Homework 1

1. **(Optional)** If you want to have a look at the code presented in the lectures, install `Node.js` available (for free) from

   http://nodejs.org

   It needs aslo the Node-packages Express, Cookie-Parser, Body-Parser and Crypto. They can be easily installed using the Node package manager `npm`.

2. Practice thinking like an attacker. Assume the following situation:

   > *Prof. V. Nasty gives the following final exam question (closed books, closed notes):*
   >
   > *Write the first 100 digits of pi:*
   > *3.*_____

   Think of ways how you can cheat in this exam? How would you defend against such cheats.

3. Here is another puzzle where you can practice thinking like an attacker: Consider modern car keys. They wirelessly open and close the central locking system of the car. Whenever you lock the car, the car "responds" by flashing the indicator lights. Can you think of a security relevant purpose for that? (Hint: Imagine you are in the business of stealing cars. What attack would be easier to perform if the lights do not flash?)

4. Imagine you are at your home a broadband contract with TalkTalk. You do not like their service and want to switch, say, to ???. The procedure between the Internet providers is that you contact ??? and set up a new contract and they will automatically inform TalkTalk to terminate the old contract. TalkTalk will then send you a letter to confirm that you want to terminate. If they do not hear from you otherwise, they will terminate the contract and will request any outstanding cancellation fees. Can you imagine in which situations this way of doing things can cause you a lot of headaches? For this consider that TalkTalk needs approximately 14 days to reconnect you.

5. A water company has a device that transmits the meter reading when their company car drives by. How can this transmitted data be abused, if not properly encrypted? If you identified an abuse, then how would you encrypt the data so that such an abuse is prevented.

6. Explain what hashes and salts are. Describe how they can be used for ensuring data integrity and storing password information.

7. What is the difference between a brute force attack and a dictionary attack on passwords?

8. What are good uses of cookies (that is browser cookies)?

9. Why is making bank customers liable for financial fraud a bad design choice for credit card payments?