EMBEDDED SECURITY SYSTEMS,
preparatory problems for 15.06.2016

Name: .....
index number: .....

Problem 1 Recall the authentication mechanism used by SIM cards. Is the mechanism used by UMTS immune against cloned SIM cards? Prove that it is immune or present a scenario showing that this is not the case.

Problem 2 Consider RFIDs that keep counter and a two current passwords: A and B. When receiving the password, the RFID increments the value of the counter if the password received equals the password stored in A. Then it sends the password stored in B and a random byte b. Then new passwords are derived as leading bits from PRNG(K, i, b), where K is a secret shared by RFID and the system, i is the current value of the counter.

Check whether the system may desynchronize so that the system cannot derive the same passwords as the RFID.

Problem 3 TESLA has to authenticate the messages of a stream sent from A to B so that the messages authenticate each other. If all messages are delivered, then integrity can be easily checked. A simplified version of this protocol is as follows:

- a chain of values is created: $K_i := Hash(K_{i+1})$ (we start with K_N chosen at random and then compute $K_{N-1}, ..., K_1$
- at time t the device A sends the tth message M_t with a MAC created with the key $K'_i = Hash'(K_i)$ and K_{t-d}

Questions:

- how the recipients checks integrity of messages?
- why it is impossible to hijack the connection?
- why we send K_{t-d} and not just K_{t-1}?

Problem 4 Recall the method presented during the last lecture aiming to prevent unfair key generation by subverted software. As mentioned, it does not protect itself against an attack where the randomness chosen by a devices comes from a very small pool of values known to the adversary. How to improve this method in order to make the system immune against a malicious manufacturer?