
Contents

List of Figures	xiii
List of Tables	xv
Preface	xvii
I Preliminaries	1
1 The RSA Cryptosystem	3
1.1 Public-Key Cryptography	3
1.2 The RSA Cryptosystem	4
1.3 The Security of RSA	8
1.3.1 Integer Factorization	8
1.3.2 Breaking RSA	9
1.3.3 Cryptanalysis of RSA	10
1.3.4 The Homomorphic Property of RSA	11
1.3.5 Semantic Security	12
1.4 Efficiency of RSA	12
1.4.1 Prime Generation	13
1.4.2 Modular Exponentiation	13
1.5 RSA Signature Scheme	14
1.6 Variants of RSA	14
1.7 Additional Notes	16
2 Some Notation, Mathematics and Techniques	17
2.1 Some Notation	17
2.2 Some Mathematics Results	19
2.3 Integer Factorization	21
2.4 Continued Fractions	22
2.5 Lattices	23
2.5.1 Definitions and Basic Facts	24
2.5.2 LLL-Reduced Bases	25
2.5.3 The Shortest Vector Problem	27
2.6 Solving Linear Equations	28
2.6.1 Modular Linear Equations	31
2.7 Coppersmith's Methods	33

2.7.1	Small Solutions of Modular Polynomials	34	6.3	Partially Known Private Exponent: LSBs	106
2.7.1.1	Known Results for Modular Polynomials	39	6.3.1	Arbitrary Exponents	106
2.7.2	Small Solutions of Integer Polynomials	40	6.3.2	Full Sized Public Exponent	108
2.7.2.1	Known Results for Integer Polynomials	42	6.3.3	Full Sized Private Exponent	108
2.7.3	Computing and Improving the Bounds	43	6.3.4	Practical Effectiveness	112
2.7.4	Assumptions for Coppersmith's Methods	45	6.4	Partially Known Primes	113
2.8	On Attacks and Proofs	46	6.4.1	Small Private Exponent Attacks	114
2.9	Additional Notes	47	6.4.2	Partial Key Exposure Attacks	115
II Cryptanalysis of RSA		49	6.4.3	Exhaustive Search Attacks	116
3	Some Early Attacks	51	6.5	Key Reconstruction with Random Errors	117
3.1	Common Modulus Attack	51	6.6	Additional Notes	118
3.2	Håstad's Broadcast Attack	52	7	More Small Private Exponent Attacks	121
3.2.1	Common Plaintext Attack	53	7.1	Common Modulus Attack	121
3.2.2	Related Plaintext Attack	53	7.1.1	Practical Effectiveness	128
3.3	Cycling Attacks	54	7.2	Common Private Exponent Attack	129
3.4	Additional Notes	55	7.2.1	Practical Effectiveness	132
4	Small Public Exponent Attacks	57	7.3	Additional Notes	134
4.1	Stereotyped Message Attack	57	III Cryptanalysis of Variants of RSA		137
4.2	Related Message Attacks	59	8	CRT-RSA	139
4.3	Random Padding Attack	61	8.1	CRT-RSA	139
4.4	Leaking Information	61	8.1.1	Variations of CRT-RSA	140
4.5	Additional Notes	63	8.1.2	Efficiency of CRT-RSA	141
5	Small Private Exponent Attacks	65	8.1.3	Breaking CRT-RSA	142
5.1	Wiener's Continued Fraction Attack	66	8.2	Small CRT-Exponent Attacks	143
5.1.1	Extending Wiener's Attack	69	8.3	Partial Key Exposure Attacks	148
5.1.2	Wiener's Attack with Lattices	70	8.4	Key Reconstruction with Random Errors	151
5.1.2.1	Heuristic Approach	71	8.5	Additional Notes	152
5.1.2.2	Provable Approach	72	9	Multi-Prime RSA	155
5.2	Boneh and Durfee's Lattice Attacks	74	9.1	Multi-Prime RSA	155
5.2.1	Lattice Attack	74	9.1.1	Efficiency of Multi-Prime RSA	157
5.2.2	Sub-Lattice Attack	79	9.1.2	Breaking Multi-Prime RSA	158
5.2.3	Blömer and May's Attack	83	9.2	Factoring the Modulus	158
5.3	Effectiveness of the Attacks	87	9.2.1	Factoring with a Hint	159
5.4	Additional Notes	89	9.3	Small Private Exponent Attacks	161
6	Partial Key Exposure Attacks	91	9.4	Partial Key Exposure Attacks	163
6.1	Factoring with a Hint	91	9.4.1	Partial Private Exponent: MSBs	164
6.2	Partially Known Private Exponent: MSBs	93	9.4.1.1	Arbitrary Exponents	164
6.2.1	Arbitrary Exponents	94	9.4.1.2	Full Sized Public Exponent	166
6.2.2	Full Sized Public Exponent	98	9.4.1.3	Full Sized Private Exponent	167
6.2.3	Full Sized Private Exponent	99	9.4.1.4	Effectiveness in Practice	168
6.2.4	Effectiveness in Practice	105	9.4.2	Partial Private Exponent: LSBs	169
			9.4.2.1	Arbitrary Exponents	170

9.4.2.2	Full Sized Public Exponent	171
9.4.2.3	Full Sized Private Exponent	171
9.4.2.4	Effectiveness in Practice	172
9.4.3	Known Primes	172
9.4.3.1	Small Private Exponent Attack	172
9.4.3.2	Partially Known Private Exponent Attack	174
9.4.4	Partial Primes	176
9.5	Common Modulus Attacks	176
9.5.1	Howgrave-Graham and Seifert's Attack	176
9.5.1.1	Practical Effectiveness	178
9.5.2	Guo's Attack	178
9.5.2.1	Practical Effectiveness	180
9.6	CRT Attacks	181
9.6.1	Small CRT-Exponent Attack	181
9.6.2	Partial CRT-Exponent Attack	182
9.7	Additional Notes	184
10	Multi-Power RSA	187
10.1	Takagi's Scheme	187
10.1.1	Efficiency of Takagi's Scheme	188
10.1.2	Breaking Takagi's Scheme	190
10.2	Factoring the Modulus	191
10.2.1	Factoring with a Hint	192
10.3	Small Private Exponent Attacks	192
10.4	Partial Key Exposure Attacks	194
10.5	Common Modulus Attack	195
10.6	Multi-Exponent RSA	196
10.6.1	Small Private Exponent Attacks	197
10.6.2	Partial Key Exposure Attacks	198
10.7	Additional Notes	200
11	Common Prime RSA	201
11.1	Common Prime RSA	201
11.1.1	Efficiency of Common Prime RSA	202
11.1.2	Breaking Common Prime RSA	203
11.2	Factoring the Modulus	203
11.2.1	Known a and b	204
11.2.2	Known g	205
11.2.3	Factoring $N - 1$ (or Computing g)	207
11.3	Small Private Exponent Attacks	208
11.3.1	Wiener's Attack	209
11.3.2	Lattice-Based Attacks	210
11.3.3	Known g Attacks	214
11.3.4	Summary of Attacks	216
11.4	Small CRT-Exponent Attacks	218

11.5	Additional Notes	219
12	Dual RSA	221
12.1	Dual RSA	221
12.2	Small Public Exponent	222
12.3	Small Private Exponent	225
12.4	Dual CRT-RSA	226
12.5	Efficiency and Comparison	228
12.5.1	Key Generation	228
12.5.2	Space Requirements	229
12.6	Additional Notes	230
A	Distribution of $g = \gcd(p - 1, q - 1)$	233
B	Geometrically Progressive Matrices	235
C	Some Algorithms	239
C.1	Dual RSA	239
	Further Reading	241
	Bibliography	243
	Index	265