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.

Solution. Straightforward from the structure of a Feistel cipher. ◯

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

Solution. $e_{K_1}(x_i) = d_{K_2}(y_i)$ can be seen from

$$\text{DES}(\text{DES}(x_i, K_1), K_2) = y_i \Leftrightarrow \text{DES}(x_i, K_1) = \text{DES}^{-1}(y_i, K_2)$$

For any fixed key pair $(k_1\prime, k_2\prime) \neq (k_1, k_2)$ (= correct key pair) we have $e_{k_1}(x_j) = d_{k_2}(y_j)$ for all $j \leq \ell$ with probability $2^{-64\ell}$ (heuristic argument). As there exist 2^{56+56} key pairs we may expect about $2^{112-64\ell}$ key pairs that meet this condition. Note that always at least one key pair (k_1, k_2) remains. ◯

(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.*

Solution. 2DES is broken under consideration of this attack, since the effort to break 2DES is approximately the same as the effort to break single DES. ◯

(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.*

Solution. Obvious. ○

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.

Solution. Clear from the stucture of 2-round DES. ○

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

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.

Solution. We are considering the electronic purse system from the lecture. A payment record looks like this:

`C_nr || T_nr || value || trans_nr || R || MAC(T,`$k_{C(MAC)}$`)`

We have the following security requirements: The payment record should...

- be linked to the purse: The value `C_nr` links the record to the purse.
- be linked to the terminal (making the theft of payment records useless): The value `T_nr` links the record to the terminal.
- contain the transferred value (price): The value `value` contains the price.
- prevent the merchant from multiple submission of one payment record: The value `trans_nr` prevents this.
- prevent replay attacks by dishonest customers: The random value `R` prevents this. Additionally a card individual key k_C is used.
- only authentic purses shall be able to generate valid payment records: The random value `R` as well as the use of a MAC with card-individual key ensures this.
- the background system shall be able to detect any manipulations of payment records: This is achieved by using a MAC in form of the value `MAC(T,`$k_{C(MAC)}$`)`, since we have a card individual key k_C for every purse.

○

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

Let DES(x, K) represent the encryption of plaintext x with key K using the DES algorithm. Suppose $y = \text{DES}(x, K)$ and $y' = \text{DES}(c(x), c(K))$, 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. 10

Solution. The Feistel-function of DES is stable under bitwise complement, i.e.: $f(c(x), c(k)) = f(x, k)$. This property is passed from round to round. QED. ○