CS 758

Assignment 2

due by 1:00 PM on Thursday, June 9, 2016

General Instructions

- Assignments must be handed in by the designated time. Please hand in a *hard copy*. 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 copying of solutions or computer code is 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

1. Suppose that Alice, Bob and Charlie all share the same secret key K. Prove that there is no secure identification scheme based on the secret key K that allows Alice to identify herself to Bob. (This question has a rather short answer!)

2. Consider the now-obsolete mutual authentication scheme defined in pages 21–25 of FIPS 196; see

   `http://csrc.nist.gov/publications/fips/fips196/fips196.pdf`

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

4. 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 $K = v^b$. Prove that the above-described scheme *zero-knowledge* against an honest verifier (i.e., a verifier Bob who chooses the challenges w as described above). That is, show that it is possible to simulate transcripts of **Bob's view of the protocol**.

5. Prove that the identification scheme presented on slide 111 is not secure if ID strings and random challenges are *not* required to have a prespecified fixed length.

   Notes:

   (a) You can assume that the users' IDs are represented in ASCII.

   (b) Remember that, before the protocol is executed, each user claims an identity to the other user, so each user has an "intended peer". The protocol can proceed only if these two users have a shared secret key.

   (c) Hint: Suppose the two users who share a key K are Ali and Alice.