Problem Set 2

Due: Monday October 11, 2010, in class.

See course information section (on course web page) for instructions and rules on working on problem sets and turning them in.

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

$$\mathsf{DESY}(K \,\|\, L, M) \;=\; \mathsf{DES}(K, L \oplus M)\ .$$

This defines a family of functions $\mathsf{DESY}\colon\ \{0,1\}^{120} \times \{0,1\}^{64} \to \{0,1\}^{64}$.

(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 $K \,\|\, L$. 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 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 $F\colon\ \{0,1\}^k \times \{0,1\}^l \to \{0,1\}^l$ 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 $F^{(r)}\colon\ \{0,1\}^k \times \{0,1\}^{2l} \to \{0,1\}^{2l}$, 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 $i = 1, \ldots, r$ do
    $L_i \leftarrow R_{i-1}$; $R_i \leftarrow F(K, R_{i-1}) \oplus L_{i-1}$
Return $L_r R_r$

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

2. **[30 points]** Show that $F^{(2)}$ is not a secure PRF by presenting a practical adversary A such that $\mathbf{Adv}^{\mathrm{prf}}_{F^{(2)}}(A)$ 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.
