Problem Set 2 Solutions

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.

A block cipher is a map $E\colon\ \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ for some k, n with the property of being invertible, namely given K, C there is a unique M such that $E(K, M) = C$. This M is denoted $E^{-1}(K, C)$ and must be easily computable given K, C.

The DESY map has the desired form with $k = 120$ and $n = 64$. The important thing is to show it is invertible. This is true because DES itself is invertible. We observe that if $\mathsf{DESY}(K \,\|\, L, M) = C$ then M can be recovered via

$$M \;=\; \mathsf{DES}^{-1}(K, C) \oplus L\ .$$

Accordingly, DESY has as inverse

$$\mathsf{DESY}^{-1}(K \,\|\, L, C) \;=\; \mathsf{DES}^{-1}(K, C) \oplus L\ .$$

This is easily computable given the key $K \,\|\, L$.

(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 equally to the target key.)

Let $T_1, \ldots, T_{2^{56}}$ denote a listing of all 56-bit DES keys. The attack is:

For $i = 1, \ldots, 2^{56}$ do
  $L \leftarrow M_1 \oplus \mathsf{DES}^{-1}(T_i, C_1)$
  If $\mathsf{DES}(T_i, L \oplus M_2) = C_2$ then return $T_i \,\|\, L$

If $T_i \,\|\, L$ is returned by the attack, then this key is consistent with the input-output examples. The attack uses 2^{56} DES computations and 2^{56} DES^{-1} computations.

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_0R_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_rR_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.

Adversary A, as per the definition of the PRF game, has access to an oracle for a function $\mathbf{Fn}\colon \{0,1\}^{2l} \to \{0,1\}^{2l}$. It is trying to determine whether $\mathbf{Fn} = F^{(1)}_K$ for some K or $\mathbf{Fn}$ was chosen at random. It works as follows:

Adversary A
    $x_1 \leftarrow 1^{2l}$
    $y \leftarrow \mathbf{Fn}(x_1)$
    Parse y as LR, where $|L| = |R| = l$
    If $L = 1^l$ then return 1 else return 0

The advantage of A is by definition

$$\mathbf{Adv}^{\mathrm{prf}}_{F^{(1)}}(A) \;=\; \Pr\left[\mathrm{Real}^A_{F^{(1)}} \Rightarrow 1\right] - \Pr\left[\mathrm{Rand}^A_{\{0,1\}^{2l}} \Rightarrow 1\right] .$$

We claim that the first term above is equal to 1 and the second term is equal to 2^{-l}. (And thus the advantage of our adversary is $1 - 2^{-l}$, which is almost 1.) To justify our claim, consider the first term. Here, we are asking what is the probability that A outputs 1 given that it is in game Real, meaning its oracle $\mathbf{Fn}$ is a random instance of the family $F^{(1)}$. Due to the fact that $L_1 = R_0$ in the code of $F^{(1)}$, the condition that A tests will always be true, so it will always output 1 in game Real. Now, consider the second term above. Here, we are asking what is the probability that A outputs 1 given that it is in game Rand, meaning its oracle $\mathbf{Fn}$ is a random function of $2l$ bits to $2l$ bits. In that case, there is a slight possibility that $\mathbf{Fn}$ will output a string that begins with l ones, causing A to output 1. Specifically, the probability of this event is 2^{-l}.

Adversary A is practical because it makes only one oracle query and has running time $O(l)$.

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.

Adversary A, as per the definition of the PRF game, has access to an oracle for a function $\mathbf{Fn}\colon \{0,1\}^{2l} \to \{0,1\}^{2l}$. It is trying to determine whether $\mathbf{Fn} = F^{(2)}_K$ for some K or $\mathbf{Fn}$ was chosen at random. It works as follows:

Adversary A

$x_1 \leftarrow 0^l 1^l$
$y_1 \leftarrow \mathbf{Fn}(x_1)$
Parse y_1 as $L_{1,2}R_{1,2}$, where $|L_{1,2}| = |R_{1,2}| = l$
$x_2 \leftarrow L_{1,2}1^l$
$y_2 \leftarrow \mathbf{Fn}(x_2)$
Parse y_2 as $L_{2,2}R_{2,2}$, where $|L_{2,2}| = |R_{2,2}| = l$
If $L_{2,2} = 0^l$ then return 1 else return 0

The advantage of A is by definition

$$\mathbf{Adv}^{\mathrm{prf}}_{F^{(2)}}(A) \quad = \quad \Pr\left[\mathrm{Real}^{A}_{F^{(2)}} \Rightarrow 1\right] - \Pr\left[\mathrm{Rand}^{A}_{\{0,1\}^{2l}} \Rightarrow 1\right] \ .$$

We claim that the first term above is equal to 1 and the second term is equal to 2^{-l}. (And thus the advantage of our adversary is $1 - 2^{-l}$, which is almost 1.) To justify our claim, consider the first term. Here, we are asking what is the probability that A outputs 1 given that it is in game Real, meaning its oracle $\mathbf{Fn}$ is a random instance of the family $F^{(2)}$. Note that, in game Real, the left half of y_1 will be $L_{1,2} = F_K(1^l) \oplus 0^l = F_K(1^l)$. In the second query, A uses this value as the left half of the input to $\mathbf{Fn}$, so it gets xor-ed with the value of the function at the right half of x_2. But A chose the right half to be 1^l, so $F_K(1^l)$ is xor-ed with itself in the first round. Since any value xor-ed with itself is 0^l, and the right half of the first round's result is propagated to the left hand side of the output, we know that the left half of y_2 will be 0^l. Now, consider the second term above. Here, we are asking what is the probability that A outputs 1 given that it is in game Rand, meaning its oracle $\mathbf{Fn}$ is a random function of $2l$ bits to $2l$ bits. In that case, there is a slight possibility that $\mathbf{Fn}$ will output a string that begins with l 0's, causing A to output 1. Specifically, the probability of this event is 2^{-l}.

Adversary A is practical because it makes only two oracle queries and has running time $O(l)$.

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.
