

CSCI 283 and CSCI 172- Graduate and Undergraduate Computer Security - Fall 2005
George Washington University

Homework V

due 16 November, 6 pm.

50 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.

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

PLEASE submit this HW on Blackboard only. One compressed file should contain all your code. Name your files:

CS283_HW1_LASTNAME_FIRSTNAME.doc or .pdf

CS172_HW1_LASTNAME_FIRSTNAME.doc or .pdf

1 (20 points). Your teacher needs to create random IDs for each student in the class so as to be able to post grades in a public place yet maintain student privacy. Her goal is to ensure that the student can check his or her own grade, but that nobody may determine another persons grade. She decides to use encryption. She encrypts each students name in one of the following ways, and gives the student the ciphertext as his or her random ID. She then lists the students grade next to the ciphertext corresponding to the student.

For each of the following, state why or why not its use would be appropriate for the problem. In particular, describe vulnerabilities and attacks and their expense to the attacker, and the *expense of a secure method* to the professor. Assume that there are n students in the class, that the professors public key is known widely, that all private keys are well protected and revealed only to persons mentioned, that the list of students in the class is publicly available, and that, in accordance with good security practice, the professor makes known the method she uses.

- a. Encrypting student names with her private key from her public/private key pair.
- b. Encrypting student names with her public key.
- c. Encrypting student names with a shift cipher, key unknown to anyone but her.
- d. Encrypting student names with a substitution cipher, key unknown to anyone but her.
- e. Encrypting student names with a private key block-cipher protocol, using a different private key for each student, and providing the student with their private key.
- f. Encrypting student names with a private key block-cipher protocol, using the same private key for each student, and not providing the key to any student.
- g. Which of the above methods allow for:
 - i. a known plaintext attack?
 - ii. a known ciphertext attack?
 - iii. a chosen plaintext attack?
 - iv. a chosen ciphertext attack?

2 (10 points). Suppose there are n students in a class who want to send encrypted messages to one another.

- a. Suppose they use private key encryption.
 - i How many keys would each student have to manage? Why?
 - ii. How many different keys would exist in the system? Why?
- b. Suppose they use public key encryption. Answer i and ii above.

3 (10 points). Suppose Alice and Bob have RSA public keys in a file on a server. They communicate regularly using authenticated, confidential messages. Eve wants to read the messages but is unable to crack the RSA private keys of Alice and Bob. However, she is able to break into the server and alter the file containing Alice and Bob's public keys.

- a. How should Eve alter that file so that she can read confidential messages sent between Alice and Bob, and forge messages from either?
- b. How might Alice and/or Bob detect Eve's subversion of public keys?

4 (10 points).

- a. Is the identity function, which outputs its own input, a good candidate for a secure hash function? Why or why not?
- b. Is the *sum* program, which exclusive or's all words in its input to generate a one-word output, a good cryptographic checksum function? Why or why not?