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 Crytposystems 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 "$p \pm 1$" 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

4.6 Chapter Notes and Further Reading 132

5. Quantum Computing Attacks 135
5.1 Introduction 135
5.2 Order Finding Problem 137
5.3 Quantum Order Finding Attack 139
5.4 Quantum Integer Factorization Attack 142
5.5 Quantum Discrete Logarithm Attack 146
5.6 Chapter Notes and Further Reading 148

6. Simple Elementary Attacks 149
6.1 Introduction 149
6.2 Guessing Plaintext Attacks 150
6.3 Blinding Attack on RSA Signatures 151
6.4 Guessing $\phi(N)$ Attack 152
6.5 Guessing d Attack 155
6.6 e^{th} Root Attack 159
6.7 Common Modulus Attack 161
6.8 Fixed-Point Attack 164
6.9 Chapter Notes and Further Readings 166

7. Public Exponent Attacks 169
7.1 Introduction 169
7.2 A Theorem of Coppersmith 170
7.3 Short e Attacks for Same Messages 173
7.4 Short e Attacks for Related Messages 177
7.5 Lattice Attack for Stereotyped Messages 183
7.6 Chapter Notes and Further Reading 187

8. Private Exponent Attacks 189
8.1 Introduction 189
8.2 Diophantine Attack 190
8.3 Extended Diophantine Attacks 195
8.4 Small Private CRT-Exponent Attacks 198
8.5 Partial Private Key Exposure Attacks 201
8.6 Chapter Notes and Further Reading 205

9. Side-Channel Attacks 207
9.1 Introduction 207
9.2 Modular Exponentiation Revisited 208
9.3 Timing Attacks 209
9.4 Time Attacks on RSA in OpenSSL 212
9.5 Power (Analysis) Attacks 215
9.6 Random Fault Attacks 216
9.7 Chapter Notes and Further Reading 222

10. The Road Ahead 223
10.1 Introduction 223
10.2 Elliptic Curve-Based Cryptography 224
10.3 Coding-Based Cryptography 225
10.4 Lattice-Based Cryptography 227
10.5 Quantum Cryptography 229
10.6 Conclusions 230
10.7 Chapter Notes and Further Reading 232

Bibliography 233

Index 251

About the Author 255

http://www.springer.com/978-0-387-48741-0

Cryptanalytic Attacks on RSA

Yan, S.Y.

2008, XX, 255 p. 20 illus., Hardcover
ISBN: 978-0-387-48741-0