The electronic health card, summer 2008

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

8. Exercise sheet
Hand in solutions until Monday, 16 June 2008.

Exercise 8.1 (Combining Encryptions). (4 points)

In this exercise we will explore some combined cryptosystem. For example take AES and encrypt a message x with AES twice using keys k_1 and k_2. Thus the encryption of x would be given by AES(AES$(x, k_1).k_2$). Explain why this constrution is roughly as secure as onle single application of AES. 4

Exercise 8.2 (Diffie Hellman key exchange). (9 points)

For a Diffie-Hellman key exchange Alice first fixes a group G with an element g of order q such that the discrete logarithm problem with base g seems difficult. After sending her group offer to Bob, Alice chooses a random(!) temporary secret $\alpha \longleftarrow \mathbb{Z}_q$, computes $a \leftarrow g^\alpha$ in G and sends it to Bob. Bob decides whether he accepts the group offer and in that case proceeds analogously. Second, Alice takes Bob's b and computes $s \leftarrow b^\alpha$. Bob proceeds analogously.

(i) Prove that Alice and Bob obtain the same s. 1

All following conversation can be encrypted and authenticated on the basis of the shared secret s.

(ii) Assume Mallory sits between Alice and Bob. Show how he can hoodwink both and intercept all traffic in the plain so that neither Alice nor Bob can notice anything but possibly a slightly slower connection. 2

(iii) Eve comes late and only registers the communication between Alice and Bob. 2

- Formulate the problem that she has to solve to obtain the common secret.
- Relate it to the discrete logarithm problem (ie. computing $(g, g^\alpha) \mapsto \alpha$) to base g.

Perform a toy example of a Diffie Hellman key exchange: Fix $p = 389$ and $g = 5 \in \mathbb{Z}_p^\times$.

(iv) Show that the order of g is 97. 1

(v) Choose $\alpha \in \mathbb{Z}_p$ (take $\alpha \notin \{0, 1\}$ to get something interesting) and calculate $a := g^\alpha$. 1

1 (vi) Choose $\beta \in \mathbb{Z}_p$ (take $\beta \notin \{0, 1, \alpha\}$ to get something interesting) and calculate $b := g^\beta$.

1 (vii) Now compute b^α and a^β and compare.

Exercise 8.3 (Signed key exchange). (3+1 points)

Alice and Bob want to exchange messages using a symmetric cryptosystem. To do this they need to agree on a common session key K. They have chosen the key exchange protocol by Diffie-Hellman. In addition they want to safeguard the exchange using ElGamal signatures. The basis of all computations is the group G with generator g. Alice has used her private key π_A to get her public key $p_A = g^{\pi_A} \in G$ certified. Bob did the same thing with π_B and $p_B = g^{\pi_B} \in G$. To compute the common session key Alice chooses α and Bob chooses β.

1 (i) Describe the individual steps of the protocol that allows Alice and Bob to agree on their common session key $g^{\alpha\beta}$. *Note:* Their protocol consists of key exchange and authentification.

1 (ii) Execute the computations needed for the individual steps using the group $G = \mathbb{Z}_{123973}^\times$, $g = 9$, $q = 10331$, $\pi_A = 8274$ and $\pi_B = 8012$. Choose $\alpha_A = 4321$ and $\alpha_B = 1234$.

1 (iii) Explain why the protocol (from part (i)) is secure with respect to a "man in the middle" (Mallory!) type attack.

+1 (iv) Would this still be correct if Alice and Bob hat not certified their public keys and instead exchanged them at the beginning of the protocol?

Note: Those parts of the protocol that are not specified by the instructions of this exercise should be (with ample comments) chosen by you.

Exercise 8.4 (Qualified Electronic Signatures). (6 points)

6 Standard electronic signatures have in general no validity at court. Sometimes, however, we want (for example when signing a contract electronically) that the resulting signature is judicially binding. For that reason so called *qualified signatures* have been introduced. Find information on qualified electronic signatures, say in Germany, the European Union, or your home country, and describe the major conditions that are imposed on them.