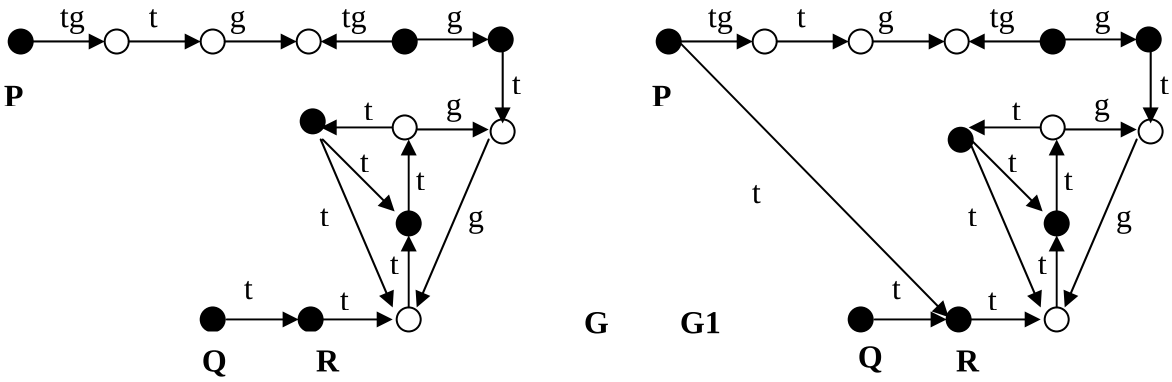
School of Information Technology
IIT Kharagpur

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

Date: February 20, 2012 **Total Time: 2 Hours**
Max. Marks: 60

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 two graphs G and G1 given below. Can you generate G1 from G using a sequence of valid graph rewriting rules as specified in the Take Grant Protection model? Having extra nodes and extra edges in the final state other than those shown in G1 is acceptable. Show the intermediate graphs and clearly state the graph rewriting rule used at each step. If it is impossible to generate G1 from G, clearly describe the reason. **[15]**



2. (a)
Consider a system implementing the HRU model has the generic rights: R = {read, write, own}. It has only the following two commands: COMMAND_A (x, y, z) and COMMAND_B (t). Both the commands have no condition/constraint. Interpretations of the two commands are given below:

```
COMMAND_A (x, y, z) :                COMMAND_B (t):
        Enter read into (x, x)               Create object t
        Destroy subject x
        Enter write into (y, z)
```

Consider the initial configuration of the system as follows: Explain clearly if this initial configuration is safe with respect to the generic right "write".

	P1
P1	

(b) Explain briefly which of the general requirements for commercial policies are handled in Clark Wilson integrity model and how.

(c) Given the security clearances/classifications Top Secret (TS), Secret (S), Confidential (C) and Unclassified (U) (ordered from highest to lowest) and categories X, Y and Z, specify which types of access (read, write) 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
Amit (TS, {X, Z})	file1 (S, {X, Y, Z})
Anita (S, {X, Y)	file2 (C, {X, Z})
Nikhil (S, {Y, Z})	file3 (TS, {X, Z})
Rita (TS, {Z})	file4 (C, {X})

[10+5+5=20]

3. (a) A password based authentication system enforces the password to be of length 4 to 6 characters chosen from the alphanumeric characters: [a-z, A-Z, 0-9]. In order to prevent dictionary attack type 2, it uses a backoff strategy with backoff delay in geometric progression having initial term of 1 and common ratio of 2. That is, for the first failed attempt, the login screen comes back after 1 second. Subsequently it comes back after 2, 4, 8, .. seconds, etc. The actual time to try a password is negligible compared to the backoff delay. A Dictionary Attack of Type 1 can be launched on the authentication system in which the rate of checking of passwords is 100 per second. Consider all passwords to be equally likely.

How many passwords can be tried using Type 2 attack during the same time in which the probability of finding a password using Type 1 attack is 0.1? **[10]**

(b) For the following questions, zero or more options may be correct. Each correct answer carries 2 marks. 1 mark will be deducted for every wrong answer. An answer will be considered correct if all the correct and only the correct choices have been selected. If you are not attempting a question, write “Not answered”. If you feel none of the options is correct, write “None”. **[2×5=10]**

(i) In Kerberos (Ver. 4), a client has to contact the Ticket Granting Server (Assuming none of the tickets acquired during a session expire during the lifetime of the session)

a. Once for each session
b. To get a ticket for accessing the authentication server
c. Once for each application server
d. Once for each application service request

(ii) In Kerberos (Ver. 4) with two realms A and B, a secret key is shared between

a. The authentication server of A and the authentication server of B
b. The authentication server of A and the ticket granting server of B
c. The ticket granting server of A and each application server of B
d. The authentication server of A and each application server of A

(iii) In Kerberos (Ver. 4), a session key is shared between

a. A client and the authentication server
b. The authentication server and the ticket granting server
c. A client and the ticket granting server
d. A client and each application server that it accesses

(iv) In Kerberos (Ver. 4), authenticators help to

a. Prove the identity of the client to the ticket granting server
b. Prove the identity of the client to the authentication server
c. Prove the identity of the ticket granting server to the application server
d. Establish reverse authentication between application server and client

(v) If an information transfer path exists between object o_1 to object o_{n+1},

a. Biba’s Low Water Mark policy enforces that $i(o_1) <= i(o_{n+1})$
b. Biba’s Ring policy enforces that $i(o_1) = i(o_{n+1})$
c. Biba’s Strict Integrity policy (Biba’s Model) enforces that $i(o_1) < i(o_{n+1})$
d. Biba’s Ring policy enforces that $i(o_1) < i(o_{n+1})$

(c) In a simplified version of S/KEY one time password based authentication system, assume that the function used is $f(x) = (2x^2)$ and the initial seed value is 1. A total of 20 passwords are generated using this scheme. Determine what should be the response by the user when the server asks for password number 16 as challenge. **[5]**