Theoretical Cryptography	Manuel Blum and Steven Rudich
HW1	Due: 2/1/06

Give 0-knowledge protocols for the following problems:

1. **Graph 3-Colorability.**

   INSTANCE: Graph $G = (V, E)$.

   QUESTION: Is G 3-colorable? *I.e.* does there exist an assignment $c : V \to \{\text{red, white, blue}\}$ such that for every $\{u, v\} \in E$, $c(u) \neq c(v)$ (that is, no two adjacent vertices have the same color)?

   (If you Google for the answer, you'll find it. Feel free to check your answer with the scribe notes of Trevisan and Wagner's class.)

2. **Graph Edge-Colorability.**

   INSTANCE: Graph G such that each node has degree $\leq d$.

   QUESTION: Can the edges of G be colored using at most d colors, such that all edges incident to a particular vertex are assigned different colors?

   (Easy, but I doubt it has been done directly, so Google won't give this.)

   Aside: It is a theorem of Graph Theory that a graph with nodes of degree at most d can always be edge-colored using at most $d + 1$ colors. At least d colors are necessary. Why?

3. **Graph Vertex-Cover.**

   INSTANCE: Graph $G = (V, E)$, and positive integer B.

   QUESTION: Does G have a vertex cover of size at most B? That is, is there a subset S of V of at most B vertices, such that all edges are incident to at least one vertex in S?

Extra Credit. Give a 0-knowledge protocol for proving that a positive integer of length $2n$ is the product of two n-bit numbers.