
Contents

Preface

I Background

1	A bird's-eye view of modern cryptography	3
1.1	Preliminaries	3
1.1.1	Typical cryptographic needs	6
1.2	Defining security in cryptography	10
1.2.1	Distinguishers	11
1.2.2	Integrity and signatures	16
1.2.3	Authenticated encryption	17
1.2.4	Abstracting cryptographic primitives	21
2	Elementary number theory and algebra background	23
2.1	Integers and rational numbers	23
2.2	Greatest common divisors in $\mathbb{Z}$	26
2.2.1	Binary GCD algorithm	30
2.2.2	Approximations using partial GCD computations	31
2.3	Modular arithmetic	33
2.3.1	Basic algorithms for modular arithmetic	34
2.3.2	Primality testing	38
2.3.3	Specific aspects of the composite case	41
2.4	Univariate polynomials and rational fractions	44
2.4.1	Greatest common divisors and modular arithmetic	45
2.4.2	Derivative of polynomials	47
2.5	Finite fields	47
2.5.1	The general case	48
2.5.2	The special case of $\mathbb{F}_{2^n}$	49
2.5.3	Solving univariate polynomial equations	55
2.6	Vector spaces and linear maps	61
2.7	The RSA and Diffie-Hellman cryptosystems	63
2.7.1	RSA	63
2.7.2	Diffie-Hellman key exchange	65

II Algorithms

3	Linear algebra	71
3.1	Introductory example: Multiplication of small matrices over $\mathbb{F}_2$	71
3.2	Dense matrix multiplication	77
3.2.1	Strassen's algorithm	80
3.2.2	Asymptotically fast matrix multiplication	89
3.2.3	Relation to other linear algebra problems	93
3.3	Gaussian elimination algorithms	94
3.3.1	Matrix inversion	98
3.3.2	Non-invertible matrices	98
3.3.3	Hermite normal forms	103
3.4	Sparse linear algebra	105
3.4.1	Iterative algorithms	106
3.4.2	Structured Gaussian elimination	113
4	Sieve algorithms	123
4.1	Introductory example: Eratosthenes's sieve	123
4.1.1	Overview of Eratosthenes's sieve	123
4.1.2	Improvements to Eratosthenes's sieve	125
4.1.3	Finding primes faster: Atkin and Bernstein's sieve	133
4.2	Sieving for smooth composites	135
4.2.1	General setting	136
4.2.2	Advanced sieving approaches	148
4.2.3	Sieving without sieving	152
5	Brute force cryptanalysis	155
5.1	Introductory example: Dictionary attacks	155
5.2	Brute force and the DES algorithm	157
5.2.1	The DES algorithm	157
5.2.2	Brute force on DES	161
5.3	Brute force as a security mechanism	163
5.4	Brute force steps in advanced cryptanalysis	164
5.4.1	Description of the SHA hash function family	165
5.4.2	A linear model of SHA-0	168
5.4.3	Adding non-linearity	171
5.4.4	Searching for collision instances	179

5.5	Brute force and parallel computers	182
6	The birthday paradox: Sorting or not?	185
6.1	Introductory example: Birthday attacks on modes of operation	186
6.1.1	Security of CBC encryption and CBC-MAC	186
6.2	Analysis of birthday paradox bounds	189
6.2.1	Generalizations	190
6.3	Finding collisions	192
6.3.1	Sort algorithms	196
6.3.2	Hash tables	207
6.3.3	Binary trees	210
6.4	Application to discrete logarithms in generic groups	216
6.4.1	Pohlig-Hellman algorithm	216
6.4.2	Baby-step, giant-step algorithm	218
7	Birthday-based algorithms for functions	223
7.1	Algorithmic aspects	224
7.1.1	Floyd's cycle finding algorithm	225
7.1.2	Brent's cycle finding algorithm	226
7.1.3	Finding the cycle's start	227
7.1.4	Value-dependent cycle finding	228
7.2	Analysis of random functions	231
7.2.1	Global properties	231
7.2.2	Local properties	232
7.2.3	Extremal properties	232
7.3	Number-theoretic applications	233
7.3.1	Pollard's Rho factoring algorithm	233
7.3.2	Pollard's Rho discrete logarithm algorithm	236
7.3.3	Pollard's kangaroos	237
7.4	A direct cryptographic application in the context of blockwise security	238
7.4.1	Blockwise security of CBC encryption	239
7.4.2	CBC encryption beyond the birthday bound	239
7.4.3	Delayed CBC beyond the birthday bound	240
7.5	Collisions in hash functions	242
7.5.1	Collisions between meaningful messages	243
7.5.2	Parallelizable collision search	244

7.6	Hellman's time memory tradeoff	246
7.6.1	Simplified case	247
7.6.2	General case	248
8	Birthday attacks through quadrisection	251
8.1	Introductory example: Subset sum problems	251
8.1.1	Preliminaries	252
8.1.2	The algorithm of Shamir and Schroepel	253
8.2	General setting for reduced memory birthday attacks	256
8.2.1	Xoring bit strings	257
8.2.2	Generalization to different groups	258
8.2.3	Working with more lists	262
8.3	Extensions of the technique	263
8.3.1	Multiple targets	263
8.3.2	Wagner's extension	264
8.3.3	Related open problems	265
8.4	Some direct applications	267
8.4.1	Noisy Chinese remainder reconstruction	267
8.4.2	Plain RSA and plain ElGamal encryptions	269
8.4.3	Birthday attack on plain RSA	269
8.4.4	Birthday attack on plain ElGamal	270
9	Fourier and Hadamard-Walsh transforms	273
9.1	Introductory example: Studying S-boxes	273
9.1.1	Definitions, notations and basic algorithms	273
9.1.2	Fast linear characteristics using the Walsh transform	275
9.1.3	Link between Walsh transforms and differential characteristics	279
9.1.4	Truncated differential characteristics	282
9.2	Algebraic normal forms of Boolean functions	285
9.3	Goldreich-Levin theorem	286
9.4	Generalization of the Walsh transform to $\mathbb{F}_p$	288
9.4.1	Complexity analysis	291
9.4.2	Generalization of the Moebius transform to $\mathbb{F}_p$	293
9.5	Fast Fourier transforms	294
9.5.1	Cooley-Tukey algorithm	296
9.5.2	Rader's algorithm	300

9.5.3	Arbitrary finite abelian groups	303
10	Lattice reduction	309
10.1	Definitions	309
10.2	Introductory example: Gauss reduction	311
10.2.1	Complexity analysis	315
10.3	Higher dimensions	318
10.3.1	Gram-Schmidt orthogonalization	319
10.3.2	Lenstra-Lenstra-Lovász algorithm	320
10.4	Shortest vectors and improved lattice reduction	327
10.4.1	Enumeration algorithms for the shortest vector	327
10.4.2	Using shortest vectors to improve lattice reduction	330
10.5	Dual and orthogonal lattices	331
10.5.1	Dual of a lattice	332
10.5.2	Orthogonal of a lattice	333
11	Polynomial systems and Gröbner base computations	337
11.1	General framework	338
11.2	Bivariate systems of equations	340
11.2.1	Resultants of univariate polynomials	341
11.2.2	Application of resultants to bivariate systems	343
11.3	Definitions: Multivariate ideals, monomial orderings and Gröbner bases	345
11.3.1	A simple example: Monomial ideals	346
11.3.2	General case: Gröbner bases	346
11.3.3	Computing roots with Gröbner bases	349
11.3.4	Homogeneous versus affine algebraic systems	351
11.4	Buchberger algorithm	352
11.5	Macaulay's matrices	354
11.6	Faugère's algorithms	355
11.6.1	The F_4 approach	356
11.6.2	The F_5 approach	359
11.6.3	The specific case of $\mathbb{F}_2$	360
11.6.4	Choosing and changing monomial ordering for Gröbner bases	361
11.7	Algebraic attacks on multivariate cryptography	362
11.7.1	The HFE cryptosystem	363

11.7.2	Experimental Gröbner basis attack	364
11.7.3	Theoretical explanation	365
11.7.4	Direct sparse approach on Macaulay's matrix	366
11.8	On the complexity of Gröbner bases computation	367

III Applications

12	Attacks on stream ciphers	373
12.1	LFSR-based keystream generators	374
12.2	Correlation attacks	376
12.2.1	Noisy LFSR model	376
12.2.2	Maximum likelihood decoding	377
12.2.3	Fast correlation attacks	380
12.2.4	Algorithmic aspects of fast correlation attacks	383
12.3	Algebraic attacks	387
12.3.1	Predicting an annihilator polynomial	388
12.4	Extension to some non-linear shift registers	389
12.5	The cube attack	390
12.5.1	Basic scenario for the cube method	392
12.6	Time memory data tradeoffs	393
13	Lattice-based cryptanalysis	397
13.1	Direct attacks using lattice reduction	397
13.1.1	Dependence relations with small coefficients	397
13.1.2	Some applications of short dependence relations	402
13.2	Coppersmith's small roots attacks	407
13.2.1	Univariate modular polynomials	407
13.2.2	Bivariate polynomials	410
13.2.3	Extension to rational roots	413
13.2.4	Security of RSA with small decryption exponent	414
14	Elliptic curves and pairings	417
14.1	Introduction to elliptic curves	417
14.1.1	The group structure of elliptic curves	418
14.1.2	Double and add method on elliptic curves	423
14.1.3	Number of points on elliptic curves	423
14.2	The Weil pairing	424
14.2.1	Weil's reciprocity law	424

14.2.2	The Weil pairing on ℓ -torsion points	429
14.3	The elliptic curve factoring method	432
14.3.1	Pollard's $p - 1$ factoring	432
14.3.2	Elliptic curve factoring	433
15	Index calculus algorithms	439
15.1	Introduction to index calculus	439
15.2	A simple finite field example	441
15.2.1	Overview	441
15.2.2	A toy example	448
15.3	Generalization to finite fields with small enough characteristic	449
15.3.1	Overview of the regular function field sieve	453
15.4	Introduction to the number field sieve	455
15.4.1	Factoring with the quadratic sieve	456
15.4.2	Discrete logarithms with the Gaussian integer method	457
15.4.3	Constructing number field sieve polynomials	461
15.5	Smoothness probabilities	463
15.5.1	Computing smoothness probabilities for polynomials	463
15.5.2	Asymptotic lower bound on the smoothness probability	467
15.5.3	Smoothness probabilities for integers	467
	References	471
	Lists	491
	Index	497