CS 758

Assignment 2

due by Noon on Friday, October 18, 2013

General Instructions

- Assignments must be handed in by the designated time. I prefer an electronic copy (.pdf file) submitted by email, but I will also accept a hard copy that is dropped off in class or at my office. Due to the large number of students in the class, no extensions will be given.
- You are permitted to discuss assignment questions *informally* with a partner. However, when you hand in the assignments you must indicate who you had discussions with, and all solutions must be written up separately. No "copied" solutions or computer code are allowed; copied assignments are considered to be plagiarism and are subject to severe penalties.
- It is recommended that you attempt to solve every question on your own. If you do use an external information source (a book or a research paper, for example), give an appropriate citation.
- Computational questions can be done using any desired programming tools, languages or calculators. Maple is **strongly recommended** as the easiest way to do the questions. Please include all source code, and sufficient output so I can verify the main steps in the computations.
- I am available to provide extra help or hints if you get stuck on a question.

Questions

In the questions below, numbered theorems, etc., refer to the mathematics notes on the course web page.

1. Consider the following possible identification scheme. Alice possesses a secret key $n = pq$, where p and q are prime and $p \equiv q \equiv 3 \pmod 4$. The value of n will be stored on Alice's certificate. When Alice wants to identify herself to Bob, say, Bob will present Alice with a random quadratic residue modulo n, say x. Then Alice will compute a square root y of x and give it to Bob. Bob then verifies that $y^2 \equiv x \pmod n$.

   (a) Explain why this scheme is insecure against Bob, i.e., show how Bob can impersonate Alice with some non-negligible probability after Alice identifies herself to him.

   (b) Is the scheme zero-knowledge from the point of view of an observer, say Oscar, who simply watches the protocol being executed by a verifier who is choosing challenges randomly? Explain.

2. Consider the mutual authentication scheme defined in pages 21–25 of the FIPS 196 standard. (This document is not currently available from the NIST website due to the U.S. government shutdown, but a copy is posted on the course webpage.) Show that this scheme is insecure if the optional field $[A]$ is omitted from sS_B and the optional field $[B]$ is omitted from sS_A.

3. Give a complete analysis of the adversary's probability of successful impersonation in the *Public-Key Mutual Identification Protocol* from slides 134–135. You should explicitly state all your assumptions, and your answer should be given in terms of q, k and ϵ. You can assume that the adversary is passive during an information-gathering phase and the signature scheme is secure in a known-message attack. The security assumption for the signature scheme will specify the number of previous signatures observed by the adversary, before he attempts to forge a new signature, to be q. There are two signatures created in each session of the identification protocol, one by each participant. These signatures are created using two different keys. Therefore, in the analysis of the protocol, it is reasonable to make the assumption that at most q sessions of the protocol take place before the adversary carries out an impersonation attack.

4. Show that the *Schnorr Identification Scheme* is not secure against an active adversary who changes the messages that are sent *from Alice to Bob*.

5. Consider the following *Diffie-Hellman* type identification scheme. Alice has a public key $v = g^a$ and a private key a. Assume that g is a primitive element in a $\mathbb{Z}_p{}^*$ where p is prime, and assume that the Discrete Logarithm Problem in $\mathbb{Z}_p{}^*$ is infeasible. Bob chooses a random b, computes $w = g^b$, and sends w to Alice. Alice computes $K = w^a$ and sends it to Bob. Bob accepts if and only if $K = v^b$.

   (a) Is the above-described scheme *zero-knowledge* against an honest verifier (i.e., a verifier who chooses the challenges w as described above)?

   (b) Is the above-described scheme *zero-knowledge* against a dishonest verifier (i.e., a verifier who chooses the challenges w in some other way)?