

x Contents

| | |
|--|------------|
| 4. The continued fraction method | 154 |
| 5. The quadratic sieve method | 160 |
| Chapter VI. Elliptic Curves | 167 |
| 1. Basic facts | 167 |
| 2. Elliptic curve cryptosystems | 177 |
| 3. Elliptic curve primality test | 187 |
| 4. Elliptic curve factorization | 191 |
| Answers to Exercises | 200 |
| Index | 231 |