

**CSCI 283 and CSCI 172- Graduate and Undergraduate Cryptography - Spring 2005**  
**George Washington University**

**Homework I**

due 27 September

Total 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.

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

**PLEASE submit all HW on Blackboard only. Name your files:**

**CS283\_HW1\_LASTNAME\_FIRSTNAME.doc or .pdf or**

**CS172\_HW1\_LASTNAME\_FIRSTNAME.doc or .pdf**

1a. (5 points) Chapter 2, exercise 1a. Consider a computer system with three users: Alice, Bob and Cyndy. Alice owns the file *alicerc*, and Bob and Cyndy can read it. Cyndy can read and write Bob's file *bobrc*, but Alice can only read it. Only Cyndy can read and write her file *cyndyrc*. Assume that the owner of each file can execute it. Using rights read, write and execute, denoted r,w,x respectively, create the access control matrix.

b. (5 points) For the problem in 1a, also create the access control lists, and the capability lists.

2. (10 points) Chapter 1, exercise 1. Classify each of the following as a violation of confidentiality, of integrity, of availability, or of some combination thereof.

a. John copies Mary's homework.

b. Paul crashes Linda's system.

c. Carol changes the amount of Angelo's check from \$100 to \$ 1000.

d. Gina forges Roger's signature on a deed.

e. Rhonda registers the domain name "AddisonWesley.com" and refuses to let the publishing house buy or use that domain name.

f. Jonah obtains Peter's credit card number and has the credit card company cancel the card and replace it with another card bearing a different account number.

g. Henry spoofs Julie's IP address to gain access to her computer.

3. (miscellaneous questions)

a. (5 points) Using the six primitive commands in section 2.3, write a command *copy\_all\_rights(p, q, s)* that copies all rights that *p* has over *s* to *q*. (Your answer should read like the example at the bottom of page 39).

b. (3 points) Chapter 1, exercise 4. Given an example of a situation in which a compromise of confidentiality leads to a compromise in integrity.

c. (7 points) Chapter 1, exercise 9. Policy restricts the use of electronic mail on a particular system to faculty and staff. Students cannot send or receive electronic mail on that host. Classify the following mechanisms as secure, precise or broad.

i. The electronic mail sending and receiving programs are disabled.

ii. As each letter is sent or received, the system looks up the sender (or recipient) in a database. If that party is listed as faculty or staff, the mail is processed. Otherwise, it is rejected. (Assume that the database entries are correct).

iii. The electronic mail sending programs ask the user if he or she is a student. If so, the mail is refused. The electronic mail receiving programs are disabled.

4a. (5 points) Consider the Shamir secret sharing scheme studied in class, with  $t = 4$  and  $n = 6$ . Suppose four of the six shares are 1, 0, 3, 5, corresponding to values of  $x = 1, 2, 3, 4$  respectively, and

the operations are modulo 7. What is the value of the secret?

b. (5 points) In a general secret sharing scheme, assume that one share takes up one unit of space, and that one multiplication/division takes one unit of time, and that addition and subtraction take negligible time. How much space does a  $(t, n)$  secret sharing scheme require? How much time is required to generate the shares, and how much to reconstruct the secret?

5. (For this problem, you will need to rely on your ability to think abstractly). Consider a graph with vertices  $V$  and edges  $E$ , where  $(v_i, v_j) \in E \Leftrightarrow v_i, v_j \in V$  and there is an edge from  $v_i$  to  $v_j$ .  $(v_i, v_i)$  is in  $E \forall v_i$ . Suppose these vertices represent states of the system. Suppose an edge represents a possible transition, i.e. if there is no edge from  $v_i$  to  $v_j$ , the system cannot directly transition from  $v_i$  to  $v_j$  (it could, however, do so along a path through other vertices). Example graphs are the one shown in class, and the one in the text, pg. 96, chapter 4.

A. Show that if  $V = V_1 \cup V_2$ , where  $V_1 \cap V_2 = \emptyset$ , and there is no edge from any vertex of  $V_1$  to any vertex of  $V_2$  and vice versa, the following are true:

a. (2 points) If  $V$  is the set of secure states, the system is secure.

b. (4 points) If  $V_1$  is the set of secure states, and  $V_2$  the set of non-secure states, the system is secure.

c. (1 point) If  $V_2$  is the set of secure states, and  $V_1$  the set of non-secure states, the system is secure.

B. In addition to the assumptions of A, suppose that, given any  $v_i, v_j \in V_1$ , there is a path from  $v_i$  to  $v_j$ . Show that the following are true:

d. (6 points) If the set of secure states is  $V'_1 = V_1 \setminus \{v\}$  for any  $v \in V_1$ , and the set of non-secure states is  $V'_2 = V_2 \cup \{v\}$ , the system is insecure. In particular, show that it can end up in exactly one of the non-secure states from any secure state it starts in.

e. (4 points) If the set of secure states is  $V'_2 = V_2 \cup \{v\}$  for any  $v \in V_1$ , and the set of non-secure states is  $V'_1 = V_1 \setminus \{v\}$ , the system is insecure. In particular, show that it can end up in a non-secure state only when it starts in a particular secure state. What state is that?

f. (3 points) Given  $V$  and  $E$ , define a maximal set of secure states  $V' \subseteq V$  as a set of states such that (a) the given system is secure with respect to it, and additionally, (b) when any vertex  $v$  not in  $V'$  is added to  $V'$ , the system is insecure. Show that  $V_2$  is a maximal set of secure states. You may use any of the results derived above.

6. Table 1 provides the number of households, in millions, for a given heated floor space area (represented by  $H$ ) and a given family income (represented by  $I$ ). So, for example,  $p(500, 6000) = 1.9$ .

a. (6 points) Consider the function  $p : H \times I \rightarrow \mathcal{R}$  represented by the lookup table, where  $r \in \mathcal{R}$  is the number of households, in millions, i.e.  $r$  is a real number. Suppose the protection function  $m$  for  $p$  provides the values of the lookup table, except when that value is  $Q$  or smaller than 5 (million), when  $m$  returns an error message “relative standard error too high”. Suppose the security policy is to report all values of the lookup table except when the value is  $Q$  or 2 (million) or smaller. Is  $m$  secure? Is it precise? Is it broad?

**Table 1: Example Without Disclosure**

**Number of Households by Heated Floorspace and Family Income  
(Million U.S. Households)**

Heated Floor Space sq ft	1990 Family income							
	Total	Less than \$5000	\$5000 to \$9999	\$10000 to \$14999	\$15000 to \$24999	\$25000 to \$34999	\$35000 to \$49999	\$50000 or more
Fewer than 600	8.0	1.5	1.9	1.6	1.5	.8	.5	.3
600 to 999	22.5	2.0	3.7	4.1	5.5	3.4	2.7	1.2
1000 to 1599	26.5	1.1	3.2	3.2	5.2	5.1	5.5	3.3
1600 to 1999	12.6	.3	1.0	1.1	2.2	2.3	2.6	3.1
2000 to 2399	9.0	Q	.5	.6	1.3	1.3	2.3	2.8
2400 to 2999	7.8	.2	.3	.5	1.0	1.4	1.7	2.7
3000 or more	7.4	Q	.2	.3	.7	1.0	1.3	3.8

NOTE: Q -- Data withheld because relative standard error exceeds 50%.

SOURCE: "Housing Characteristics 1990", Residential Energy Consumption Survey, Energy Information Administration, DOE/EIA-0314(90), page 54.

b. (4 points) Consider another function  $q : H \times I \rightarrow \mathcal{R}$  which provides the total number of households, in millions, over all incomes, independent of the family income requested. So, for example,  $q(500, 6000) = 8$ . Suppose  $m_q$  is the protection function for  $q$  and is  $q$  itself. Suppose the confidentiality policy  $c$  is  $c : H \times I \rightarrow H$ . Is  $m_q$  secure? Is it precise?

c. (3 points) Consider  $m$  of (a) above. Is it secure as a protection function of  $q$  with respect to confidentiality policy  $c$  above? Why or why not?

d. (7 points) Consider the function  $p$  above, and the protection functions  $m$  and  $m_q$ . Suppose the confidentiality policy is  $c' : H \times I \rightarrow A$  where

$$c'(h, i) = \begin{cases} (h, i) & h \geq 2000 \text{ and } i \geq 15,000 \\ h & \text{else} \end{cases}$$

i.e. both area and household income may be revealed if area is larger than 2000 square feet and household income is larger than 15,000, but only area may be revealed otherwise. Is  $m$  secure? Is it precise? Is  $m_q$  secure? Is it precise?

7. Consider a function  $r : R \times G \rightarrow \mathcal{R}$  where  $\mathcal{R}$  is the set of real numbers,  $R$  the set of races,  $R = \{\text{African-American, Asian-American, Caucasian-American, Hispanic-American, Other}\}$ , and  $G$  the set of genders,  $G = \{\text{male, female}\}$ . The function  $r$  provides the average Social Security pay obtained by individuals in a particular database according to race and gender, so, for example,  $r(\text{Hispanic-American, female})$  is the average Social Security obtained by female Hispanic-Americans in the database. The security policy is that  $r(\text{race, gender})$  should return an error if there are fewer than 5 individuals of that particular race and gender, i.e. in the example above, if the number of Hispanic-American females is smaller than 5,  $r$  should return an error.

a. (4 points) Suppose  $m_1$  and  $m_2$  are protection functions, such that  $m_1(\text{race, gender})$  returns the value of  $r(\text{race, gender})$  except when the number of individuals of that race is 5 or fewer, and  $m_2(\text{race, gender})$  returns the value of  $r(\text{race, gender})$  except when the number of individuals of that gender is 5 or fewer. Is  $m_1$  secure? Is  $m_2$  secure?

b. (6 points) Define  $m_3 = m_1 \cap m_2$  as the function that returns the value of  $r$  when both  $m_1$  and  $m_2$  provide it, and returns an error otherwise. Is  $m_3$  secure? Is it precise?