CSCI 283 and CSCI 172- Graduate and Undergraduate Computer Security - Fall 2010
George Washington University

Extra Credit HW
due 10 December, 6 pm.
75 points

Policy on collaboration: All examinations, papers, and other graded work products and assignments are to be completed in conformance with The George Washington University Code of Academic Integrity. You may discuss HWs among yourselves, and work on them in groups. However, each student is expected to write his or her own HW out independently; you may not copy one another's assignments, even in part. You may not collaborate with others on the test and final.

You are expected to cite all your sources in any written work that is not closed book: papers, books, web sites, discussions with others - faculty, friends, students. For example, if, in a group, one student has a major idea that leads to a solution to a HW problem, all other students in the group should cite this student.

You may not refer to solutions to previous years' problem sets, or ask for help students from previous years, except the TA.

Any violations will be treated as violations of the Code of Academic Integrity.

PLEASE submit all HW on Blackboard only. Name your files:
CS283_HW3_LASTNAME_FIRSTNAME.zip or .rar or
CS172_HW3_LASTNAME_FIRSTNAME.zip or .rar

For the Encrypted Key Exchange (EKE) authentication protocol described in class (*Authentication* slide set), answer the following:

A. (10 points) Describe what the security goals are. (A few sentences).

B. (10 points) Describe what the assumptions are. (One-third page)

C. (25 points) Why is the protocol secure given the assumptions? (One page)

D. (15 points) What would an adversary's goals be? How might an adversary achieve these goals (note that an assumption would need to be violated)? (Half a page)

E. (15 points) Suppose you were to prototype the protocol in software, using Java, C or C++. The input to your program would be interactive. You would use standard libraries for the cryptographic primitives – encryption, secure hash functions and random number generator algorithms. What would your choices for the various cryptographic primitives be? Why? (Half a page)