Cryptography, winter 2006

Prof. Dr. Werner Schindler, Dipl.-Inf. Daniel Loebenberger

5. Exercise sheet (13.12.2006)
Hand in solutions to the homework exercises on Wednesday, January 10th, in the tutorial/the lecture.

Exercise 5.1 (Repetition: Feistel Cipher).

Recall the structure of Feistel ciphers. Prove that the decryption in a Feistel cipher can be done by applying the encryption algorithm to the ciphertext, with the key schedule reversed.

Exercise 5.2 (2DES).

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).

(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 $2^{2 \cdot 56 - 64\ell}$.*

(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.*

(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.*

Exercise 5.3 (2-round DES).

We are considering an attack on 2-round DES. Describe how to perform a key splitting to break this cipher.

Exercise 5.4 (Homework: Payment records). (10 points)

$\boxed{10}$ Consider the electronic purse system described in Example B.58 in the lecture. Explain why this type of payment record meets the security requirements formulated on slide 60. You can find these slides online on the course homepage.

Exercise 5.5 (Homework: DES – Inversion Property). (10 points)

$\boxed{10}$ Let DES(x, K) represent the encryption of plaintext x with key K using the DES algorithm. Suppose $y =$ DES(x, K) and $y' =$ DES$(c(x), c(K))$, where $c(.)$ denotes the bitwise complement of its arguments. Prove $y' = c(y)$. Note that this can be only proved using only a "high-level" description of DES. The actual structure of the S-boxes is irrelevant for this.