2. L. M. Adleman and J. DeMarrais, "A subexponential algorithm for discrete logarithms over all finite fields," *Math. Comp.* **61** (1993), 1–15.
3. D. Coppersmith, "Fast evaluation of logarithms in fields of characteristic two," *IEEE Transactions on Information Theory IT-30* (1984), 587–594.
4. D. Coppersmith, A. Odlyzko, and R. Schroeppel, "Discrete logarithms in $GF(p)$," *Algorithmica* **1** (1986), 1–15.
5. W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory IT-22* (1976), 644–654.
6. T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory IT-31*, (1985), 469–472.
7. T. ElGamal, "A subexponential-time algorithm for computing discrete logarithms over $GF(p^2)$," *IEEE Transactions on Information Theory IT-31* (1985), 473–481.
8. M. Fellows and N. Koblitz, "Fixed-parameter complexity and cryptography," *Proc. Tenth Intern. Symp. Appl. Algebra, Algebraic Algorithms and Error Correcting Codes* (San Juan, Puerto Rico), 1993.
9. D. Gordon, "Discrete logarithms in $GF(p)$ using the number field sieve," *SIAM J. Discrete Math.* **6** (1993), 124–138.
10. D. Gordon and K. McCurley, "Massively parallel computation of discrete logarithms," *Advances in Cryptology — Crypto '92*, Springer-Verlag, 1993.
11. D. E. Knuth, *The Art of Computer Programming*, Vol. II, Addison–Wesley, 1973.
12. B. LaMacchia and A. Odlyzko, "Computation of discrete logarithms in prime fields," *Designs, Codes and Cryptography* **1** (1991), 47–62.
13. J. L. Massey, "Logarithms in finite cyclic groups — cryptographic issues," *Proc. 4th Benelux Symposium on Information Theory* (1983), 17–25.
14. K. McCurley, "The discrete logarithm problem," *Cryptology and Computational Number Theory, Proc. Symp. Appl. Math.* **42** (1990), 49–74.
15. A. M. Odlyzko, "Discrete logarithms in finite fields and their cryptographic significance," *Advances in Cryptology, Proc. Eurocrypt 84*, Springer, 1985, 224–314.
16. P. K. S. Wah and M. Z. Wang, "Realization and application of the Massey–Omura lock," *Proc. International Zürich Seminar* (1984), 175–182.

4 Knapsack

In this section we describe another type of public key cryptosystem, which is based on the so-called "knapsack problem." Suppose you have a large knap-