1. Consider the following pair of initial and final graphs representing protection states of a system where each node represents a subject. 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.

2. Consider a database system in which access control is enforced through evaluation of Boolean expressions. The various users, their groups and roles are as follows:

<table>
<thead>
<tr>
<th>user</th>
<th>group</th>
<th>role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amit</td>
<td>Programmer</td>
<td>Team Member</td>
</tr>
<tr>
<td>Kaushik</td>
<td>Analyst, Designer</td>
<td>Team Leader, Manager</td>
</tr>
<tr>
<td>Nitin</td>
<td>Programmer, Analyst, Designer</td>
<td>Team Member</td>
</tr>
</tbody>
</table>

The database tables have the following default access rules

<table>
<thead>
<tr>
<th>Mode of Access</th>
<th>Default Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select</td>
<td>1</td>
</tr>
<tr>
<td>Insert</td>
<td>0</td>
</tr>
<tr>
<td>Delete</td>
<td>0</td>
</tr>
<tr>
<td>Update</td>
<td>1</td>
</tr>
</tbody>
</table>

Specific rules for access to the tables Employee, Accounts, Project and Design are given below.
(a) Draw the access control matrix for the above protection system at 11:00 AM.
(b) If the default access rules table is changed so that default rule for all the four modes of access
(i.e., Select, Insert, Update and Delete) is 0, draw the new access control matrix of the
protection system at 7:00 PM. \[5+5=10\]

3. Consider the set of generic rights \( G = \{\text{read}, \text{write}, \text{own}\} \) and a Command \( \text{ADD_RW_RIGHTS} \)
\((a, b, c)\) in the HRU model. This command causes subject \( a \) to give \text{write} and \text{read} rights to \( b \) on
\( c \) only if \( a \) owns \( c \).

(a) Write the interpretation of this command in terms of the primitive operations as
defined in the HRU model.
(b) Starting with an arbitrary protection state before the execution of the command,
show the final protection state at the end of execution of the command. You must
also show the intermediate states at the end of each primitive operation.
(c) Let us state the Principle of Attenuation of Privileges (POAP) as follows: “A subject
can only give a right it possesses while executing any primitive operation.” Consider
that \( \text{ADD_RW_RIGHTS} \) (a, b, c) you have defined above must also satisfy the
POAP. In that case, is the following protection state transition valid? If yes, write
the new interpretation of \( \text{ADD_RW_RIGHTS} \) (a, b, c) augmented with POAP. If no,
clearly and precisely state why no. \[5+5+5=15\]

4. (a) Why is Bell LaPadula model called a Lattice model of security?
(b) What is the difference between certifications and enforcements in the Clark-Wilson’s
Integrity policy?
(c) State the requirements of a commercial system as suggested by Lipner.
(d) Explain how Clark Wilson’s Integrity policy handles the Principle of Separation of Duty and
Auditing requirements. \[5+3+4+3=15\]

5. Consider a password-based authentication system in which all passwords are of length between
8 to 10 characters chosen from an alphabet of size 20. To prevent Dictionary Attack of Type 2,
it employs a backoff strategy such that it takes 1 sec. to try the first password and subsequent
backoff periods form an Arithmetic Progression series of common diff. 2 sec. After 5 failed
attempts, it disconnects. The periods of disconnections form a series of duration 1 second, 2
seconds, 4 seconds, 8 seconds, etc. The backoff series is not reset after disconnection. That is, if
the attacker reconnects and tries, the backoff time will continue the original series.
A Dictionary Attack of Type 1 can be launched on the authentication system in which the
rate of checking of passwords is 50 per second. 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 0.8? Consider all passwords to be equally likely. \[10\]