Assignment 2

- Task 1: zero knowledge proof for that
  - $(c_1, c_2) = (g^\beta, u^\beta \cdot g^1)$ and $(d_1, d_2) = (g^\gamma, u^\gamma \cdot g^0)$ are the encryption of 1 and 0 respectively
  - Hint: use the proof for DDH tuple

- Task 2: Implement the proof

- Write a report about this

- submit via Blackboard, Deadline: 10 Apr. 11:00 pm