CRYPTOGRAPHY and SECURITY, exam Feb 2022, preparation tasks

Problem 1 Modify Smart-ID construction so that there are two independent authorities on the side of the server involved instead of just one. It should provide resilience even if the chip provider colludes with one of the authorities.

Please have a specification of Smart-ID at hand during the exam (Estonian webpage whitepaper is hard to read, take the lecture note – they will suffice)

Problem 2 Recall the concept of differential privacy and consider a database with salaries of employees. The algorithm A simply returns a median salary (with no name of the employee).

Does it satisfy the condition of differential privacy? For which ϵ?

Problem 3 We have not discussed the details of symmetric encryption used by TOR anonymous communication system. In order to implement a "lightTOR" it has been decided to use the ECB mode of block encryption for the phase of establishing a connection. (We also assume that later the payload communication is encrypted symmetrically using a different, more secure mode.)

Please evaluate security consequences of the decision to use ECB. While ECB in general is not recommended, evaluate the consequences in this concrete case.

Problem 4 Read the KRACK description from the notes for the lecture and understand its mechanism for the further examples given.

`https://kutylowski.im.pwr.wroc.pl/lehre/cs21/internal/CS21-WIFI-sh.pdf`