

## Homework 8

Instructor: Anna Lysyanskaya

Due: April 11, 2007

**Problem 1: Discrete Logarithm Assumption**

The discrete log assumption says:

Let  $Gen(1^k)$  be an algorithm which generates a  $k$ -bit prime  $p$ , and a generator  $g$  of  $Z_p^*$ . We assume that for all PPT adversaries  $\mathcal{A}$  there exists negligible  $\nu$  such that

$$\Pr[(p, g) \leftarrow Gen(1^k); i \leftarrow Z_p; i' \leftarrow \mathcal{A}(p, g, g^i \bmod p) : g^i = g^{i'} \bmod p] = \nu(k)$$

In class used a modified version in which we required that  $i$  be relatively prime to  $p - 1$ :

Let  $Gen(1^k)$  be an algorithm which generates a  $k$ -bit prime  $p$ , and a generator  $g$  of  $Z_p^*$ . We assume that for all PPT adversaries  $\mathcal{A}$  there exists negligible  $\nu$  such that

$$\Pr[(p, g) \leftarrow Gen(1^k); i \leftarrow \{u \in Z_p : \gcd(u, p - 1) = 1\}; i' \leftarrow \mathcal{A}(p, g, g^i \bmod p) : g^i = g^{i'} \bmod p] = \nu(k)$$

We proposed a hash function and showed that if this modified discrete log assumption holds, then the hash function is collision resistant.

Now, prove that the modified assumption is equivalent to the discrete log assumption.

- First prove that if the modified assumption holds, then the original discrete log assumption holds.

Hint: First show that discrete log is randomly self reducible, then proceed as we did in problem 2 of homework 5.

- Then prove that if the original discrete log assumption holds, then the modified assumption holds.

Hint: Recall that one in  $k$   $k$ -bit numbers is a prime.

**Problem 2: Collision Resistant Hash Functions**

Consider the following hash function family:

$Gen(1^k)$ : generate 2  $k$  bit primes  $p, q$ . Let  $n = pq$ . Choose random  $y \leftarrow QR_n$ . Output  $n, y$ .  
 $H_{(n,y)}(x) = y^x \bmod n$

- What is the definition of a collision resistant hash function?
- Recall that the RSA assumption says that, given an RSA public key  $(n, e) \leftarrow G_{RSA}(1^k)$  and a random  $y \in Z_n^*$ , it is hard to find  $x \in Z_n^*$  such that  $x^e = y$ . In experiment notation: for all probabilistic polynomial-time adversaries  $\mathcal{A}$ , there exists a negligible function  $\nu(k)$  such that

$$\Pr[(n, e) \leftarrow G_{RSA}(1^k); y \leftarrow Z_n^*; x \leftarrow \mathcal{A}(n, e, y) : y = x^e] = \nu(k)$$

Prove that if the RSA assumption holds, then the hash function described above is collision resistant (use a reduction as usual).

Hint: Show that if we had an adversary which could find collisions for this hash function family, then we could build an algorithm to find a multiple of  $\phi(n)$  given only  $n$ . Then show that this would allow us to break the RSA assumption.

### Problem 3: Broken Signatures

A signature scheme can be broken in a number of ways. It can be shown to be existentially forgeable, which means that the adversary can find some message for which it can forge a signature. It can be target-message forgeable, which means that an adversary can forge a signature for any given message. Or, in the worst case, its secret key can be completely recoverable.

In order to break a signature scheme, different flavors of attacks can be launched: a public-key only attack where the adversary only gets to see the public-key, or an interactive attack where the adversary asks for signatures on messages of his choice.

Consider the following signature scheme: The public key of this signature scheme consists of a Blum integer  $n = pq$ . (Recall that Blum integers have the property that  $-1$  is a nonsquare mod  $p$  and mod  $q$ ). The secret key is  $n$ 's factorization. The message space is  $\text{QR}_n \cup \text{QNR}_n$ . A signature  $\sigma$  on message  $m$  is computed as follows: if  $m$  is a quadratic residue, then  $\sigma$  is some arbitrary square root of  $m$ . Otherwise,  $\sigma$  is some arbitrary square root of  $-m$ .

Prove the following facts about this signature scheme:

- a. With a public-key only attack (i.e., without access to the signer, only the signer's public key), a target-message attack on this signature scheme is as hard as factoring. (Give a reduction.)
- b. This signature scheme is existentially forgeable with a public-key only attack. (Describe an attack.)
- c. The secret key of this signature scheme can be recovered by an adversary making adaptive queries to the signer. (Describe an attack.)