which, whenever a button is pushed, chooses a random permutation of the three colors and then resets each vertex according to the permutation. For example, if the device B chooses the transposition of red and blue, then it goes to all vertices with blue lights, switches them to red lights, goes to all vertices with red lights, switches them to blue lights, and leaves the vertices with green lights alone. Vivales has no control over the device B and does not even know which permutations it generates.

We further suppose that the lights inside the vertex balls are hidden from view. However, whenever someone grabs onto the bar connecting two vertices, the lights in those two vertices (and no others) become visible.

Now Pícara has figured out a 3-coloring of the graph, and uses the device A to set the vertices with the corresponding colors. Here is the procedure used to convince Vivales that she has been successful in doing this:

1. Vivales is allowed to grab any one of the edge-bars, revealing the colors of the two vertices at each end. He will see that those two vertices have different colors, thereby giving a little bit of evidence that Pícara has a valid coloring (recall that "valid" means that no two adjacent vertices have the same color).
2. Next, Pícara pushes the button on B, permuting the colors.
3. Vivales may then grab another edge-bar.
4. Pícara and Vivales repeat steps #2 and #3 in alternation, until Vivales has tested all the bars (or, if he insists, until he has tested all the bars several times — perhaps he suspects that Pícara has cheated by resetting the vertices on a bar that was tested earlier).

After a little thought, two things should be clear: (1) If Pícara has really not been able to 3-color the graph, she won't be able to fool Vivales — eventually step #3 will reveal adjacent vertices of the same color. (2) Because of the random permutations of the colors, Vivales learns nothing about the coloring, except for the fact that Pícara has been successful. That is, if he, too, now wants to 3-color the graph, it will be just as hard for him to 3-color it after going through steps #1–4 above as it would have been before.

To prove the claim that Vivales has learned nothing about the coloring, one argues as follows. Suppose that a third person, Clyde, does not know how to 3-color the graph but *does* know in advance which edge-bar Vivales will grab. Then Clyde could produce the exact same result as Pícara, i.e., the information Vivales receives from Clyde is indistinguishable from what Pícara would have given him. But Clyde could hardly be conveying anything useful about 3-coloring the graph, since he himself does not know a 3-coloring. We say that Clyde "simulates" the role of Pícara. This argument by simulation is the standard way to show that a certain protocol is really a zero-knowledge proof.

Zero-knowledge proof of having found a discrete logarithm. As in §3, suppose that G is a finite group containing N elements (whose group oper-