The problem of determining whether a graph has a 3-coloring is NP-complete, whereas the problem of factoring numbers is not known or believed to be NP-complete. (If this terminology is unfamiliar, that is fine – it is not needed to solve this homework problem.) This motivates the following problem.

A graph $G$ is a finite set $V$ of vertices $v$ together with a set $E$ of edges $e$, each of which connects two distinct vertices, say $v_1$ and $v_2$, in $V$. Two vertices can only have one edge between them. A 3-coloring of a graph is an assignment of the color “red”, “white”, or “blue” to each vertex in $V$ in such a way that for each edge $e$ in $V$, the two vertices $v_1$ and $v_2$ connected by $e$ have distinct colors.

Peggy has a graph $G$ and wants to convince Victor that she knows a 3-coloring of $G$ without giving away any information whatsoever about the coloring. Here is an incomplete description of a zero-knowledge proof that Peggy can use.

1. Peggy draws the graph $G$ on a chalkboard in a classroom. She 3-colors the graph using the 3-coloring she knows and covers each vertex with a Post-it note.
2. Victor comes into the room. He is allowed to remove two Post-it notes, subject to the restriction that __________, and checks that __________.
3. They repeat the protocol many times, but in between each round, Peggy changes the coloring by __________.

**Question 1**: Fill in the blanks, and explain why the protocol will be successful if Peggy has a 3-coloring.

**Question 2**: If this is repeated many times, why should Victor be convinced that Peggy has a 3-coloring? How many times should the protocol be repeated to assure at least a 50% confidence that Peggy can 3-color the graph?

**Question 3**: Explain informally why an observer Eve could simulate the entire protocol without any information from Alice or Victor, which shows that this protocol is indeed zero-knowledge.