

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

**Homework II**

due 12 October, 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 all HW on Blackboard only. Name your files:**

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

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

1.

a. (2 points) Encrypt the following plaintext using the Caesar cipher with shift = 21:

CAN I GO HOME NOW?

b. Decrypt the following ciphertexts, encrypted using the Caesar cipher with unknown shift:

i. (2 points) xibut gps mvodi

ii. (2 points) ufw kc

c. Provide the following (1 point each):

i.  $3^{-1} \pmod{11}$ ii.  $5^2 \pmod{11}$ iii.  $\frac{5}{3} \pmod{11}$ iv.  $\frac{7}{2} \pmod{11}$ 

2.

a. (4 points) Suppose  $y = 2x + 7 \pmod{23}$  is the encryption function of an affine cipher. What is its decryption function?b. (1 point) Encrypt  $x = 8$  using the cipher of (a)c. (1 point) Decrypt  $y = 3$  using the cipher of (a)d. (4 points) How many distinct affine ciphers are there over  $\mathcal{Z}_{12}$ ? Count the identity as one cipher.

3. (10 points)

Let  $y = DES(x, K)$  represent the encryption of plaintext  $x$  with key  $K$  using the DES cryptosystem. Suppose  $y'$  is the encryption of the bitwise complement of  $x$  with the bitwise complement of the key  $K$ . Show that  $y'$  is the complement of  $y$ , i.e. if the plaintext and the key are complemented, then so is the ciphertext.

More formally, if  $y = DES(x, K)$  and  $y' = DES(\bar{x}, \bar{K})$ , where  $\bar{x}$  denotes the bitwise complement of  $x$ , prove that  $y' = \bar{y}$ . Note that this can be proved for any S-box structure.

Is this a vulnerability? If so, what kinds of cryptanalysis does it make DES vulnerable to?

Make sure you provide all steps for full credit.

4. Suppose  $o(X)$  is one of TOP SECRET (TS), SECRET (S), CONFIDENTIAL (C), PUBLIC (P); and  $TS > S > C > P$ . Suppose further that the compartments in the database are: Tests, Solutions, Grades, Slides. Figure 1 shows the domination relationships among the various nodes, for example,  $v$  dominates  $u$ . The arrows are directions of allowed information flow in the Bell-La Padula model. Let  $(o(x), U(X))$  be the pair denoting the position of  $X$  in the access hierarchy, where  $U \subset \{Tests, Solutions, Grades, Slides\}$ . Answer the following (1 point each)

a. Suppose  $z$  is  $(P, \{Slides\})$ .i. Can  $u$  access data from the compartment Slides that is classified P?

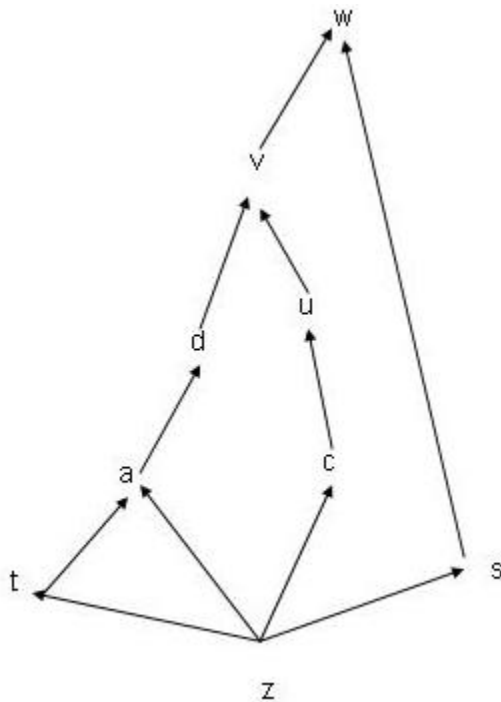


Figure 1:

- ii. Can a be prevented from accessing data from the compartment Slides that is classified P?
- iii. Can a be prevented from accessing data from the compartment Slides that is classified C?
  - b. Suppose further that u is (P, {Slides}).
- iv. Can c be classified (P, {Slides})?
- v. Can c be classified (P, {Slides, Tests})?
- vi. Suppose further still that d is classified (TS, {Tests, Slides}). What is the minimum classification of v?
  - c. Suppose s is classified (P, {Slides}).
- vii. Ignoring the previous given values of u and d, and taking into consideration only the value of z, are all the possible domination relationships shown in the graph?
- viii. If not, what three other edges representing these relationships would provide all the required information in graphical form?
  - d. Assuming (a), (b), (vi) and (c), i.e. the given values for z, u, d and s
- ix. Redraw the graph so that vertices with the same pairs are collapsed into one node bearing the names of all the vertices corresponding to it.
- x. Provide one possible pair of o and compartments for each of the vertices on the new graph.

5. Shannon’s condition for perfect secrecy is that, on receiving the ciphertext, the adversary should not be able to make a guess on the key or message that is better than random (or better than the

guess they would have made before receiving the ciphertext). Are the following ciphers perfectly secret? Why or why not?

- a. (3 points) The one-time pad, with a message of size two bytes and a key of size one byte, repeated.
- b. (3 points) The Feistel cipher, acting on two bytes, with a two byte key.
- c. (4 points) A single SPN layer with message length = key length.