

CSCI 283 and CSCI 172- Graduate and Undergraduate Computer Security - Fall 2006
George Washington University

Homework 3

due 27 November, 6 pm.

100 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

ASSIGNMENT:

Implement the two challenge-response protocols – S/Key and Encrypted Key Exchange – described in class. The input to your program will be interactive. You may use standard libraries for the cryptographic primitives – encryption, hash and random number generator algorithms.

Submit a written report that describes what your program does. Clearly describe your choices for the various cryptographic primitives, and reasons for the choices. Describe the weaknesses of your implementation. Include all references, including code libraries used. In an appendix to the report, also submit (a) all your code, and (b) a sample input and output to demonstrate that the code works.

You may use Java, C, C++ or Python for this assignment. Your code should run on a seas account. A large fraction of your grade will depend on how well-documented your code is, and how easy it is for the TA to understand.