Step 1. Vivales, who knows n, but not p and q, chooses an integer x at random. He computes the least nonnegative residue of x^4 modulo n, and sends this number — which we denote y — to Pícara.
Step 2. When Pícara receives y, she computes a square root modulo n (which is easy, since she knows the factorization of n; see Exercise 5 above). Of the four possible square roots, she chooses the unique one which is a quadratic residue modulo both p and q. This must be the least positive residue of x^2 modulo n. She sends this integer to Vivales.
Step 3. Vivales checks that the number he received from Pícara is in fact the residue of x^2 modulo n. He is then convinced that she can take square roots modulo n, something that would have been impossible if she didn't know the factors of n.

9. Find the drawback of the following procedure for a zero-knowledge proof of factorization. Suppose that n is the product of two primes p and q. Suppose that a "trusted Center" supplies an unending sequence of random squares modulo n, as in the text: $y_1, y_2, \ldots$. For each of the successive y_i, Pícara finds one of its square roots x_i, and sends it to Vivales, who verifies that $x_i^2 \equiv y \ (mod\ n)$.

References for §IV.5

1. M. Bellare and S. Micali, "Non-interactive oblivious transfer and applications," *Advances in Cryptology – Crypto '89*, Springer-Verlag, 547–557.
2. M. Ben-Or, O. Goldreich, S. Goldwasser, J. Håstad, J. Kilian, S. Micali, and P. Rogaway, "Everything provable is provable in zero-knowledge," *Advances in Cryptology — Crypto '88*, Springer-Verlag, 1990, 37–56.
3. M. Blum, P. Feldman, and S. Micali, "Non-interactive zero-knowledge proofs and their applications," *Proc. 20th ACM Symposium on the Theory of Computing* (1988).
4. D. Chaum, J.-H. Evertse, J. van de Graaf, and R. Peralta, "Demonstrating possession of a discrete logarithm without revealing it," *Advances in Cryptology – Crypto '86*, Springer–Verlag, 1987, 200–212.
5. M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness,* W. H. Freeman, 1979.
6. S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," *SIAM J. Computing* **18** (1989), 186–208.
7. J. Kilian, "Founding cryptography on oblivious transfer," *Proc. 20th ACM Symposium on the Theory of Computing* (1988), 20–31.
8. M. Rabin, "How to exchange secrets by oblivious transfer," *Technical Report TR-81*, Aiken Computation Laboratory, Harvard University, 1981.
9. A. Shamir, "The search for provably secure identification schemes," *Proc. Intern. Cong. Math.* (1986), 1488–1495.