Handout 8: Digital Signatures

Boaz Barak

Total of 115 points.
Exercises due November 22nd, 2005 1:30pm.

Exercise 1 (Simple RSA-based Signatures are not secure, 15 points). Consider the following simple signature schemes based on the RSA permutation, where signing is by decrypting/inverting the permutation: **Public key:** $n = pq$ for p, q random primes, $e \in \mathbb{Z}^*_{\phi(n)}$, **Private key:** $d = e^{-1} \mod \phi(n)$ **Signing:** signature for m is $m^d \pmod n$ **Verifying:** to verify σ is a signature for m, verify that $m = \sigma^e$.

1. Prove that this scheme is *not* a secure signature scheme.
2. Prove that this scheme is insecure even if we consider a weaker definition of security where the attacker has to forge a message given to it as input. That is, the attacher first gets an input message m, during the attack can query the signing oracle only on messages $m' \neq m$ and at the end to succeed needs to output a valid signature for m.

Exercise 2 (Collision resistant hash functions for arbitrary length, 20 points). Prove the following: if there exists a collision resistant hash function collection mapping $n+1$ bit strings into n bits strings, then there exists a collection mapping arbitrary length bit strings into n bit strings.

Exercise 3 (Hash functions have at most $2^{n/2}$ security, 20 points). Prove that that there is no collection of functions $\{h_k\}_{k\{0,1\}^*}$ with $h_k : \{0,1\}^{2n} \to \{0,1\}^n$ that is $(102^{n/2}, 1/10)$-collision resistant.

Exercise 4 (Signatures for identification protocols, 60 points). Consider the identification problem (i.e., there's a "box" that controls access to some resource and authorized people are given some secret information that enables them to use the resource, but unauthorized people cannot do so, even if the know the contents of the box).

1. Consider the weakest security definition of this problem where the only attack we're considering is an adversary that knows the contents of the box (but can't construct a "fake box" or listen on conversations between honest users and the box). Construct a non-interactive (i.e., a protocol consisting of a single message from the user to the box) protocol solving the identification problem and prove its security.
2. Construct a non-interactive identification protocol that remains secure under the stronger attack where an adversary may listen in on other conversations and also construct "fake boxes". Prove the security for your protocol. You may assume that all parties have access to a perfectly synchronized global clock.

3. One problem in identification protocols is that authorized people may provide their secret information to their friends (or sell it) to allow them also to access the resource. Can you design a (possibly interactive) protocol where there's a strong disincentive for them to do so? (You may assume that each person has a secret, such as their social-security number, that is known also to the central authority, but they are reluctant to give to their friends. However, the protocol should not allow an eavesdropping adversary or even a fake box adversary to learn this secret.)