Cheat-sheet specifications

November 24, 2019

- Submit a PDF file generated with LaTeX. Deadline is Friday 20.12.19
- If you want to write in HTML/CSS/Javascript, make sure you add some interactive functionality.
- You have to formulate everything in your own words.
- Quote your sources. LaTeX uses a special mechanism called `BibTex` to accomplish this.
- Defenses of your cheat sheet start immediatley after holidays. You can determine the order of groups.
- Grading of your cheat sheets depends on
  - completeness
  - precision of your statments
  - layout

  If I have the impression that work on the cheat sheet was not equally distributed I will assign individual grades.
- During the defense I will ask you questions to test your understanding of what you wrote in the cheat sheet. The final grade is the mean of the individual grade and the grade for the cheat-sheet.

Topics

One Time Pads

- What are *One Time Pads*?
- Under what conditions are they perfectly safe and why are the perfectly safe under the these conditions?
- Give examples or code fragments to show that using the same key twice is not safe
- Implement *One Time Pads* in Python

Public Key Crypography

- How can you hand over a bike to someone you don't want to meet, without trusting anybody and without leaving the bike unlocked at any moment?
- Which properties of this example do you need for *public key cryptography*. Does this work with *One Time Pads*?
- How does modular arithmetic work?
- Why are powers modulo prime numbers so interesting for encryption and what is a generator?
- Use python code fragments to give examples.
- How does the Diffie-Hellman key exchange work schematically?
- Why is computing powers so much easier than taking logarithms in modular arithmetic?
- How does El Gamal encryption work?
- In what respect is RSA simpler and why can it be used as a digital signature?

Bitcoin

- Which problem does the *blockchain* solve?
- What is a *hash function*?
- Describe how the *blockchain* works
- What are *smart contracts*?