Cryptography

Priv.-Doz. Dr. Adrian Spalka, Konstantin Ziegler

1 Assignment

(Due: Thursday, 4 November 2010, 12^{00})

Exercise 1.1 (security policies)**.** (6 points) Determine the values and how they have to be protected for two information systems in the following environments:

(i) a social network,

(ii) a university administration,

(iii) a hospital.

Which of the aspects of a derived security policy would be mandatory (where specified?) and which would be at digression (whose?)?

Exercise 1.2 (trusted third parties)**.** (8 points)

(i) Find examples for an IS-architecture and a communication structure, whose security depends on the cooperation of a trusted third party.

(ii) Analyze the role of these parties with respect to outsourcing and cloud computing.

(iii) Write down in detail your fundamental thoughts on the claim "Trusted third parties considered harmful."[1]

Exercise 1.3 (secret sharing)**.** (8 points) There are n people and everyone carries a part of a secret. Every k people – in arbitrary combination – can compute/reconstruct the secret, but not $k-1$ or less. Think of it as an electronic safe with n locks, which opens only, when at least k keys are inserted.

[1] "XY considered harmful" used to be a popular title, whenever the invention XY was not considered an improvement anymore.

(i) Formulate a secret-sharing system formally as a function.

(ii) Give at least one example for a concrete secret-sharing system and show its mode of operation with an example.

Exercise 1.4 (mathematical bonus)**.** (+2 points) Let n be an integer and q its checksum. Show, that n and q leave the same remainder after division by 9.