FOUNDATIONS OF CRYPTOGRAPHY

CS668A	*Homework 4*
Fall 2004	*Due: December 2, 2004*
Prof. Rebecca N. Wright	

If at all possible, please use an appropriate text-processing package to write up your solutions, such as LaTeX or MS-Word. You may leave space for mathematical formulas and drawings and insert them by hand.

Each problem is worth 10 points.

Problem 1: Let $n = pq$ be an RSA modulus, where $p > 3$ and $q > 3$ are distinct primes.

Suppose $\alpha \in \mathbb{Z}_n^*$ such that $\mathrm{ord}(\alpha) = \phi(n)/2$. It can be proven that if $\beta = \alpha^n \pmod{n}$ and $a = \log_\alpha \beta$, then $n - a = \phi(n)$. [You may use this fact without proof.]

Now, suppose that you are given $\alpha \in \mathbb{Z}_n^*$ such that $\mathrm{ord}(\alpha) = \phi(n)/2$, and further suppose that you have a discrete logarithm oracle for α (so that given any $\beta \in \langle\alpha\rangle$, the oracle returns $a = \log_\alpha \beta$ to you). Show how to use this to factor n.

Problem 2: Suppose Alice uses the same cryptosystem both for encryption and for digital signatures. (This requires a system for which encryption and decryption commute, such as RSA). Further suppose that she uses the *same* public and private key for both her encryptions and her signatures, (that is, she uses the same private key to decrypt ciphertexts and to sign messages, and the corresponding public key can be used for others to encrypt messages and to verify signatures), and that she is willing to sign any message presented to her.

Now suppose an attacker overhears a ciphertext c encrypted with Alice's public key, and wishes to find the cleartext m.

a. Consider the case that Alice does not use the hash-then-sign paradigm, and show that the attacker can always succeed in the above goal.

b. Now consider the case that Alice uses the hash-then-sign paradigm. Can the attacker succeed in the above goal? What properties are needed for h in order to thwart the attacker?

Problem 3: Show that if the same value k is used for multiple messages in the Schnorr signature scheme, then an attacker can perform a total break of the system.