

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. Explain what hashes and salts are. Describe how they can be used for ensuring data integrity and storing password information.
4. What is the difference between a brute force attack and a dictionary attack on passwords?
5. What are good uses of cookies (that is browser cookies)?
6. Why is making bank customers liable for financial fraud a bad design choice for credit card payments?