Esecurity: secure internet & e-passports, summer 2011

MICHAEL NÜSKEN, RAOUL BLANKERTZ

11. Exercise sheet
Hand in solutions until Sunday, 26 June 2011, 23:59

Exercise 11.1 (Doc 9303). (14+4 points)

To answer the following questions read Doc 9303 and further reading, where required.

(i) What bit rates are possible for the communication between a MRTD and a reader? [4]

(ii) What is published in the ICAO PKD? Find the up to date CSCA certificate of Germany. For which time period is it valid and for which period is it used to sign? [4]

(iii) Imagine you work for a government, which wants to introduce the eMRTD. You are ask to decide which cryptographic scheme should be used in their Country Signing CA.

List all possible schemes. Which of them is the best? Why? Compare the runtime, the key size and the security of these schemes. [6] [+3]

(iv) In the lecure we saw "M / M" in the sex field of an Utopia visa. Find out what "M / M" stands for. What format does the sex field have? [+1]

Exercise 11.2 (Entropy of the MRZ). (4 points)

Give a first rough upper bound on entropy of the MRZ by simply considering the types of entries for all involved places. Next reduce this bound using reasonable assumptions on the information. What else can you do using publicly available information of a given person? [4]

Exercise 11.3 (Computing power of RFID). (2 points)

In Lee et al. (2008) we find the following computing times for a RFID with an elliptic curve processor: Performing Schnorr's signing scheme for an elliptic curve over $GF(2^{163})$ takes 244.43 msec with a clock rate of $1\,130$ kHz.

Due to high power consumption, that is ca. 36 μW in the above example, one has to reduce the clock rate. By scaling the result from above,

[1] (i) how fast can Schnorr's signing scheme be performed with a clock rate of 423 kHz?

[1] (ii) how low can you choose the clock rate with just being faster than a second?