ation will be written multiplicatively), b is a fixed element of G, and y is an element of G for which Pícara has found a discrete logarithm to the base b, i.e., she has solved the equation $b^x = y$ for a positive integer x. She wants to demonstrate to Vivales that she knows x without giving him a clue as to what x is. We first suppose that Vivales knows the order N of the group. Here is the sequence of steps performed by the two of them:

1. Pícara generates a random positive integer $e < N$, and sends Vivales $b' = b^e$.
2. Vivales flips a coin. If it comes up heads, Pícara must reveal e, and Vivales checks that in fact b' is b^e.
3. If the coin comes up tails, then Pícara must reveal the least positive residue of $x + e$ modulo N, at which point Vivales checks that $yb' = b^{x+e}$.
4. Steps #1–3 are repeated until Vivales is convinced that Pícara must know the value x of the discrete logarithm.

Notice that if Pícara does not know the value x of the discrete log, then she will not be able to respond to more than one possible result of the coin toss. If she has performed step (1) as she was supposed to, then she can respond to heads — but not to tails — without knowing x. On the other hand, if she anticipates tails and so in step (1) decides to send Vivales $b' = b^e/y$ (so that in step (3) she can send him simply e instead of $x + e$), then she will be in a jam if the coin comes up heads (since she does not know the power of b that gives b').

Further notice that the zero-knowledge property of this protocol can be proved by a simulation argument. Namely, suppose that Clyde does not know the discrete log of y to the base b but *does* know in advance how the coin toss will go. Then Clyde can simulate the same steps as Pícara (by sending $b' = b^e$ for heads and $b' = b^e/y$ for tails), giving Vivales information that is indistinguishable from what Pícara would have given him. Clyde cannot be telling Vivales anything useful for finding the discrete log, since he himself has no idea what the discrete log is.

In the exercises we will examine the situation when Vivales does not know N. For example, suppose that he knows that $G = (\mathbf{Z}/M\mathbf{Z})^*$, but he does not know the factorization of M. (Recall that if M is a product of two primes, then knowing its factorization is equivalent to knowing $N = \varphi(M)$, see §I.3.) Then ideally Pícara (or the simulator Clyde), who uses the value of N in step (1), must avoid conveying to Vivales any information about N (or else we don't really have a "zero knowledge" proof). This might seem to be too much to ask for, but one can insist that no more than a very small amount of information be conveyed.

Oblivious transfer. An "oblivious transfer channel" from Pícara to Vivales is a system for Pícara to send Vivales two encrypted packets of information subject to the following conditions:

1. Vivales can decipher and read exactly one of the two packets;
2. Pícara does not know which of the two packets he can read; and