

Contents

Foreword	v
Preface to the Second Edition	vii
Chapter I. Some Topics in Elementary Number Theory	1
1. Time estimates for doing arithmetic	1
2. Divisibility and the Euclidean algorithm	12
3. Congruences	19
4. Some applications to factoring	27
Chapter II. Finite Fields and Quadratic Residues	31
1. Finite fields	33
2. Quadratic residues and reciprocity	42
Chapter III. Cryptography	54
1. Some simple cryptosystems	54
2. Enciphering matrices	65
Chapter IV. Public Key	83
1. The idea of public key cryptography	83
2. RSA	92
3. Discrete log	97
4. Knapsack	111
5. Zero-knowledge protocols and oblivious transfer	117
Chapter V. Primality and Factoring	125
1. Pseudoprimes	126
2. The rho method	138
3. Fermat factorization and factor bases	143