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

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

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

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