84
2.3.2.2	Image Improvement —	84
2.3.2.3	Image Restoration —	86
2.3.2.4	Image Compression —	86
2.3.2.5	Image Analysis —	92
2.4	Television —	92
3	Random Processes —	99
3.1	Probability Theory —	99
3.1.1	Terms and axioms of the probability theory —	100
3.1.2	Conditional Probability, Total Probability and Bayes' Theorem —	102
3.2	Random signals —	104
3.2.1	Random Variables and Random Vectors —	105
3.2.1.1	Distribution Function and Probability Density Function —	106
3.2.1.2	Random Vectors —	107
3.2.1.3	Conditional Probabilities of Random Vectors —	108
3.2.2	Examples of Often Used Distributions —	109
3.2.2.1	Uniform Distribution —	109
3.2.2.2	Normal (Gaussian) Distribution Function —	110
3.2.2.3	Exponential Distribution Function —	111
3.2.3	Variance and Higher Order Moments —	113
3.2.4	Moment Generating Function —	116
3.2.5	Characteristic Function —	118
3.2.6	Distribution of Function of Random Variable —	119
3.2.7	Central Limit Theorem —	121
3.3	Stochastic Processes —	123
3.3.1	Ensemble, Stationarity and Ergodicity —	123
3.3.2	Power Spectral Density and Wiener-Khinchin Theorem —	126
3.3.2.1	White and Colored Noise —	128
4	Information Theory and Coding —	129
4.1	Information Theory —	129
4.1.1	Coding Components of Communication System —	129
4.1.2	Definition of Information —	131
4.1.3	Entropy —	132
4.2	Source Coding —	136

4.2.1	Code Definition —	138
4.2.2	Compression Algorithms —	140
4.2.2.1	Huffman Coding —	140
4.2.2.2	Arithmetic Coding —	142
4.3	Channel Coding —	144
4.3.1	Block Coding —	145
4.3.1.1	Hamming Codes —	147
4.3.1.2	Cyclic Codes —	148
4.3.1.3	Cyclic Redundancy Check Codes —	150
4.3.1.4	Reed Solomon Codes —	152
4.3.1.5	Low Density Parity Check Codes —	155
4.3.2	Convolutional Coding —	159
4.3.2.1	Viterbi Algorithm —	162
4.3.2.2	Turbo Codes —	163
4.4	Concatenated Codes —	171
4.5	Joint Source and Channel Coding —	172
5	Digital Transmission —	175
5.1	Model of a Digital Transmission System —	175
5.2	Channel Model —	175
5.3	Channel Capacity —	182
5.4	Base-band Transmission —	186
5.4.1	Line Coding —	186
5.4.1.1	Non-Return-To-Zero (NRZ) and Non-Return-To-Zero Inverted (NRZI) —	188
5.4.1.2	Return-To-Zero (RZ) and Return-To-Zero Inverted (RZI) —	189
5.4.1.3	Alternate Mark Inversion and Inverted Alternate Mark Inversion —	191
5.4.1.4	Manchester —	192
5.4.1.5	Differential Manchester —	192
5.4.1.6	High Density Bipolar n (HDBn) —	193
5.4.1.7	Binary 3 Ternary / Modified Monitored Sum 43 —	194
5.4.1.8	Scrambling —	195
5.4.2	Intersymbol Interference —	196
5.4.3	Partial Response Signalling —	203
5.4.4	Optimization of Transmission System —	204
5.4.4.1	Optimum and Matched Filter —	204
5.4.4.2	Correlation Receiver —	205
5.4.4.3	Integrate & Dump Receiver —	205
5.4.5	Equalization —	206
5.5	Digital Modulation —	207
5.5.1	Amplitude Shift Keying —	208

5.5.2	Frequency Shift Keying —	210
5.5.3	Phase Shift Keying —	216
5.5.4	ASK/PSK —	225
5.5.5	M-Quadrature Amplitude Modulation (M-QAM) —	226
6	Multiplexing —	229
6.1	Introduction —	229
6.2	Space Division Multiplexing —	230
6.3	Time Division Multiplexing —	231
6.3.1	Synchronous Time Division Multiplexing —	231
6.3.2	Plesiochronous Digital Hierarchy —	233
6.3.3	Synchronous Digital Hierarchy —	235
6.3.4	Aynchronous (statistical) Time Division Multiplex —	238
6.4	Frequency Division Multiplexing —	240
6.5	Orthogonal Frequency Division Multiplexing —	242
6.5.1	Principles —	242
6.5.2	OFDM Scheme —	245
6.5.2.1	OFDM Transmitter —	245
6.5.2.2	OFDM Receiver —	247
6.5.2.3	OFDM Signal —	248
6.5.3	Coded Orthogonal Frequency Division Multiplexing —	249
6.6	Wavelength Division Multiplexing —	252
6.7	Polarization Division Multiplexing —	254
6.8	Orbital Angular Momentum Multiplexing —	256
6.9	Code Division Multiplexing (CDM) —	257
6.9.1	Code Sequences —	257
6.9.1.1	Pseudonoise Sequences —	258
6.9.1.2	Walsh Sequences —	260
6.9.2	Spread Spectrum —	261
6.9.2.1	Frequency Hopping —	261
6.9.2.2	Direct Sequence —	264
6.9.2.3	Time Hopping —	268
6.9.2.4	Chirp Spread Spectrum —	268
7	Wired Transmission Media —	271
7.1	Introduction —	271
7.2	Cables with Copper Conductors —	271
7.2.1	Communication Lines —	272
7.2.2	Applications of Copper Cables —	284
7.2.2.1	Cables with Twisted Pairs —	284
7.2.2.2	DSL Technology —	289

7.2.2.3	Coaxial Cables — 293
7.3	Optical Cables — 297
7.3.1	Propagation of Light through Optical Waveguides — 297
7.3.2	Attenuation in Glass Fibers — 305
7.3.3	Dispersion in optical fibers — 310
7.3.4	Types of optical fibers and cables — 313
7.3.5	Construction Structures of Optical Cables and Their Applications — 318
7.3.6	Historical Milestones and Development Trends in Fiber Optics — 322
8	Wireless Channel — 329
8.1	Channel Characteristics — 329
8.2	Multipath Propagation — 331
8.3	Propagation Model — 334
8.3.1	One-Way Propagation — 334
8.3.2	Two-Way Propagation — 335
8.3.3	<i>N</i> -Way Propagation — 336
8.4	Fading Model — 336
8.4.1	Rayleigh Fading — 336
8.4.2	Rician Fading — 337
8.5	Doppler Shift — 339
8.6	Diversity — 342
8.6.1	Diversity and Combining Techniques — 342
8.6.1.1	Selection Combining — 344
8.6.1.2	Switched Combining — 345
8.6.1.3	Maximal Ratio Combining — 346
8.6.1.4	Equal Gain Combining — 348
8.6.2.1	Precoding — 351
8.6.2.2	Spatial multiplexing — 351
8.6.2.3	Diversity coding — 352
8.7	Propagation and Path Loss in Free Space — 352
8.7.1	Concept of Free Space — 352
8.7.2	Path Loss — 352
8.7.3	Path Loss in Free Space — 353
8.7.4	Effective Isotropic Radiated Power — 353
8.8	Path Loss Prediction Models — 354
8.9	Software Defined Radio — 354
8.10	Cognitive Radio — 356
9	Cryptography — 361
9.1	Basic terminologies — 361

9.1.1	Crypto ABC — 361
9.1.2	Cryptographic Design Principles — 362
9.1.3	Encryption/Decryption — 362
9.1.4	Key Based Encryption — 363
9.1.5	Symmetric Cryptography — 364
9.1.6	Asymmetric Cryptography — 365
9.1.6.1	Asymmetric Encryption — 366
9.1.6.2	Digital Signatures — 366
9.1.6.3	Man-in-the-Middle Attack — 368
9.1.6.4	Certificate — 368
9.2	One Way Collision Resistant Hash Function — 370
9.2.1	Characteristics — 370
9.2.2	Security of a One Way Collision Resistant Hash Function — 371
9.2.2.1	Random Oracle and Avalanche Effect — 373
9.2.3	Hash Functions in Practice — 373
9.3	Block Cipher — 374
9.3.1	Product Cipher — 374
9.3.2	Padding — 375
9.3.3	Block Ciphers in Practice — 376
9.3.3.1	Advanced Encryption Standard — 376
9.3.3.2	Lightweight Cipher PRESENT — 377
9.4	Modes of Operations for Block Ciphers — 379
9.4.1	Electronic Codebook (ECB) — 379
9.4.2	Cipher Block Chaining (CBC) — 381
9.4.3	Cipher Feedback (CFB) — 382
9.4.4	Output Feedback (OFB) — 383
9.4.5	Counter Mode (CTR) — 384
9.4.6	Other Modes of Operation — 385
9.5	Bit Stream Ciphers — 386
9.6	Message Authentication Codes — 388
9.6.1	Generation — 388
9.6.2	MAC generation using symmetric block cipher — 389
9.6.3	MAC Generation Using Dedicated Hash Function — 390
9.6.4	Security Aspects — 390
9.6.4.1	Length Extension Attack — 390
9.7	Digital Signatures — 392
9.7.1	Digital Signatures with Appendix — 392
9.7.2	Digital Signatures with Message Recovery — 394
9.7.3	RSA — 395
9.7.3.1	Introduction — 395
9.7.3.2	Generation of RSA key system — 396

9.7.4	El-Gamal —	398
9.7.4.1	Introduction —	398
9.7.4.2	Authentication of Message —	398
9.7.4.3	Verification of Message —	399
9.7.5	Digital Signature Algorithm (DSA) —	400
9.7.5.1	Introduction —	400
9.7.5.2	Authentication of Message —	400
9.7.5.3	Verification of Message —	401
9.7.6	Elliptic curve digital signature algorithm (ECDSA) —	402
9.7.6.1	Elliptic Curves —	402
9.7.6.2	ECDSA —	405
9.8	Random Numbers —	407
9.8.1	Randomness —	407
9.8.2	Random Number Generation —	408
9.8.2.1	True Random Number Generation —	408
9.8.2.2	Pseudo Random Number Generation —	408
9.8.2.3	Cryptographically Secure Pseudo Random Number Generation —	409

References — 411**List of Acronyms — 431****Index — 447**

