

---

## Problem Set 2

**Due:** Wednesday January 21, 2009, in class.

See course information section (on course web page) for instructions and rules on working on problem sets and turning them in. The part of the course notes relevant to this problem set is Chapters 3 and 4.

---

**Problem 1. [30 points]** Let  $K$  be a 56-bit DES key and  $L$  a 64-bit auxiliary key. For any 64-bit plaintext  $M$  let

$$\text{DESY}(K \parallel L, M) = \text{DES}(K, L \oplus M) .$$

This defines a family of functions DESY:  $\{0, 1\}^{120} \times \{0, 1\}^{64} \rightarrow \{0, 1\}^{64}$ .

- (a) **[8 points]** Show that DESY is a block cipher.
- (b) **[22 points]** Let  $(M_1, C_1), (M_2, C_2)$  be input-output examples of DESY under a random 120-bit target key  $K \parallel L$ . Present an attack that given  $(M_1, C_1), (M_2, C_2)$  recovers the target key using at most  $2^{57}$  computations of DES or  $\text{DES}^{-1}$ . (As usual, the job is actually only to recover a key consistent with the input-output examples, but in practice this is typically the target key.)

---

**Problem 2. [50 points]** Let  $F: \{0, 1\}^k \times \{0, 1\}^l \rightarrow \{0, 1\}^l$  be a family of functions and let  $r \geq 1$  be an integer. The  $r$ -round Feistel cipher associated to  $F$  is the family of functions  $F^{(r)}: \{0, 1\}^k \times \{0, 1\}^{2l} \rightarrow \{0, 1\}^{2l}$ , defined as follows for any key  $K \in \{0, 1\}^k$  and input  $x \in \{0, 1\}^{2l}$ —

Function  $F^{(r)}(K, x)$

Parse  $x$  as  $L_0 R_0$  with  $|L_0| = |R_0| = l$

For  $i = 1, \dots, r$  do

$L_i \leftarrow R_{i-1}$ ;  $R_i \leftarrow F(K, R_{i-1}) \oplus L_{i-1}$

Return  $L_r R_r$

- [20 points]** Show that  $F^{(1)}$  is not a secure PRF by presenting a practical adversary  $A$  such that  $\text{Adv}_{F^{(1)}}^{\text{prf}}(A)$  is close to one.
- [30 points]** Show that  $F^{(2)}$  is not a secure PRF by presenting a practical adversary  $A$  such that  $\text{Adv}_{F^{(2)}}^{\text{prf}}(A)$  is close to one.

For both **(1)** and **(2)** above, say what is the advantage achieved by your adversary. Also say what is its running time and the number of oracle queries it makes.

---