

Index

- abelian group, 33
 - type of, 174
- Adleman-Huang primality test, 190
- Adleman-Pomerance-Rumely primality test, 134-135
- affine map, 57, 59, 68, 75
 - plane, 171
- algebraic, 32
- algorithm, 9
 - Berlekamp, 104
 - deterministic, 127
 - for discrete log, 102-106
 - factor-base, 103, 148
 - index-calculus, 103-106
 - probabilistic, 86, 95, 127
 - Schoof, 179, 183
 - Silver-Pohlig-Hellman, 102-103, 183
- alphabet, 54
 - Cyrillic, 63, 78
- arms control, 90-91, 214
- Atkin primality test, 187, 190
- authentication, 88, 95
- automorphism, 32, 36

- B*-number, 145, 160

- base of number system, 1
 - two, 1, 3
- big-*O* notation, 7-8
- bit, 3
 - operation, 3
- Bond, James, 82, 185, 210, 214
- breaking a code, 56
 - the knapsack, 114

- Caesar, Julius, 56
- Carmichael number, 127-128, 136
- Casanova, 84-85
- characteristic of a field, 33
- Chinese Remainder Theorem, 21
- Chor-Rivest knapsack, 115
- ciphertext, 54
- classical cryptosystem, 88
- Cohen-Lenstra primality test, 134-135
- coin toss, 91, 96-97, 215
- coloring map or graph, 118
- complex numbers, 17
 - Gaussian integers, 17, 37, 42-43, 171
- composite number, 12
- composition of cryptosystems, 64, 79