

# Contents

<b>1</b>	<b>A Short Course on Cryptography</b>	1
1.1	Ahlsvede's Immediate Response to Shannon's Work	3
1.1.1	Introduction	3
1.1.2	A Simple Cipher for Shannon's Secrecy System	6
1.1.3	A Robustification of Shannon's Secrecy System	10
1.2	The Wiretap Channel	13
1.2.1	The Classical Wiretap Channel	14
1.2.2	The Multi-user Wiretap Channel	19
1.2.3	The Compound Wiretap Channel	24
1.2.4	The Arbitrary Varying Wiretap Channel	29
1.2.5	Discussion and Open Questions	37
1.3	Worst Codes for the BSC	39
1.4	Shannon's Information-Theoretic Approach to Cryptosystems	42
1.5	Homophonic Coding	44
1.6	Spurious Decipherments	46
1.7	Authentication	48
	References	52
<b>2</b>	<b>Authentication and Secret-Key Cryptology</b>	55
2.1	Introduction	55
2.2	Models and Notation	59
2.2.1	Secret-Key Cryptology	59
2.2.2	Authentication	62
2.3	Authentication	65
2.3.1	General Bounds and Perfectness	65
2.3.2	Authentication Codes Without Secrecy	72
2.3.3	Estimates on the Number of Messages Given the Success Probability of the Opponent	83
2.3.4	Authentication as an Hypothesis Testing Problem	103

- 2.4 Secret-Key Cryptology . . . . . 113
  - 2.4.1 Preliminaries . . . . . 113
  - 2.4.2 The Lower Bound for Locally Regular Ciphers . . . . . 116
  - 2.4.3 A Simple Cipher . . . . . 119
  - 2.4.4 Data Compression . . . . . 123
  - 2.4.5 Randomization . . . . . 131
- 2.5 Public-Key Cryptology . . . . . 135
  - 2.5.1 Introduction . . . . . 135
  - 2.5.2 Number Theory . . . . . 138
  - 2.5.3 Prime Number Tests and Factorization Algorithms . . . . . 144
  - 2.5.4 The Discrete Logarithm . . . . . 146
  - 2.5.5 Knapsack Cryptosystems . . . . . 147
  - 2.5.6 Further Cryptographic Protocols . . . . . 150
- References . . . . . 152

**3 The Mathematical Background of the Advanced Encryption**

- Standard . . . . . 155**
- 3.1 Introduction . . . . . 155
- 3.2 The AES Selection Process . . . . . 157
- 3.3 Finite Fields . . . . . 158
  - 3.3.1 Polynomials Over a Field . . . . . 159
  - 3.3.2 The Field  $\langle F[x]_d, \oplus, \odot \rangle$  . . . . . 159
  - 3.3.3 Byte-Operations in Rijndael . . . . . 162
- 3.4 A Key-Iterated Block Cipher . . . . . 167
  - 3.4.1 Boolean Functions . . . . . 168
  - 3.4.2 A Key-Iterated Block Cipher . . . . . 169
- 3.5 The Wide Trail Strategy . . . . . 170
  - 3.5.1 Linear Trails . . . . . 170
  - 3.5.2 Differential Trails . . . . . 180
  - 3.5.3 The Wide Trail Strategy . . . . . 183
- 3.6 The Specifications of Rijndael . . . . . 193
  - 3.6.1 The Input, the Output, and the State . . . . . 194
  - 3.6.2 The Non-linear Layer . . . . . 195
  - 3.6.3 The Linear Layer . . . . . 198
  - 3.6.4 The AddRoundKey Step . . . . . 201
  - 3.6.5 The Key Schedule . . . . . 202
  - 3.6.6 Encryption . . . . . 204
  - 3.6.7 Decryption . . . . . 206
  - 3.6.8 Complexity . . . . . 207
  - 3.6.9 Security . . . . . 209
- 3.7 Cryptanalysis . . . . . 210
  - 3.7.1 The Saturation Attack . . . . . 210
  - 3.7.2 Further Cryptanalysis . . . . . 218

- 3.8 The Extended Euclidean Algorithm . . . . . 218
  - 3.8.1 The Euclidean Algorithm . . . . . 219
  - 3.8.2 The Extended Euclidean Algorithm . . . . . 220
  - 3.8.3 Results . . . . . 222
- References . . . . . 224
- 4 Elliptic Curve Cryptosystems . . . . . 225**
  - 4.1 Cryptography . . . . . 226
    - 4.1.1 Secret-Key Cryptography . . . . . 226
    - 4.1.2 Public-Key Cryptography . . . . . 228
    - 4.1.3 Trapdoor One-Way Functions . . . . . 230
    - 4.1.4 Digital Signature Standard (DSS) . . . . . 234
    - 4.1.5 Discrete Logarithms in Finite Groups . . . . . 235
    - 4.1.6 Factorization of Composite Numbers . . . . . 238
  - 4.2 Elliptic Curves . . . . . 241
    - 4.2.1 Definitions . . . . . 241
    - 4.2.2 Group Law . . . . . 246
    - 4.2.3 Elliptic Curves over the Finite Field  $\mathbb{F}_q$  . . . . . 253
    - 4.2.4 Elliptic Curves over the Ring  $\mathbb{Z}_n$  . . . . . 267
    - 4.2.5 Elliptic Curves over  $\mathbb{Q}$  . . . . . 268
  - 4.3 Elliptic Curves: Algorithms . . . . . 269
    - 4.3.1 Efficient m-fold Addition in  $E(\mathbb{F}_p)$  . . . . . 269
    - 4.3.2 Finding Random Points in  $E(\mathbb{F}_q)$  . . . . . 277
    - 4.3.3 Counting the Number of Points on  $E(\mathbb{F}_p)$  . . . . . 278
  - 4.4 Elliptic Curve Cryptosystems Based on Factorization . . . . . 279
    - 4.4.1 Cryptosystem Schemes . . . . . 279
    - 4.4.2 Known Attacks on KMOV and Demytko . . . . . 282
    - 4.4.3 Integer Factorization . . . . . 286
    - 4.4.4 Conclusion . . . . . 289
  - 4.5 Elliptic Curve Cryptosystems Based on the ECDLP . . . . . 290
    - 4.5.1 Public-Key Schemes . . . . . 291
    - 4.5.2 Elliptic Curve Discrete Logarithm Problem . . . . . 294
    - 4.5.3 Elliptic Curve Construction . . . . . 322
    - 4.5.4 Designing New Public-Key Cryptosystems . . . . . 328
    - 4.5.5 Conclusion . . . . . 332
- References . . . . . 333
- 5 Founding Cryptography on Oblivious Transfer . . . . . 337**
  - 5.1 Introduction . . . . . 337
  - 5.2 Upper and Lower Bounds on the Oblivious Transfer Capacity . . . . . 338
    - 5.2.1 Statement of Results . . . . . 338
    - 5.2.2 The Proofs . . . . . 340
    - 5.2.3 Discussion and Examples . . . . . 343
- References . . . . . 344

<b>Obituary for Rudi</b> . . . . .	345
<b>Comments by Rüdiger Reischuk</b> . . . . .	349
<b>List of Notations</b> . . . . .	351
<b>Author Index</b> . . . . .	353
<b>Subject Index</b> . . . . .	355



<http://www.springer.com/978-3-319-31513-3>

Hiding Data - Selected Topics

Rudolf Ahlswede's Lectures on Information Theory 3

Ahlswede, R. - Ahlswede, A.; Althöfer, I.; Deppe, C.;

Tamm, U. (Eds.)

2016, XIV, 356 p. 17 illus. in color., Hardcover

ISBN: 978-3-319-31513-3