School of Information Technology
IIT Kharagpur

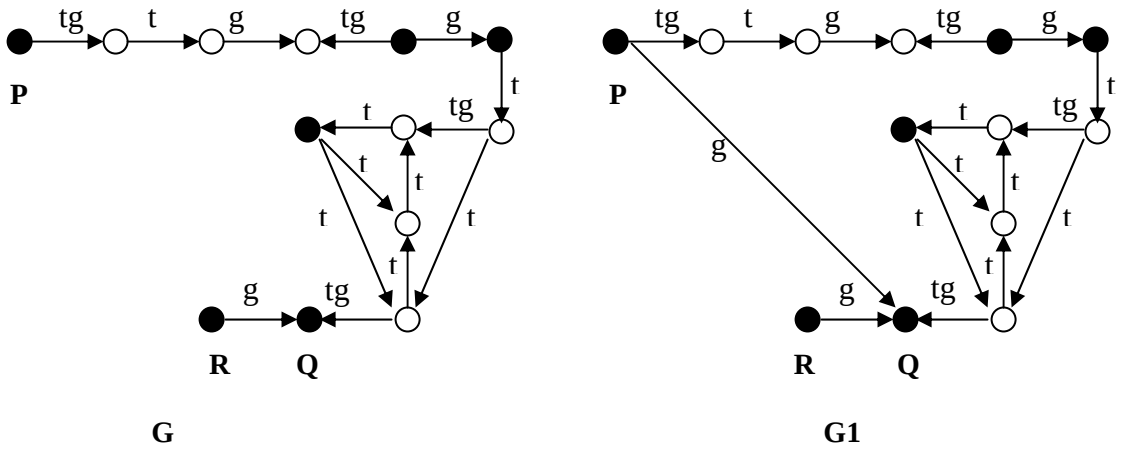
Course Id: IT60112 Information and System Security (Mid Semester Examination)

Date: February 25, 2011 **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 Take Grant Protection model? If your answer is YES, show the intermediate graphs and clearly state the graph rewriting rule used at each step. If your answer is NO, state and explain in detail the reason why it would not be possible.

You may name the intermediate nodes other than P, Q and R in any way you wish. **[15]**



2. Consider a password-based authentication system in which all passwords are of length 5 chosen from an alphabet of size 10. To prevent Dictionary Attack of Type 2, it employs a combination of backoff strategy and disconnection strategy such that the backoff periods form an Arithmetic Progression series with initial term of 1 second and common difference of *d* seconds. After every 100 failed attempts, it immediately disconnects and reconnects after a delay. The durations of disconnections form a geometric progression series of initial term 1 second and common ratio of 0.5 second. The backoff arithmetic progression series is not reset after disconnection. That is, if the attacker reconnects, tries and fails again, the backoff time will continue the original series. The actual time to try a password is negligible compared to the backoff and disconnection delays.

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. What should be the value of the common difference *d* of backoff period such that approximately the same number of passwords that can be tried without success using Type 2 attack during the time in which the probability of finding a password using Type 1 attack is 0.1? Consider all passwords to be equally likely. You may make approximations while computing your result but they should be reasonable. **[15]**

3.

(a) In a simplified version of S/KEY one time password based authentication system, assume that the function used is $f(x) = (2^x \bmod 13)$ and the initial seed value is 1. A total of 7 passwords are generated using this scheme. Determine what should be the response by the user when the server asks for password number 5 as challenge.
(b) How are the passwords actually entered by a user against a challenge in usual S/Key One-time password system?
(c) If a user is on a trip where he might be using unsecure client machines like those provided at airports, how can he use the S/KEY scheme?
(d) Which secure system design principles are followed in S/KEY and how?

[8+2+2+3=15]

4.

(a) How is Separation Duty handled in Clark Wilson security policy?
(b) A consultancy firm deals in the Oil sector with three companies and also in the Banking sector with five companies. What is the minimum number of consultants they need for handling datasets of all the eight companies if they implement (a) Chinese Wall Simple Security Condition only (b) Chinese Wall Simple Security Condition as well as Chinese Wall *-property?
(c) Describe the components of the HRU model with the help of an example. **[5+5+5=15]**