

Homework 2

Instructor: abhi shelat

You may collaborate with other students on the homework but you must submit your own individually written solution and you must identify your collaborators. If you make use of any other external source, you must acknowledge it. You are not allowed to submit a problem solution which you cannot explain orally to the course staff.

Problem 1 *One-way functions based on f_{mult}*

1. Given that the *Factoring assumption* is true, prove that f_{mult} as defined in class is a weak OWF. (Hint: Use Chebyshev's Theorem on density of primes.)
2. Use the weak one-way function f_{mult} to construct a strong one-way function. Prove that your construction satisfies the definition of strong one-wayness without referencing the general hardness amplification theorem.

Problem 2 *Number Theory*

1. Suppose that the Prime Discrete Logarithm problem is easy: That is, suppose that there exists a p.p.t machine A that solves the Prime Discrete problem with probability $2/3$, i.e. on input p, g and $g^x \bmod p$, outputs x if p is prime, g is a generator of Z_p^* and $g^x \bmod p$ is prime. Show that there exists a p.p.t machine B , that solves the Discrete Logarithm Problem. (Hint: Show that given a fixed element g^x in Z_p^* , g^{x+r} is a random element in Z_p^* , if r is a random element in Z_p^* . Finally, using Chebychev's theorem on the density of primes, construct the required p.p.t machine)
2. The Diffie-Hellman problem is as follows: Given input (p, q, g, g^x, g^y) where p is a safeprime, i.e. p is a prime of the form $2q + 1$ where q is prime, g is a generator of a subgroup of order q in Z_p , and $x, y \in Z_q$, compute the element $g^{xy} \bmod p$.

The Square problem is as follows: Given input (p, q, g, g^x) where p is a safeprime, i.e. p is a prime of the form $2q + 1$ where q is prime, g is a generator of a subgroup of order q in Z_p , and $x \in Z_q$, compute the element $g^{x^2} \bmod p$.

Show that the Diffie-Hellman and the Square problem are polynomial-time equivalent. In other words, show that an algorithm that solves the Square problem can be used to solve the Diffie-Hellman problem (with at most a polynomial amount of extra work) and vice-versa.

Bonus Question: Show that if there is a p.p.t machine that solves Diffie-Hellman problem on a random x, y with probability at least $\frac{2}{3}$, then there is a p.p.t machine that solves the Square problem with probability at least $\frac{2}{3}$. (Hint: Use ideas from Part 1 and a generalization of Lagrange theorem taught in class which states that in any group, the order of an element divides the order of the group.)

3. Suppose $p > 2$ is a prime and g and h are both generators of Z_p^* . Prove or disprove the following statements:

- A:** $\{x \leftarrow Z_p^* : g^x \bmod p\} = \{x \leftarrow Z_p^*; y \leftarrow Z_p^* : g^{xy} \bmod p\}$
B: $\{x \leftarrow Z_p^* : g^x \bmod p\} = \{x \leftarrow Z_p^* : h^x \bmod p\}$
C: $\{x \leftarrow Z_p^* : g^x \bmod p\} = \{x \leftarrow Z_p^* : x^g \bmod p\}$
D: $\{x \leftarrow Z_p^* : x^g \bmod p\} = \{x \leftarrow Z_p^* : x^{gh} \bmod p\}$

(Recall that $\{x \leftarrow Z_p^* : g^x \bmod p\}$ is a probability distribution. To show that two distributions are identical prove that each member of one distribution occurs with same probability in both the distribution. To show they are not identical, give a counter example, by finding a member in one distribution, which occurs with different probability in the two distributions.)

Problem 3 *Trapdoor One-way Functions*

Let f be a one-way permutation. In this problem, we will use f to construct a family of *trapdoor* one-way functions G (not one-way permutations!). The idea is to evaluate the function f as usual. The only exception is that when the input is a special value α , then g operates in a way that makes it easy to invert. Define $G = \{g_\beta\}_{\beta \in \{0,1\}^*}$ as follows: g_β is a function $\{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$, where $|\beta| = n$.

$$g_\beta(e, v) = \begin{cases} v & \text{if } f(e) = \beta \\ f(v) & \text{otherwise} \end{cases}$$

Define Gen and the sampling function for the domain of g_β and prove that G is a collection of *trapdoor* one-way functions.

Bonus Question: Show that any one-way function f can also be extended to obtain a collection of *trapdoor* one-way functions.