Cryptanalytic Attacks on RSA

by

Song Y. Yan
University of Bedfordshire, UK
and
Massachusetts Institute of Technology, USA
# Table of Contents

Preface ................................................. xi
Notations ............................................. xv

1. Computational/Mathematical Preliminaries .......... 1
   1.1 Introduction ..................................... 1
   1.2 Computability, Complexity and Intractability .... 4
   1.3 Efficient Number-Theoretic Algorithms .......... 15
   1.4 Intractable Number-Theoretic Problems .......... 41
   1.5 Chapter Notes and Further Reading .............. 54

2. RSA Public-Key Cryptography ....................... 55
   2.1 Introduction ..................................... 55
   2.2 Public-Key Cryptography ....................... 60
   2.3 RSA Public-Key Cryptography ................... 66
   2.4 RSA Problem and RSA Assumption ............... 71
   2.5 RSA-Type Cryptosystems ....................... 73
   2.6 Chapter Notes and Further Readings ............. 88

3. Integer Factorization Attacks ....................... 91
   3.1 Introduction ..................................... 91
   3.2 Fermat Factoring Attack ....................... 93
   3.3 The “p ± 1” and ECM Attacks ................... 94
   3.4 Quadratic Sieve Attack ....................... 98
   3.5 Successful QS Attack ......................... 103
   3.6 Number Field Sieve Attack ................... 105
   3.7 Chapter Notes and Further Reading ............. 110

4. Discrete Logarithm Attacks ......................... 111
   4.1 Introduction ..................................... 111
   4.2 Baby-Step Giant-Step Attack ................... 115
   4.3 Silver-Pohlig-Hellman Attack ................... 118
   4.4 Index Calculus Attacks ....................... 122
   4.5 Xedni Calculus Attack ....................... 127
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>10. The Road Ahead</td>
<td>223</td>
</tr>
<tr>
<td>10.1 Introduction</td>
<td>223</td>
</tr>
<tr>
<td>10.2 Elliptic Curve-Based Cryptography</td>
<td>224</td>
</tr>
<tr>
<td>10.3 Coding-Based Cryptography</td>
<td>225</td>
</tr>
<tr>
<td>10.4 Lattice-Based Cryptography</td>
<td>227</td>
</tr>
<tr>
<td>10.5 Quantum Cryptography</td>
<td>229</td>
</tr>
<tr>
<td>10.6 Conclusions</td>
<td>230</td>
</tr>
<tr>
<td>10.7 Chapter Notes and Further Reading</td>
<td>232</td>
</tr>
<tr>
<td>Bibliography</td>
<td>233</td>
</tr>
<tr>
<td>Index</td>
<td>251</td>
</tr>
<tr>
<td>About the Author</td>
<td>255</td>
</tr>
</tbody>
</table>