1 INTRODUCTION 1

1.1 The Meaning of the Word Cryptography 2
1.2 Symmetric Key Cryptography 2
  1.2.1 Impact of Technology 3
  1.2.2 Confusion and Diffusion 3
  1.2.3 DES and AES 4
1.3 Public Key (Asymmetric) Cryptography 5
  1.3.1 Diffie–Hellman Key Exchange 5
  1.3.2 RSA 5
  1.3.3 ElGamal 6
1.4 Key Establishment 7
1.5 Cryptography—More than just Hiding Secrets 8
  1.5.1 Digital Signatures 8
  1.5.2 Authentication 9
  1.5.3 Nonrepudiation 9
1.6 Standards 9
1.7 Attacks 10

2 CONGRUENCE EQUATIONS 13

2.1 Congruence Arithmetic 14
  2.1.1 Computer Examples 17
  2.1.2 Problems 18
2.2 The Euclidean Algorithm—Finding Inverses 18
  2.2.1 Computer Examples 24
  2.2.2 Problems 25
5.1.3 Adding a Point to Its Negative 86
5.1.4 Adding a Point to Itself 86
5.1.5 Computer Examples 90
5.1.6 Problems 91
5.2 Elliptic Curve Cryptography 92
5.2.1 Elliptic Curve Groups and the Discrete Logarithm Problem 92
5.2.2 An Elliptic Curve ElGamal System 93
5.2.3 Elliptic Curve Key Exchange (ECKE) 95
5.2.4 Computer Examples 96
5.2.5 Problems 98
5.3 The Elliptic Curve Factoring Scheme 99
5.3.1 Computer Examples 100
5.3.2 Problems 101

6 DIGITAL SIGNATURES 103
6.1 Hash Functions 104
6.1.1 SHA-1 108
6.1.2 MD5 109
6.1.3 The Search for New Hash Functions 112
6.1.4 Computer Examples 113
6.1.5 Problems 114
6.2 Digital Signature Schemes 116
6.2.1 Direct Digital Signature Schemes 116
6.2.2 Using RSA for Signing 117
6.2.3 Using ElGamal for Signing 118
6.2.4 Arbitrated Digital Signature Schemes 118
6.2.5 The Digital Signature Standard 119
6.2.6 Computer Examples 121
6.2.7 Problems 122
6.3 Attacks on Digital Signatures 123
6.3.1 The Birthday Attack 123
6.3.2 Intruder-in-the-Middle Attack 124
6.3.3 Intruder-in-the-Middle and Diffie–Hellman 125
6.3.4 An Attack on RSA Signatures: What if Eve Uses Alice’s Signature? 126
6.3.5 Protecting ElGamal with Signatures 127
6.3.6 Oscar Tries to Trick Bob 127
6.3.7 Oscar Captures a Message with a Signed Version 128
7 PRIMALITY TESTING

7.1 Fermat’s Approach and Wilson’s Theorem 134
  7.1.1 Computer Examples 135
  7.1.2 Problems 135

7.2 The Miller–Selfridge–Rabin Primality Test 136
  7.2.1 The Miller–Selfridge–Rabin Algorithm (Long Version) 137
  7.2.2 The MSR Algorithm (Short Version) 138
  7.2.3 Computer Examples 140
  7.2.4 Problems 140

7.3 True Primality Tests 141
  7.3.1 Pocklington’s Theorem 141
  7.3.2 Proth’s Theorem 142
  7.3.3 Computer Examples 144
  7.3.4 Problems 144

7.4 Mersenne Primes and the Lucas–Lehmer Test 144
  7.4.1 The Lucas–Lehmer Test 145
  7.4.2 Computer Examples 145
  7.4.3 Problems 146

7.5 Primes is in $P$ 146
  7.5.1 Polynomial Rings 146
  7.5.2 A Division Algorithm for Polynomials 147
  7.5.3 A Euclidean Algorithm for Polynomials 147
  7.5.4 Computer Examples 149
  7.5.5 Problems 150

8 FACTORING METHODS

8.1 Fermat Again 152
  8.1.1 Fermat’s Difference of Squares Method 152
  8.1.2 Using the Miller–Selfridge–Rabin Algorithm to Factor 153
  8.1.3 Euler’s Factoring Method 153
  8.1.4 Kraitchik’s Method 154
  8.1.5 Computer Examples 155
  8.1.6 Problems 156
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2</td>
<td>The Quadratic Sieve</td>
<td>156</td>
</tr>
<tr>
<td></td>
<td>8.2.1 Computer Examples</td>
<td>158</td>
</tr>
<tr>
<td></td>
<td>8.2.2 Problems</td>
<td>159</td>
</tr>
<tr>
<td>8.3</td>
<td>Pollard’s $p - 1$ and rho Methods</td>
<td>160</td>
</tr>
<tr>
<td></td>
<td>8.3.1 Pollard’s $p - 1$ Method</td>
<td>160</td>
</tr>
<tr>
<td></td>
<td>8.3.2 The Pollard $p - 1$ Algorithm</td>
<td>160</td>
</tr>
<tr>
<td></td>
<td>8.3.3 Pollard’s rho Method</td>
<td>161</td>
</tr>
<tr>
<td></td>
<td>8.3.4 The Pollard rho Algorithm</td>
<td>161</td>
</tr>
<tr>
<td></td>
<td>8.3.5 Computer Examples</td>
<td>162</td>
</tr>
<tr>
<td></td>
<td>8.3.6 Problems</td>
<td>163</td>
</tr>
<tr>
<td>8.4</td>
<td>Continued Fractions and Factoring</td>
<td>164</td>
</tr>
<tr>
<td></td>
<td>8.4.1 The Setup</td>
<td>164</td>
</tr>
<tr>
<td></td>
<td>8.4.2 Pell’s Equation</td>
<td>167</td>
</tr>
<tr>
<td></td>
<td>8.4.3 Back to Factoring</td>
<td>167</td>
</tr>
<tr>
<td></td>
<td>8.4.4 Computer Examples</td>
<td>169</td>
</tr>
<tr>
<td></td>
<td>8.4.5 In Summary</td>
<td>171</td>
</tr>
<tr>
<td></td>
<td>8.4.6 Problems</td>
<td>171</td>
</tr>
</tbody>
</table>

**Appendix: Solutions to Problems** 175

**Notation** 193

**Bibliography** 195

**Index** 199