- Preface p. xiii
- Acknowledgement p. xv
- Glossary p. xix
- Acronyms and Abbreviations p. xxiii
- 1 Threats and Solutions p. 1
- 1.1 The Technical Threats to Communications Security p. 4
- 1.2 Authentication p. 4
- 1.2.1 Text/Data Message Authentication p. 6
- 1.3 Confidentiality p. 7
- 1.4 Integrity p. 8
- 1.4.1 Digital Signatures p. 8
- 1.5 Availability p. 10
- 1.5.1 PINs and Passwords p. 10
- 1.5.2 Biometric Access Tools p. 13
- 1.5.3 Challenge/Response Control p. 14
- 1.5.4 Tamperproof Modules p. 15
- 1.6 Compromising Emanation/Tempest Threats p. 16
- 1.6.1 Compromising Emanation Definitions p. 16
- 1.6.2 Compromising Emanation p. 16
- 1.6.3 Modulated Harmonics p. 16
- 1.6.4 Electronic Coupling p. 19
- 1.6.5 Preventative Measures in Electronic Equipment Construction p. 21
- 2 An Introduction to Encryption and Security Management p. 25
- 2.1 Analogue Scrambling p. 25
- 2.1.1 Phonemes and the Structure of Voice Signals p. 26
- 2.1.2 Frequency Scrambling p. 28
- 2.1.3 Time Element Scrambling p. 29
- 2.1.4 Digital Ciphering p. 30
- 2.1.5 Digital Stream Ciphering p. 31
- 2.1.6 Block Ciphering p. 33
- 2.1.7 Summary p. 37
- 2.2 Algorithms p. 38
- 2.2.1 Symmetrical Cryptography p. 38
- 2.2.2 Asymmetrical Cryptography p. 39
- 2.2.3 Hash Algorithms p. 41
- 2.2.4 MACs (Message Authentication Codes) p. 41
- 2.2.5 Digital Signature Algorithms p. 41
- 2.2.6 Key Agreement/Exchange Algorithms p. 42
- 2.2.7 Summary of Comparisons Between Asymmetric and Symmetric Algorithms p. 42
- 2.3 Goodbye DES, Hello AES p. 43
- 2.4 Fundamentals in Key Management p. 44
- 2.4.1 Key Generation p. 45
- 2.4.2 Key Storage p. 47
- 2.4.3 Key Distribution p. 48

- 2.4.4 Key Changes p. 51
- 2.4.5 Key Destruction p. 54
- 2.4.6 Separation p. 55
- 2.5 Evaluating Encryption Equipment p. 57
- 2.5.1 The Main Points of Evaluation p. 58
- 3 Voice Security in Military Applications p. 61
- 3.1 Analogue Encryption of Naval Long Range, HF Radio Communications p. 62
- 3.1.1 Ship Communications Operation p. 63
- 3.1.2 The Cipher/Scrambler Features p. 65
- 3.1.3 Synchronisation p. 68
- 3.1.4 Security Parameters p. 69
- 3.1.5 Key Distribution and Management p. 70
- 3.2 Stand-alone Digital Cipher Units in Land-based Operations p. 70
- 3.2.1 The Ground Force Scenario p. 71
- 3.2.2 The Cipher Unit Features p. 71
- 3.2.3 Synchronisation p. 74
- 3.2.4 Security Parameters p. 76
- 3.2.5 Key Management p. 77
- 3.3 Radio Integrated Cipher Module p. 82
- 3.3.1 Typical Features p. 83
- 3.3.2 Cryptographic Parameters p. 83
- 3.3.3 Other Security Parameters and Features p. 83
- 4 Telephone Security p. 87
- 4.1 Specific Threats to Telephone Operations p. 88
- 4.1.1 Telephone Security Requirements and Features p. 89
- 4.2 Network Technologies p. 90
- 4.2.1 Secure Telephone Communication p. 90
- 4.2.2 INMARSAT Communications p. 91
- 4.3 Telephone Security Solutions p. 95
- 4.3.1 STU III/IIB p. 96
- 4.3.2 The Alternative Telephone Security p. 98
- 4.3.3 Hardware Security Features p. 101
- 4.3.4 Telephone Security Architecture and Functions p. 102
- 4.4 Key and Access Management p. 103
- 4.4.1 The Complete Key System p. 104
- 4.4.2 The 'ZUPPA' Network p. 107
- 4.5 Network Implementation p. 108
- 4.6 Key Distribution p. 111
- 4.7 Summary p. 112
- 5 Secure GSM Systems p. 113
- 5.1 The Basic GSM Architecture p. 113
- 5.1.1 System Components p. 114
- 5.1.2 The GSM Subsystems p. 116
- 5.1.3 The GSM Radio Um Interface p. 117

- 5.2 Standard GSM Security Features p. 118
- 5.2.1 The AuC p. 119
- 5.2.2 The HLR p. 119
- 5.2.3 The VLR p. 120
- 5.2.4 SIM Card p. 120
- 5.2.5 The IMSI and TMSI p. 121
- 5.2.6 Standard GSM Encryption p. 121
- 5.2.7 Cryptographic Attacks on the GSM Algorithms p. 126
- 5.2.8 TDMA Time Division Multiple Access p. 127
- 5.2.9 Frequency Hopping p. 127
- 5.3 Custom Security for GSM Users p. 128
- 5.3.1 The Custom Encryption Process p. 130
- 5.3.2 Key Systems p. 133
- 5.3.3 Cryptographic Parameters and Algorithms p. 135
- 5.3.4 Security Architecture p. 135
- 5.3.5 Cipher Unit Hardware Elements p. 136
- 5.3.6 System Overview with Secure GSM and Fixed Subscriber Equipment p. 137
- 5.4 Key Management and Tools p. 138
- 5.4.1 Key Distribution and Loading p. 138
- 5.4.2 Chip Cards and Readers p. 138
- 5.4.3 Key Signatures p. 138
- 5.5 GPRS General Packet Radio Systems p. 139
- 5.5.1 Basic GPRS Operation and Security p. 139
- 6 Security in Private VHF/UHF Radio Networks p. 143
- 6.1 Applications and Features p. 143
- 6.1.1 The Ship Group p. 143
- 6.1.2 The Escort Group p. 145
- 6.1.3 The Close Support Group p. 145
- 6.1.4 The Telephone Groups p. 146
- 6.2 Threats p. 146
- 6.2.1 Confidentiality p. 146
- 6.2.2 Integrity p. 146
- 6.2.3 Authenticity p. 147
- 6.2.4 Access p. 147
- 6.3 Countermeasures p. 147
- 6.3.1 Protection of Confidentiality p. 147
- 6.3.2 Authentication p. 147
- 6.3.3 Access Control p. 149
- 6.4 Communications Network Design and Architecture p. 150
- 6.4.1 The Close Support Group p. 151
- 6.4.2 The Escort Group p. 152
- 6.4.3 The Ship Group p. 152
- 6.5 Hardware Components and Functions p. 153
- 6.5.1 Hand-held UHF Radios p. 153

- 6.5.2 Base Stations/Repeaters p. 158
- 6.5.3 Telephone Patch p. 160
- 6.5.4 Security Management Tools p. 162
- 6.6 Security and Key Management p. 162
- 6.6.1 Functions of the Management Centre p. 162
- 6.6.2 Frequency Management p. 163
- 6.6.3 Key Management p. 165
- 6.7 Other Security Features p. 168
- 6.7.1 Remote Key Cancelling p. 168
- 6.7.2 Remote Blocking p. 168
- 6.7.3 Silent Mode Tracking p. 168
- 7 Electronic Protection Measures - Frequency Hopping p. 171
- 7.1 ESM p. 171
- 7.2 EA p. 172
- 7.3 EPM p. 172
- 7.3.1 Methods of Attack p. 172
- 7.3.2 Spread Spectrum Techniques p. 177
- 7.3.3 COMSEC and TRANSEC p. 182
- 7.4 Military Applications p. 183
- 7.4.1 Applications Requirements p. 183
- 7.4.2 Operational Requirements p. 184
- 7.4.3 Security Requirements p. 184
- 7.4.4 Anti Jamming Requirements p. 184
- 7.4.5 Co-location p. 185
- 7.4.6 Air Defence Scenario p. 185
- 7.4.7 Close Air Support Scenario p. 187
- 7.5 Network Architecture and Management p. 189
- 7.5.1 Mission Procedures p. 190
- 7.6 Characteristics of Frequency Hopping Networks p. 191
- 7.6.1 COMSEC p. 191
- 7.6.2 TRANSEC p. 192
- 7.7 Key/Data Management and Tools p. 201
- 7.7.1 Algorithm Data p. 202
- 7.7.2 Frequency Data p. 203
- 7.7.3 Pre-set Data p. 203
- 7.7.4 Configuration Parameters p. 203
- 7.7.5 Key Distribution p. 203
- 7.7.6 The Time Problem p. 206
- 7.8 Hardware Components p. 207
- 7.8.1 Airborne Transceiver p. 207
- 8 Link and Bulk Encryption p. 211
- 8.1 Basic Technology of Link Encryption p. 211
- 8.1.1 Frame Modes p. 211
- 8.2 The Ciphering Process p. 212

- 8.3 Cryptographic Parameters p. 214
- 8.3.1 Key Agreement p. 216
- 8.4 Key and Network Management p. 216
- 8.4.1 Civilian Application p. 216
- 8.5 Military Link Security p. 222
- 8.5.1 Military Topology and Features p. 223
- 9 Secure Fax Networks p. 227
- 9.1 Basic Facsimile Technology p. 228
- 9.2 The Basic Operation of an Encrypted Fax Machine p. 229
- 9.2.1 Fax by Telephone Line p. 229
- 9.2.2 Fax by Radio p. 230
- 9.2.3 The GB Fax Protocol p. 230
- 9.3 Manual/Automatic Key Selection p. 232
- 9.3.1 Multi-key Fax Networks p. 233
- 9.3.2 Single Key Fax Networks p. 234
- 9.3.3 Facsimile Transmission over Radio p. 235
- 9.4 Network Architecture p. 235
- 9.4.1 Interesting Features of DEFNET p. 236
- 9.4.2 Ministry of Defence Subnet p. 237
- 9.5 Key Management and Tools p. 237
- 9.5.1 Key Management of DEFNET p. 237
- 9.5.2 Key Generation p. 237
- 9.5.3 Operating Parameters p. 239
- 9.5.4 Key and Parameter Distribution p. 239
- 9.6 Fax Over Satellite Links p. 239
- 10 PC Security p. 241
- 10.1 Security Threats and Risks p. 244
- 10.2 Implementation of Solutions p. 244
- 10.2.1 Unauthorised Read Out of Data Stored on Local Storage Media p. 244
- 10.2.2 Unauthorised Read Out of 'Deleted' Data p. 245
- 10.2.3 Unauthorised Read Out of Data Stored on a Remote LAN p. 246
- 10.2.4 Unauthorised Manipulation of Data Stored on a LAN p. 247
- 10.2.5 Eavesdropping on an Untrusted LAN or Public Network p. 249
- 10.2.6 Spoofing or Masquerading p. 249
- 10.2.7 Unauthorised Manipulation of Data During Transmission over a Public Network p. 249
- 10.2.8 Unauthorised Access to/Read Out of/Analysis of/Manipulation of/the Security System p. 249
- 10.2.9 'Brute-force' Attack p. 250
- 10.2.10 Inefficient Security and Key Management p. 251
- 10.2.11 Analysis of Residual Plain Information p. 251
- 10.2.12 The Compromise of Information, Due to Loss or Theft of Equipment or the Transfer of Security Personnel p. 251

- 10.2.13 The Storage or Transmission of Data in Plain, Due to Loss of Keys or Key Incompatibility p. 252
- 10.2.14 Illegal Access to Equipment Under Maintenance or Repair p. 252
- 10.2.15 Unauthorised Intrusion into the PC Environment Whilst Connected to a Public or Untrusted Network p. 252
- 10.3 Access Protection p. 253
- 10.3.1 Access Control Systems p. 253
- 10.3.2 Access by Chip Card p. 254
- 10.3.3 Access by PC Cards p. 254
- 10.3.4 Access by PCMCIA Module p. 256
- 10.4 Boot-up Protection by On-board Hardware with Smart Card p. 256
- 10.5 LAN Security p. 256
- 10.5.1 LAN Workstation Scenario p. 257
- 10.5.2 Business Trip Notebook Scenario p. 258
- 10.6 Model Application of PC Security p. 259
- 10.7 System Administration p. 264
- 11 Secure E-mail p. 265
- 11.1 The E-mail Scenario p. 265
- 11.2 Threats p. 267
- 11.2.1 Information Disclosure p. 267
- 11.2.2 Modification of Messages p. 269
- 11.2.3 Replay Attack p. 269
- 11.2.4 Masquerading p. 269
- 11.2.5 Spoofing p. 269
- 11.2.6 Denial of Service Attack p. 269
- 11.3 Type and Motivation of Attackers p. 270
- 11.4 Methods of Attack p. 270
- 11.5 Countermeasures p. 271
- 11.6 Guidelines for E-mail Security p. 274
- 12 Secure Virtual Private Networks p. 275
- 12.1 Scenario p. 275
- 12.2 Definition of VPN p. 275
- 12.3 Protocols p. 277
- 12.4 Packet Header Formats p. 278
- 12.5 Security Association List p. 281
- 12.6 Tunnel Table p. 282
- 12.7 Routing Tables p. 282
- 12.8 Packet Filtering p. 283
- 12.9 Threats and Countermeasures p. 284
- 12.9.1 Attacks Within the Public Network p. 285
- 12.9.2 Attacks Within Nodes of the Trusted Network p. 285
- 12.9.3 Attacks Aimed at Gaining Access to the Private Network p. 285
- 12.10 Example Application--'Diplomatic Network' p. 285
- 13 Military Data Communications p. 289

- 13.1 Applications p. 290
- 13.1.1 Data Over Radio Links p. 290
- 13.1.2 Modes of Radio Operation, Automatic Repeat Request and Forward Error Correction p. 290
- 13.1.3 Use of GAN Terminals in Battlefield Applications p. 291
- 13.2 Data Terminals and Their Operating Features p. 292
- 13.3 Technical Parameters p. 293
- 13.4 Security Management p. 294
- 13.4.1 Access Control p. 294
- 13.4.2 Data Encryption p. 295
- 13.4.3 Loss of Data p. 295
- 13.4.4 TEMPEST p. 295
- 13.5 Key Management p. 295
- 13.6 Combat Packet Data Networks p. 296
- 13.6.1 Packet Radios p. 296
- 13.6.2 Packet Data Networks p. 297
- 14 Management, Support and Training p. 301
- 14.1 Environments of Security Management p. 303
- 14.1.1 The Global Environment p. 303
- 14.1.2 The Local/Task Environment p. 306
- 14.2 Infrastructure and Planning p. 307
- 14.2.1 Strategic Goals p. 308
- 14.2.2 Tactical Goals p. 308
- 14.2.3 Operational Goals p. 308
- 14.3 Operational Hierarchies p. 308
- 14.4 Training p. 310
- 14.5 Customer Support p. 312
- 14.6 Troubleshooting p. 312
- 14.6.1 The Scanning Stage p. 312
- 14.6.2 The Categorisation Stage p. 313
- 14.6.3 The Diagnostics Stage p. 313
- 14.6.4 Generating Solutions p. 313
- References p. 315
- Index p. 317