

Contents

| | |
|--|-------------|
| Preface | xiii |
| About the Authors | xvii |
| Acknowledgments | xix |
| 1 Classic Ciphers | 1 |
| 1.1 Introduction | 1 |
| 1.2 Good Guys and Bad Guys | 1 |
| 1.3 Terminology | 2 |
| 1.4 Selected Classic Crypto Topics | 4 |
| 1.4.1 Transposition Ciphers | 5 |
| 1.4.2 Substitution Ciphers | 8 |
| 1.4.3 One-Time Pad | 18 |
| 1.4.4 Codebook Ciphers | 20 |
| 1.5 Summary | 21 |
| 1.6 Problems | 22 |
| 2 World War II Ciphers | 25 |
| 2.1 Introduction | 25 |
| 2.2 Enigma | 26 |
| 2.2.1 Enigma Cipher Machine | 26 |
| 2.2.2 Enigma Keyspace | 29 |
| 2.2.3 Rotors | 31 |
| 2.2.4 Enigma Attack | 34 |
| 2.2.5 More Secure Enigma? | 37 |
| 2.3 Purple | 38 |
| 2.3.1 Purple Cipher Machine | 38 |
| 2.3.2 Purple Keyspace | 44 |
| 2.3.3 Purple Diagnosis | 45 |
| 2.3.4 Decrypting Purple | 49 |
| 2.3.5 Purple versus Enigma | 50 |
| 2.4 Sigaba | 52 |

| | | |
|----------|---|------------|
| 2.4.1 | Sigaba Cipher Machine | 52 |
| 2.4.2 | Sigaba Keyspace | 57 |
| 2.4.3 | Sigaba Attack | 59 |
| 2.4.4 | Sigaba Conclusion | 67 |
| 2.5 | Summary | 68 |
| 2.6 | Problems | 69 |
| 3 | Stream Ciphers | 79 |
| 3.1 | Introduction | 79 |
| 3.2 | Shift Registers | 81 |
| 3.2.1 | Berlekamp–Massey Algorithm | 83 |
| 3.2.2 | Cryptographically Strong Sequences | 85 |
| 3.2.3 | Shift Register-Based Stream Ciphers | 89 |
| 3.2.4 | Correlation Attack | 90 |
| 3.3 | ORYX | 93 |
| 3.3.1 | ORYX Cipher | 91 |
| 3.3.2 | ORYX Attack | 97 |
| 3.3.3 | Secure ORYX? | 102 |
| 3.4 | RC4 | 103 |
| 3.4.1 | RC4 Algorithm | 105 |
| 3.4.2 | RC4 Attack | 105 |
| 3.4.3 | Preventing the RC4 Attack | 110 |
| 3.5 | PKZIP | 110 |
| 3.5.1 | PKZIP Cipher | 111 |
| 3.5.2 | PKZIP Attack | 113 |
| 3.5.3 | Improved PKZIP? | 120 |
| 3.6 | Summary | 120 |
| 3.7 | Problems | 121 |
| 4 | Block Ciphers | 127 |
| 4.1 | Introduction | 127 |
| 4.2 | Block Cipher Modes | 128 |
| 4.3 | Feistel Cipher | 131 |
| 4.4 | Hellman's Time-Memory Trade-Off | 133 |
| 4.4.1 | Cryptanalytic TMTO | 133 |
| 4.4.2 | Bad Chains | 137 |
| 4.4.3 | Success Probability | 141 |
| 4.4.4 | Distributed TMTO | 142 |
| 4.4.5 | TMTO Conclusions | 143 |
| 4.5 | CMEA | 144 |
| 4.5.1 | CMEA Cipher | 141 |
| 4.5.2 | SCMEA Cipher | 146 |
| 4.5.3 | SCMEA Chosen Plaintext Attack | 147 |

| | | |
|----------|--|------------|
| 4.5.4 | CMEA Chosen Plaintext Attack | 148 |
| 4.5.5 | SCMEA Known Plaintext Attack | 151 |
| 4.5.6 | CMEA Known Plaintext Attack | 158 |
| 4.5.7 | More Secure CMEA? | 159 |
| 4.6 | Akelarre | 160 |
| 4.6.1 | Akelarre Cipher | 160 |
| 4.6.2 | Akelarre Attack | 166 |
| 4.6.3 | Improved Akelarre? | 169 |
| 4.7 | FEAL | 170 |
| 4.7.1 | FEAL-4 Cipher | 171 |
| 4.7.2 | FEAL-4 Differential Attack | 172 |
| 4.7.3 | FEAL-4 Linear Attack | 177 |
| 4.7.4 | Confusion and Diffusion | 182 |
| 4.8 | Summary | 183 |
| 4.9 | Problems | 183 |
| 5 | Hash Functions | 193 |
| 5.1 | Introduction | 193 |
| 5.2 | Birthdays and Hashing | 200 |
| 5.2.1 | The Birthday Problem | 200 |
| 5.2.2 | Birthday Attacks on Hash Functions | 201 |
| 5.2.3 | Digital Signature Birthday Attack | 202 |
| 5.2.4 | Nostradamus Attack | 203 |
| 5.3 | MD4 | 208 |
| 5.3.1 | MD4 Algorithm | 208 |
| 5.3.2 | MD4 Attack | 210 |
| 5.3.3 | A Meaningful Collision | 224 |
| 5.4 | MD5 | 225 |
| 5.4.1 | MD5 Algorithm | 225 |
| 5.4.2 | A Precise Differential | 231 |
| 5.4.3 | Outline of Wang's Attack | 233 |
| 5.4.4 | Wang's MD5 Differentials | 235 |
| 5.4.5 | Reverse Engineering Wang's Attack | 238 |
| 5.4.6 | Stevens' Implementation of Wang's Attack | 252 |
| 5.4.7 | A Practical Attack | 253 |
| 5.5 | Summary | 256 |
| 5.6 | Problems | 257 |
| 6 | Public Key Systems | 265 |
| 6.1 | Introduction | 265 |
| 6.2 | Merkle Hellman Knapsack | 267 |
| 6.2.1 | Lattice-Reduction Attack | 270 |
| 6.2.2 | Knapsack Conclusion | 275 |

| | | |
|----------|--|------------|
| 6.3 | Diffie-Hellman Key Exchange | 275 |
| 6.3.1 | Man-in-the-Middle Attack | 277 |
| 6.3.2 | Diffie-Hellman Conclusion | 278 |
| 6.4 | Arithmetic Key Exchange | 279 |
| 6.4.1 | Hughes-Fauncubbaum Length Attack | 283 |
| 6.4.2 | Arithmetic Conclusion | 284 |
| 6.5 | RSA | 281 |
| 6.5.1 | Mathematical Issues | 285 |
| 6.5.2 | RSA Conclusion | 288 |
| 6.6 | Rabin Cipher | 289 |
| 6.6.1 | Chosen Ciphertext Attack | 291 |
| 6.6.2 | Rabin Cryptosystem Conclusion | 292 |
| 6.7 | NTRU Cipher | 293 |
| 6.7.1 | Meet-in-the-Middle Attack | 299 |
| 6.7.2 | Multiple Transmission Attack | 301 |
| 6.7.3 | Chosen Ciphertext Attack | 302 |
| 6.7.4 | NTRU Conclusion | 304 |
| 6.8 | ElGamal Signature Scheme | 305 |
| 6.8.1 | Mathematical Issues | 308 |
| 6.8.2 | ElGamal Signature Conclusion | 308 |
| 6.9 | Summary | 309 |
| 6.10 | Problems | 309 |
| 7 | Public Key Attacks | 315 |
| 7.1 | Introduction | 315 |
| 7.2 | Factoring Algorithms | 316 |
| 7.2.1 | Trial Division | 316 |
| 7.2.2 | Dixon's Algorithm | 317 |
| 7.2.3 | Quadratic Sieve | 323 |
| 7.2.4 | Factoring Conclusions | 327 |
| 7.3 | Discrete Log Algorithms | 330 |
| 7.3.1 | Trial Multiplication | 330 |
| 7.3.2 | Baby-Step Giant-Step | 331 |
| 7.3.3 | Index Calculus | 332 |
| 7.3.4 | Discrete Log Conclusions | 333 |
| 7.4 | RSA Implementation Attacks | 334 |
| 7.4.1 | Timing Attacks | 334 |
| 7.4.2 | Glitching Attack | 353 |
| 7.4.3 | Implementation Attacks Conclusions | 354 |
| 7.5 | Summary | 355 |
| 7.6 | Problems | 355 |

| | |
|--------------------------------|------------|
| Appendix | 361 |
| A-1 MD5 Tables | 361 |
| A-2 Math | 371 |
| A-2.1 Number Theory | 371 |
| A-2.2 Group Theory | 372 |
| A-2.3 Ring Theory | 372 |
| A-2.4 Linear Algebra | 373 |
| Annotated Bibliography | 375 |
| Index | 393 |

