# Test Questions Security and Cryptography II

**Task 1 :**
Name five methods / techniques for achieving anonymity.

**Task 2 :**
Name and describe anonymity / privacy related protection goals.

**Task 3 :**
Which protection goal can be achieved with which anonymity technique?

**Task 4 :**
How secure is the achieved anonymity in the case of broadcast with respect to observing / modifying attackers?

**Task 5 :**
Will end-to-end encryption solve the problem of modifying attacks on broadcast?

**Task 6 :**
Describe the attacker model of the ring net.

**Task 7 :**
Why do we need "digital signal regeneration"

**Task 8 :**
Describe how PIR / query and superpose work.

**Task 9 :**
Describe the attacker model.

**Task 10 :**
Which "security level" could be achieved?

**Task 11 :**
Do you need to consider something while sending query vectors / receive the results form the database servers?

**Task 12 :**
Describe how one can save bandwidth from user to database(s)

**Task 13 :**

How can we decrease the bandwidth from the databases to the user?

**Task 14 :**
What is the drawback of the two optimisations mentioned above?

**Task 15 :**
Regarding the optimisation user to database: Do we still need to encrypt the one remaining query vector?

**Task 16 :**
Describe how the DC net works.

**Task 17 :**
Describe the DC net attacker model.

**Task 18 :**
Which “level of security” can be achieved with the DC net?

**Task 19 :**
What is the global sum?

**Task 20 :**
How to deal with collisions (sending of multiple messages at the same time)?

**Task 21 :**
Describe how the reservation scheme works.

**Task 22 :**
Describe how the collision resolution scheme based on mean calculation works.

**Task 23 :**
How can/will recipient anonymity be achieved within the DC net?

**Task 24 :**
Are there attacks on the recipient anonymity possible?

**Task 25 :**
How can we prevent a successful attack on the recipient anonymity?

**Task 26 :**
How does a Mix network work? What are the basic functions of a Mix?

**Task 27 :**
Why “discard repeats”?

**Task 28 :**
Why indeterministic asymmetric cryptography?

**Task 29 :**
How to achieve recipient anonymity?

**Task 30 :**
Why asymmetric crypto in Mixes?