This problem set is due on: Wednesday, February 16, 2005. Note that Problem 5 is optional. If you turn in a solution to Problem 5, your lowest score among the five problems will be dropped when determining your grade for this problem set.

Problem 1

Suppose \( p \) is a prime and \( g \) and \( h \) are both generators of \( \mathbb{Z}_p^* \). Prove or disprove the following statements about equality of probability distributions:

A: \( \{ x \leftarrow \mathbb{Z}_p^* : g^x \mod p \} = \{ x \leftarrow \mathbb{Z}_p^* : y \leftarrow \mathbb{Z}_p^* : g^{xy} \mod p \} \)

B: \( \{ x \leftarrow \mathbb{Z}_p^* : g^x \mod p \} = \{ x \leftarrow \mathbb{Z}_p^* : h^x \mod p \} \)

C: \( \{ x \leftarrow \mathbb{Z}_p^* : g^x \mod p \} = \{ x \leftarrow \mathbb{Z}_p^* : x^g \mod p \} \)

D: \( \{ x \leftarrow \mathbb{Z}_p^* : x^g \mod p \} = \{ x \leftarrow \mathbb{Z}_p^* : x^{gh} \mod p \} \)

Problem 2

Suppose that the Prime Discrete Logarithm Problem is easy. That is, suppose that there exists a probabilistic, polynomial time algorithm \( A \) that, on inputs \( p, g \) and \( g^x \mod p \), outputs \( x \) if \( p \) is a prime, \( g \) is a generator of \( \mathbb{Z}_p^* \) and \( g^x \mod p \) is prime. Show that there exists a probabilistic polynomial-time algorithm, \( B \), that solves the Discrete Logarithm Problem.

Problem 3

We define the Lily problem as: given two integers \( n \) and \( S \) determine whether \( S \) is relatively prime to \( \phi(n) \). Prove that if it is hard to determine on inputs two integers \( n \) and \( e \) whether \( e \) is relatively prime with \( \phi(n) \), then the RSA function is hard to invert.
Problem 4: Factoring

Let $O_n$ be an oracle that on input $x$ returns a square root of $x \mod n$, if one exists, and ⊥ otherwise. Prove that there exists a probabilistic polynomial-time algorithm that on input an integer $n$ and access to $O_n$ outputs $n$’s factorization.

Problem 5: Factoring and OWF (OPTIONAL)

Prove that if factoring is hard, then one-way functions (as defined in class) exist.