Homework 5

Please submit your homeworks through CS Dropbox:
https://dropbox.cs.princeton.edu/COS433_S2018/HW5

1 Problem 1 (10 points)

Let $\mathbb{G}$ be a cyclic finite group of prime order p. Consider the following commitment scheme:

- The message space is $\mathbb{Z}_p$.
- $\mathsf{Setup}()$: choose a random $g \in \mathbb{G}, g \neq 1$ and a random $a \in \mathbb{Z}_p$, $a \neq 0$, and compute $h = g^a$. The commitment key is g, h.
- $\mathsf{Com}((g,h), m; r)$: output $g^m h^r$, where r is a random element in $\mathbb{Z}_p$.

(a) Show that the scheme is perfectly hiding.

(b) Show that the scheme is computationally binding, assuming the discrete log problem is hard for $\mathbb{G}$.

2 Problem 2 (20 points)

(a) Show that the original version of the decisional Diffie Hellman problem that we saw in class is easy. That is, fix a prime p. You are given

$$(g, g^a \bmod p, g^b \bmod p, h)$$

where g is a random generator of $\mathbb{Z}_p^*$, $a, b \leftarrow \mathbb{Z}_{p-1}$, and h is either $g^{ab} \bmod p$ or $g^c \bmod p$ for a random $c \in \mathbb{Z}_{p-1}$.

Show how to tell whether $h = g^c \bmod p$ or $h = g^{ab} \bmod p$.

(b) Explain why, despite the above attack, the *computational* Diffie Hellman problem might still be hard

(c) Generalize the above attack as follows. Suppose $\mathbb{G}$ is a cyclic finite group of order N, and suppose N has a small factor r. Show that the decisional Diffie Hellman problem can be broken in time proportional to r (and polylogarithmic in N).

(d) A number N is t-smooth if all of its prime factors are at most t. Let $\mathbb{G}$ be a cyclic finite group of order N, where N is the product of distinct prime factors and N is t-smooth for some small t. Show that the discrete log problem is easy in $\mathbb{G}$: given any g and g^a, it is possible efficiently recover a, with a running time that grows with t, but is otherwise logarithmic in N. The Chinese Remainder Theorem will be helpful here.

(e) Show that the discrete log problem is easy over $\mathbb{Z}_N^*$ for any smooth N. That is, if N is t-smooth, you should give an algorithm for the discrete log over $\mathbb{Z}_N^*$ whose running time grows with t, but is otherwise logarithmic in N

Note that the N in part (e) is different from the N in part (d). In part (d), N is the order of the group (the number such that $g^N = 1$), whereas in (e), the order of the group is something very different.

3 Problem 3 (10 points)

The Euler totient function $\phi(N)$ counts the number of elements in $\mathbb{Z}_N^*$, the number of integers in $\{0, 1, ..., N-1\}$ that are relatively prime to N (1 is relatively prime to N, but 0 is not for $N > 1$).

(a) Show that for a prime power $q = p^a$, that $\phi(q) = (p-1)p^{a-1} = \left(1 - \frac{1}{p}\right) q$

(b) Show that for a positive integer N, $\phi(N) = N \times \prod_p \left(1 - \frac{1}{p}\right)$. Here, p varies over the prime factors of N, where each p is counted only once. The Chinese Remainder Theorem will be useful here.

4 Problem 4 (20 points)

Here, we generalized the fact that computing square roots mod a composite is as hard as factoring.

(a) Let $N = pq$ for unknown primes p, q, and suppose that e is prime and divides either $p-1$ or $q-1$, but not both. Show that computing eth roots mod N is as hard as factoring. That is, if you are able to efficiently compute eth roots, then you can factor N.

[Hint: if e divides $p-1$, then how many roots does an eth residue have mod p? What if e does not divide $p-1$?]

(b) Extend the above to handle arbitrary e, as long as e is *not* relatively prime to $\phi(N) = (p-1)(q-1)$. You may assume you know the prime factorization of e. Note that if e *is* relatively prime to $\phi(N)$, computing eth roots is the RSA problem, which is not believed to be as hard as factoring.

For part (b), this means the following cases are possible, and must be handled by your proof:

- e divides both $p-1$ and $q-1$
- e is composite
- e is does not divide $p-1$, but it shares a common factor with $p-1$
- e shares common factors with both $p-1$ and $q-1$ (and maybe not the same common factor)