Homework 1

Please submit your solutions to the email address 7ccsmsen at gmail dot com. Please submit only one homework per email. Please also submit only ASCII text or PDFs. Every solution should be preceded by the corresponding question, like:

Qn**:**	**...a difficult question from me...**
A:	**...an answer from you ...**
Q$n+1$	**...another difficult question...**
A:	**...another brilliant answer from you...**

Solutions will only be accepted until 30th December!

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: 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.

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

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

7. Even good passwords consisting of 8 characters, can be broken in around 50 days (obviously this time varies a lot and also gets shorter and shorter over time). 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?

8. The biggest dictionary for dictionary attacks I know contains 15 Billion entries. If you try out all of these 15 Billion entries in order to hack one password how much percent of the full brute-force space did you cover. For this assume passwords use 62 charcaters and are typically 8 characters long.

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

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

11. **(Optional)** This question is for you to provide regular feedback to me. No need to address every aspect of the suggested question: What were the most interesting, least interesting, or confusing parts in this lecture? Please feel free to share any other questions or concerns.