'84, Springer-Verlag, 1985, 54–65; revised version in *IEEE Transactions on Information Theory IT-34* (1988), 901–909.

4. M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP–Completeness*, W. H. Freeman, 1979.
5. R. M. F. Goodman and A. J. McAuley, "A new trapdoor knapsack public key cryptosystem," *Advances in Cryptography, Proc. Eurocrypt 84*, Springer, 1985, 150–158.
6. M. E. Hellman, "The mathematics of public-key cryptography," *Scientific American* **241** (1979), 146–157.
7. M. E. Hellman and R. C. Merkle, "Hiding information and signatures in trapdoor knapsacks," *IEEE Transactions on Information Theory IT-24* (1978), 525–530.
8. A. Odlyzko, "The rise and fall of knapsack cryptosystems," *Cryptology and Computational Number Theory, Proc. Symp. Appl. Math.* **42** (1990), 75–88.
9. C. Schnorr, "Efficient identification and signatures for smart cards," *Advances in Cryptology — Crypto '89*, Springer-Verlag, 1990, 239–251.
10. A. Shamir, "A polynomial time algorithm for breaking the basic Merkle–Hellman cryptosystem," *Proc. 23rd Annual Symposium on the Foundations of Computer Science* (1982), 145–152.
11. P. van Oorschot, "A comparison of practical public-key cryptosystems based on integer factorization and discrete logarithms," in G. Simmons, ed., *Contemporary Cryptology: The Science of Information Integrity*, IEEE Press, 1992, 289–322.

5 Zero-knowledge protocols and oblivious transfer

"Zero knowledge" is the name of a cryptographic concept first developed in the early 1980's to deal with the following problem. Suppose someone wants to prove that she has figured out how to do something — find a solution to an equation, prove a theorem, solve a puzzle — while at the same time conveying no knowledge about her proof or solution. Can this ever be done? How can you convince someone that you have a solution without exhibiting it? The somewhat surprising fact is that in many situations it is possible to do this.

The "prover," whom we shall call Pícara, is the person with the solution; the "verifier" Vivales is the one who in the end must become satisfied that Pícara has a solution, while still not having the foggiest idea of what that solution is.

In this section we shall first give a simple, visual example of a zero-knowledge proof which is interactive (i.e., it requires communication back and forth between Pícara and Vivales). This example concerns map coloring and does not use number theory. Then we give a second example: how to prove that you have found a discrete logarithm without helping the verifier