1. Consider the following key agreement protocols I and II. The protocols are the modifications of the basic Diffie-Hellman key exchange. The group $\mathbb{Z}_q^*$ and its generator $g$ are public knowledge. The participants A and B have long term private keys $x_A$ and $x_B$, respectively. They also have public keys $y_A = g^{x_A}$ and $y_B = g^{x_B}$, respectively. A chooses a secret integer $r_A$, and B $r_B$. The protocol I is as follows:

i) $A \rightarrow B$: $g^{r_A}$

ii) $B \rightarrow A$: $g^{r_B}$

After the second step, the participants can calculate the common secret

$$K_{AB} = t^x_A y^r_B = t^x_B y^r_A.$$

The second protocol II is as follows:

i) $A \rightarrow B$: $y^{r_A}_B$

ii) $B \rightarrow A$: $y^{r_B}_A$

The common key is

$$K_{AB} = g^{r_A r_B} = (y^{r_B}_A)^{x_A} r_A = (y^{r_A}_B)^{x_B} r_B.$$

Do the protocols satisfy the forward or partial forward security property? Remember that a protocol is forward secure, if the compromise of long term keys does not reveal the short term keys (i.e. keys $K_{AB}$). A protocol is partially forward secure, if the compromise of one long term key does not reveal the short term keys.

2. Consider the GDH.3 protocol. Design the algorithms for the addition and deletion of a member into the group.

3. Consider the following key tree:

- $M_1: (1, 0)$
- $M_2: (2, 0)$
- $M_3: (2, 1)$

Show how $M_1$, $M_2$ and $M_3$ calculate the shared secret $K_{0,0}$ (expressed as a formula with the primitive root $\alpha$ and members’ secrets $r_i$).
4. Consider the following key tree:

```
   (0,0)
  /   \
(1,0)  (1,1)
 \
(2,0)  (2,1)  (2,2)  (2,3)
```

Show all the new calculations (expressed with \( \alpha \) and \( r_i \)) performed by all the remaining members, when \( M_2 \) (2, 1) is deleted. Analyse why \( M_2 \) does not know the new group key.

5. Simulate the Burmestel-Desmedt protocol with four members and show how everybody calculates the group secret (using again \( \alpha \) and \( r_i \) in the formulas).