Cryptographic passports & biometrics, summer 2009

MICHAEL NÜSKEN, KONSTANTIN ZIEGLER

7. Exercise sheet
Hand in solutions until Monday, 15 June 2009.

Any claim needs a proof or argument.

Exercise 7.1 (Basic Access Control). (5 points)

(i) On the usage of the chip's first random number `RND.ICC`: What happens if you try to communicate with the chip and playback a communication with the chip? (Note that an attacker might first record a communication and then steal the passport chip and then try to get more information by inducing errors in the chip using strong magnetic or electric fields for example while repeating the recorded communication.) $\boxed{1}$

(ii) Reanalyze: which information do we need to get the information in the chip? In particular, is it enough to steal the passport (and place it back later)? $\boxed{1}$

(iii) Does a read operation leave any trace on the passport? Should it? $\boxed{1}$

(iv) Are hash collisions a danger? Describe an "attack" that uses a hash collision to forge a passport (or two) with a wrong picture. And explain how to prevent it. $\boxed{1}$

(v) If someone gets hold of the document signer's private key she can forge a passport. Of course, as soon as this gets noticed the key will be revoked. How could an attacker still successfully cross the border with the forged passport? $\boxed{1}$

Exercise 7.2 (2DES). (6 points)

Consider the product cipher 2DES $=$ DES $\circ$ DES. This cipher uses two 56 bit keys. Assume we have several plaintext-ciphertext pairs $(x_1, y_1), \ldots, (x_\ell, y_\ell)$, $\ell \in \mathbb{N}$, which were obtained using the same unknown key (K_1, K_2). This exercise describes a *meet in the middle attack* on 2DES.

(i) Prove that $e_{K_1}(x_i) = d_{K_2}(y_i)$ for all $1 \leq i \leq \ell$. Give an heuristic argument that the expected number of keys (K_1, K_2) such that $e_{K_1}(x_i) = d_{K_2}(y_i)$ for all $1 \leq i \leq \ell$, is roughly $2^{2 \cdot 56 - 64\ell}$. $\boxed{2}$

(ii) Assume that $\ell \in \{1, 2\}$. A tradeoff of time and memory can be used to compute the unknown key (K_1, K_2). We compute one list, containig 2^{56} items where each item contains an ℓ-tuple of elements of plaintext blocks as well as an element of the keyspace (i.e. one possible K_1). If one sorts the list and computes the same for K_2, then a common ℓ-tuple can be identified by means of a search through the list. Discuss the security of 2DES under consideration of this attack. $\boxed{2}$

$\boxed{2}$ (iii) Show that the memory required for the attack can be reduced by a factor of 2^t if the total number of encryptions is increased by a factor of 2^t.
Hint: Break the problem into 2^t subcases, each of which is specified by simultaneously fixing t bits of K_1 and K_2.