School of Information Technology
IIT Kharagpur

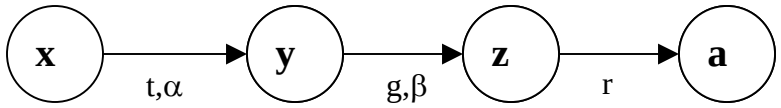
Course Id: IT60112 Information and System Security **Mid-semester Examination**

Date: February 22, 2006 **Total Time: 2 Hours**
Max. Marks: 80

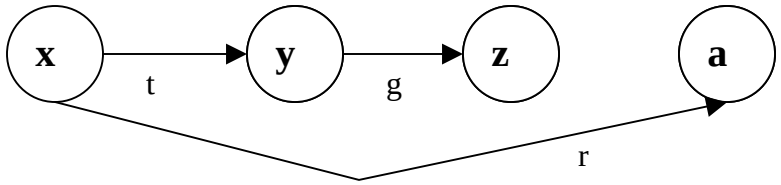
Instructions: Answer all questions. You may answer the questions in any order. However, all parts of the same question must be answered together. Clearly state any reasonable assumption you make.

1. Consider the following pair of initial and final graphs representing protection states of a system. t and g stand for take and grant rights while α, β and r are arbitrary rights.

Initial



Final



Is there a valid sequence of graph rewriting rules to achieve the final state from the initial state? If yes, draw each intermediate graph, clearly identifying the rule that was applied at each step. If no, clearly explain why it cannot be achieved. **[10]**

2.

(a) Why is Bell LaPadula model called a Lattice model of security?

(b) Given the security levels Top Secret (TS), Secret (S), Confidential (C) and Unclassified (U) (ordered from highest to lowest) and categories A, B and C, specify which types of access (read, write, append, execute) will the following subjects have on the objects under Bell-LaPadula Model (For each subject specify the type of access on each object).

Subject	Object
Ankur (TS, {A, B, C})	firstfile (S,{B, C, A})
Anita (C, {C})	secondfile (C, {B, C})
Atul (S, {A, C})	thirdfile (C, {A, C})
Anil (TS, {A, C})	fourthfile (C, {A})

(c) If we consider the above levels to be integrity levels instead of security levels (with the same definition of dominate relationship), then specify which types of access (read, write and execute) will be allowed for the above subjects and objects under Biba's Low Water Mark policy? **[8+4+8=20]**

3.

(a) Define an Information Transfer Path
(b) State Biba's Ring Policy
(c) Prove or Disprove the theorem that if there is an Information Transfer Path from object $o_1 \in O$ to object $o_{n+1} \in O$, then enforcement of the Ring Policy requires that $i(o_{n+1}) \leq i(o_1)$ for all $n > 1$ where O is the set of objects and i denotes the integrity level.
(d) State Biba's Low Water Mark policy (denoted by LWM2) is such a way that integrity levels of objects decrease instead of that of subjects.
(e) Does the above theorem hold for LWM2? If yes, prove it. If no, give a counterexample.

[4+4+4+4+4=20]

4.

(a) What is the difference between certifications and enforcements in the Clark-Wilson's Integrity policy?
(b) State the security requirements of a commercial system as suggested by Lipner.
(c) Explain how Clark Wilson's Integrity policy can meet Lipner's requirements of a commercial security system. **[2+3+5=10]**

5.

(a) State the Chinese Wall Security Policy.
(b) Consider an invest banking consultancy company (IBCC) which deals with the following Industry sectors and company data sets. How many employees does IBCC need to handle all the company accounts if (i) Chinese Wall Security Policy – only Simple Security Condition is enforced (ii) Chinese Wall Security Policy – Both Simple Security Condition and *-property are enforced.

Industry Sector	**Company**
Banking	SBI
	UBI
	CB
	AMEX
Oil	Enron
	Shell
	Amoco
	BP
Steel	Mittal
	Tata

(c) If Rohit, Sumit and Geeta are working in IBCC, draw a possible Access Control Matrix (at the level of company dataset) that needs to satisfy only the Simple Security Condition of the Chinese Wall Security Policy, and at the same time, the maximum number of accounts is handled.
(d) With the Access Control Matrix you have specified above, assume Abhik joins IBCC, draw a possible Access Control Matrix (at the level of company dataset) that needs to satisfy both the Simple Security Condition and the *-property of the Chinese Wall Security Policy, and at the same time, the maximum number of accounts is handled.

[5+5+5+5=20]