2. Pícara finds the four square roots of $y$ modulo $n$, namely, $\pm x$, $\pm x'$. She arbitrarily chooses $x_0$ to be one of these four square roots.
3. Pícara randomly picks an integer $r$ and sends Vivales the integer $s = r^2 \bmod n$. She sets $m_1 = r\ mod\ n$, $m_2 = x_0 r\ mod\ n$, and sends these two messages to Vivales by oblivious transfer.
4. Vivales is able to read exactly one of the two messages. He checks that its square modulo $n$ is $s$ (if his random $i$ is 1) or $ys$ (if $i = 2$).
5. Steps 1–4 are repeated (with different public keys $(\beta_1, \beta_2)$). If Pícara meets the test $T$ times, then Vivales is satisfied (with certainty $1-2^{-T}$) that Pícara really knows the factorization.

## *Exercises*

1. In the zero-knowledge proof of possession of a discrete logarithm, if Pícara does not really know the discrete log, then what are the odds against her successfully fooling Vivales for $T$ repetitions of steps (1)-(3)?
2. In the zero-knowledge proof of possession of a discrete logarithm, suppose that Vivales does not know the value of $N$.
(a) Explain how the protocol described in the text is not really "zero knowledge."
(b) How could Pícara decrease the amount of information Vivales obtains about the magnitude of $N$?
3. Suppose that Pícara does not know $N$, and so in step (1) she chooses a random $e$ in some other range (e.g., $e < B$, where $B$ is an upper bound for the possible value of $N$), and in step (3) she sends simply $x + e$ rather than the least positive residue of $x + e$ modulo $N$. Explain why this is not a zero-knowledge proof. Why is the procedure followed by Clyde not a valid simulation?
4. Explain how the zero-knowledge proof in the text for possession of a discrete logarithm can be used for public key electronic identification. (This means that Pícara convinces Vivales that she really is Pícara.)
5. Explain why being able to extract square roots modulo $n = pq$ is essentially equivalent to knowing the factorization of $n$.
6. Can the same public key $(\beta_1, \beta_2)$ for oblivious transfer be used by several different people to give Vivales zero-knowledge proofs that they all independently know the same factorization? Assume that each person can eavesdrop on the transmissions of the others.
7. Using oblivious transfer, construct a non-interactive zero-knowledge proof for possession of a discrete logarithm. (Suppose that the order $N$ of the group is known to everyone.)
8. The following scheme was recently proposed as a zero-knowledge protocol for Pícara to use in order to demonstrate to Vivales that she knows the factors $p$ and $q$ of an integer $n$, where $n$ is known to be a product of two primes that are $\equiv 3 \pmod 4$. Find a basic flaw in the scheme.