

---

# Contents

Foreword: MASS and REU at Penn State University	v
Preface	vii
Chapter 1. Finite Fields	1
§1. Introduction	1
§2. Finite fields	1
§3. Extension fields	6
§4. Trace and norm functions	15
§5. Bases	19
§6. Polynomials	26
§7. Notes	36
§8. Exercises	37
Chapter 2. Combinatorics	43
§1. Introduction	43
§2. Latin squares	43
§3. Affine and projective planes	59
§4. Block designs	66
§5. Hadamard matrices	71
§6. Notes	75
§7. Exercises	75

---

Chapter 3. Algebraic Coding Theory	79
§1. Introduction	79
§2. Basic properties of codes	81
§3. Bounds for parameters of codes	88
§4. Decoding methods	91
§5. Code constructions	94
§6. Codes and combinatorial designs	101
§7. Codes and latin squares	104
§8. Notes	106
§9. Exercises	106
Chapter 4. Cryptography	109
§1. Introduction to cryptography	110
§2. Symmetric key cryptography	112
§3. Public key cryptography	114
§4. Threshold schemes	126
§5. Notes	128
§6. Exercises	129
Appendix A. Background in Number Theory and Abstract Algebra	133
§1. Number theory	133
§2. Groups	135
§3. Rings and fields	137
§4. Homomorphisms	140
§5. Polynomials and splitting fields	141
§6. Vector spaces	146
§7. Notes	150
§8. Exercises	150
Appendix B. Hints for Selected Exercises	155
References	165
Index	171