5. Exercise sheet
Hand in solutions until Monday, 11 May 2015, 11:59

Exercise 5.1 (X.509). (8 points)
Read RFC 5280 and answer the following questions:

(i) What classes of certificates are there? 2

(ii) What is the basic syntax of X.509 v3 certificates? Describe the Certificate Fields in detail. Which signature algorithms are supported? 2

(iii) What is a trust anchor? Can one use different trust anchors? 2

(iv) What conditions are satisfied by a prospective certification path in the path validation process? 2

Exercise 5.2 (Zero-Knowledge). (10 points)
Read Quisquater, Quisquater, Quisquater, Quisquater, Guillou, Guillou, Guillou, Guillou, Guillou, Guillou, Guillou, Guillou & Berson (1989) to one of your children. Alternatively take one of your fellow students.

(i) Write down the protocol in a form appropriate for computer science students rather than for children. 4

(ii) Prove for this protocol the following three properties:

○ If the prover’s claim is true, the verification returns true — always.

○ If the prover’s claim is false, the verification fails — with high probability.

○ The verifier does not learn anything about the private information. 6
References