Esecurity: secure internet & e-cash, summer 2012

MICHAEL NÜSKEN, RAOUL BLANKERTZ

3. Exercise sheet
Hand in solutions until Sunday, 22 April 2012, 23:59

Exercise 3.1 (GnuPG cont.). (4 points)

Consider the model of trust in GnuPG. Describe how trust is transfered (ie. which keys are trusted?). Which parameters can be adjusted? [4]

Exercise 3.2 (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 3.3 (Security reduction). (4 points)

For a signature scheme, a message is first hashed and then the hash value is signed. Assume that the signature scheme is secure in the EUF-CMA model. Does that imply that the hash function is collision resistant? Prove your answer. [4]

Exercise 3.4 (Random exit). (8 points)

You are trapped in a locked room. Once every hour you have the chance to open the door. This succeeds with a certain probability p.

(i) What is the chance that you can leave the room after

[0] (a) exactly one hour?

[1] (b) exactly two hours?

[1] (c) exactly three hours?

[1] (d) exactly four hours?

(ii) What is the expected number of hours that you have to stay

[2] (a) ...by definition? [Give a formula.]

[3] (b) ...by value? [Prove that it equals $1/p$.]