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 also 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?) Should the car also make a "beep noise" when it unlocks the doors? Which threat could be thwarted by that?

4. And another one: Imagine you have at home a broadband contract with TalkTalk. You do not like their service and want to switch, say, to Virgin. The procedure between the Internet providers is that you contact Virgine 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 proceed with terminating the contract and will request any outstanding cancellation fees. Virgin on the other hand sends you a new router and paperwork about the new contract. Obviously this way of doing things is meant to make switching for you as convenient as possible. Still can you imagine in which situations this way of switching providers can cause you a lot of headaches to you? For this consider that TalkTalk needs approximately 14 days to reconnect you and might ask for reconnection fees.

5. And another one: A water company installed devices that transmit meter readings 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. Hint: Consider the fact that every person uses approximately 120l of water every day.

6. And another one: Nowadays everybody is scared at a bomb going off at a big event, say a football game. To mitigate such a threat, you order expensive metal detectors and hire a security team that will staff these detectors at each game. Think whether people are really safer at a football game with metal detectors or not. Hint: People certainly might **feel** safer by going through metal detectors, but the question is whether they **are** safer. Hint: Consider how people arrive at such an event: within a relative short amount of time, thousands, if not more, spectators will arrive at your football game.

7. And another one: Imagine you are researching security products (e.g. CCTV, alarms etc) on a helpful website. They ask you for you address details? Think about whether this can be bad for you.

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

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

10. Even good passwords consisting of 8 characters, can be broken in around 50 days (obviously this time varies a lot and also gets shorterand shorter). Do you think it is good policy to require users to change their password every 3 months (as King's did until recently)? Under which circumstance should users be required to change their password?

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

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