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

2. Consider the Burmester-Desmedt protocol without broadcasts. Prove that everybody calculates the same key.

3. Consider the following key tree:

```
(0, 0)  ↙  ↙  ↙  ↙  ↙  ↙
  (1, 0)  ↙  ↙  ↙  ↙  ↙  ↙
    (2, 0)  (2, 1)  (2, 2)  (2, 3)
  (1, 1)  ↙  ↙  ↙  ↙  ↙  ↙
```

Show how $M_1 ((2, 0)), M_2 ((2, 1))$ and $M_3 ((2, 2))$ 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)  ↙  ↙  ↙  ↙  ↙  ↙
    (2, 0)  (2, 1)  (2, 2)  (2, 3)
  (1, 1)  ↙  ↙  ↙  ↙  ↙  ↙
```

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. We have had many conference protocols: GDH.1-3, Burmester-Desmedt and TGDH. Make an array which shows the efficiency of the protocols. You should have at least four columns in your array: the number of exponentiations, messages, broadcasts and rounds. It is possible to decide which is the most efficient protocol? Give typical situations and applications where each protocol shows its best and worst sides.