600.472 Theoretical Cryptography February 12, 2008

Handout 3: Homework 2

Instructor: Susan Hohenberger *TA: Matthew Green*

DUE: February 21, 2008 at the start of lecture.

Problem 1 *(22 points) Arithmetic Warmup*

Do the following problems by hand. Show your work.

1. (6 points) Apply the extended Euclidean algorithm to primes 59 and 17 to find x and y such that $59x + 17y = 1$.
2. (6 points) What is the inverse of 59 (i.e., 8) modulo 17 and what is the inverse of 17 modulo 59?
3. (10 points) Prove that 2 is a generator of $\mathbb{Z}_{59}^*$, while 4 is not a generator of $\mathbb{Z}_{59}^*$. (HINT: Recall, g is a generator of $\mathbb{Z}_p^*$, where p is prime, if and only if $g^a \neq 1 \bmod p$ for every non-trivial divisor $1 < a < p-1$ of $(p-1)$.)

Problem 2 *(20 points) One-way function based on f_{mult}*

Recall the function $f_{mult} : \mathbb{N}^2 \to \mathbb{N}$ defined as $f_{mult}(x, y) = xy$ where $|x| = |y|$. Given that the *Factoring assumption* is true, prove that f_{mult} is a weak OWF. (Hint: Use Chebyshev's Theorem on the density of primes.)

Problem 3 *(28 points) Identical Distributions*

Suppose $p > 2$ is a prime and g and h are both generators of $\mathbb{Z}_p^*$. Prove or disprove the following statements:

A: $\{x \leftarrow \mathbb{Z}_p^* : g^x \bmod p\} = \{x \leftarrow \mathbb{Z}_p^*; y \leftarrow \mathbb{Z}_p^* : g^{xy} \bmod p\}$

B: $\{x \leftarrow \mathbb{Z}_p^* : g^x \bmod p\} = \{x \leftarrow \mathbb{Z}_p^* : h^x \bmod p\}$

C: $\{x \leftarrow \mathbb{Z}_p^* : g^x \bmod p\} = \{x \leftarrow \mathbb{Z}_p^* : x^g \bmod p\}$

D: $\{x \leftarrow \mathbb{Z}_p^* : x^g \bmod p\} = \{x \leftarrow \mathbb{Z}_p^*; y \leftarrow \mathbb{Z}_p^* : (xy)^g \bmod p\}$

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

Problem 4 *(30 points) Simplifying the World's Problems*

A core skill when writing cryptographic proofs is the ability to creatively relate and compare standard problems, which are believed to be hard, to the problem of breaking your construction. In this problem, we are going to practice this skill.

Consider the following problems.

Definition 1 (Computational Diffie-Hellman) *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 $\mathbb{Z}_p$, and $x, y \in \mathbb{Z}_q$, compute the element $g^{xy} \bmod p$.*

Definition 2 (Square) *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 $\mathbb{Z}_p$, and $x \in \mathbb{Z}_q$, compute the element $g^{x^2} \bmod p$.*

Definition 3 (Inverse) *The Inverse 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 $\mathbb{Z}_p$, and $x \in \mathbb{Z}_q$, compute the element $g^{1/x} \bmod p$.*

1. (20 points) 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.

2. (10 points) Show that if the Square problem is hard, then so is the Inverse problem.

Bonus 1 *(10 extra points) Simplifying the World's Worst Problems*

It is very difficult to reason about the trustworthiness of an assumption, especially when the problem is overly complicated. Consider the following example:

Definition 4 (Wild) *The Wild problem is as follows: Given input:*

$$(p, q, g, g^a, g^b, g^{c_1}, \ldots, g^{c_n}, g^{ab/c_1}, \ldots, g^{ab/c_n}, \forall_{\substack{i,j \\ i \neq j}} g^{abc_i/c_j})$$

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 $\mathbb{Z}_p$, and $a, b, c_1, \ldots, c_n \in \mathbb{Z}_q$, compute the element $g^{ab} \bmod p$.*

As a bonus exercise, you are asked to simplify the Wild problem. First, devise a new problem X where the input only contains $O(n)$ terms (and not $O(n^2)$ terms as in Wild). Next, show that if problem X is hard, then so is the Wild problem.