Problem Set 8

Due in class on Thursday, December 1, 2005.

In the problems below, "textbook" refers to *Introduction to Cryptography with Coding Theory: Second Edition* by Trappe and Washington..

Problem 36: Zero knowledge interactive proof for 3-colorability

An undirected graph $G = (V, E)$ is said to be 3-colorable if there is an assignment $\gamma : V \to \{1, 2, 3\}$ such that for all edges $\{v, w\} \in E$, $\gamma(v) \neq \gamma(w)$. The problem of testing if an arbitrary graph is 3-colorable is known to be $\mathcal{NP}$-complete. Alice claims to know a coloring γ for the public graph G.

Here is the idea for a zero knowledge interactive proof whereby Alice can demonstrate knowledge of a 3-coloring γ to Bob without revealing any information about γ. Alice generates a random permutation $\rho : \{1, 2, 3\} \to \{1, 2, 3\}$, defines a new coloring of the graph $\gamma' = \rho \circ \gamma$, commits to each of the colors $\gamma'(v)$ for $v \in V$ using bit commitment, and then sends each of the commitments to Bob. Bob picks an edge $\{v, w\}$ of G and asks Alice to reveal the hidden colors corresponding to v and w. Alice does so and Bob verifies that they are different.

(a) Explain why Bob's verification always succeeds if Alice and Bob are honest.

(b) Explain how a dishonest Alice who does not know a 3-coloring of G can fool Bob if she can correctly guess in advance which edge Bob is going to ask about.

(c) Explain why a dishonest Alice who could successfully answer any of Bob's permissible questions in fact does knowq (i.e., could efficiently compute) a 3-coloring of G.

(d) What is the probability that Bob will catch a dishonest Alice who doesn't know a 3-coloring of G on one round of the protocol?

(e) How many times does this protocol need to be repeated in order to make Alice's probability of successful cheating less than 10^{-6}?

(f) Explain why the protocol is zero knowledge.

Problem 37: Secret sharing basics

(a) Textbook, problem 12.3.2.

(b) Textbook, problem 12.3.3.

Problem 38: Secret sharing with cheater

Textbook, problem 12.3.6.

Problem 39: Secret sharing implementation

Textbook, problem 12.4.3.