EMBEDDED SECURITY SYSTEMS,
preparatory problems for 19.06.2013

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

Problem 1 Consider an electronic purse according to specification

`read.pudn.com/downloads41/ebook/142386/E5212851.pdf`

Try to design an access system with these cards (access to rooms, to servers, ...). What are the problems? What can be achieved?

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. Propose how to improve the scheme.

Problem 3 μTESLA 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.

What happens if errors occur in a transmission? Consider the case of burst errors (a group of subsequent messages is effected) as well as the case when the errors occur independently at random with some relatively small probability for each message.

Problem 4 Consider multiplication of numbers of length m on a grid of size $2m \times 4$, where the input is given to the bottom $2m$ nodes of the grid, and according to the natural ordering: to compute $x \cdot y$ the nodes get the following bits from left to the right: $x_{m-1}, x_{m-2}, \ldots, x_0, y_{m-1}, y_{m-2}, \ldots, y_0$.

Estimate the time needed to deliver the result. Matching lower and upper bounds are to be presented.