
Problem Set 2 Solutions

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

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

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

(a) [8 points] Show that DES is a block cipher.

A block cipher is a map $E: \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ 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 DES 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 $\text{DES}(K\|L, M) = C$ then M can be recovered via

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

Accordingly, DES has as inverse

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

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

For $i = 1, \dots, 2^{56}$ do
 $L \leftarrow M_1 \oplus \text{DES}^{-1}(T_i, C_1)$
 If $\text{DES}(T_i, L \oplus M_2) = C_2$ 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 $F: \{0, 1\}^k \times \{0, 1\}^l \rightarrow \{0, 1\}^l$ 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_0R_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_rR_r

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

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

Adversary A^g
 Let $x_1 = 1^{2l}$ be the string of $2l$ ones
 Query g on input x_1 , and get back response $y = g(x_1)$
 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

$$\mathbf{Adv}_{F^{(1)}}^{\text{prf}}(A) = \Pr[\mathbf{Exp}_{F^{(1)}}^{\text{prf-1}}(A) = 1] - \Pr[\mathbf{Exp}_{F^{(1)}}^{\text{prf-0}}(A) = 1].$$

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 world 1, meaning its oracle g 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 world 1. Now, consider the second term above. Here, we are asking what is the probability that A outputs 1 given that it is in world 0, meaning its oracle g is a random function of $2l$ bits to $2l$ bits. In that case, there is a slight possibility that g will output a string that begins with l ones, causing D 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 $\mathbf{Adv}_{F^{(2)}}^{\text{prf}}(A)$ is close to one.

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

Adversary A^g
 Let $x_1 = 0^l1^l$ be the string consisting of l zeros followed by l ones
 Query g on point x_1 , and get back response $y_1 = g(x_1)$
 Parse y_1 as $L_{1,2}R_{1,2}$, where $|L_{1,2}| = |R_{1,2}| = l$

Query g on point $x_2 = L_{1,2}1^l$, and get back response $y_2 = g(x_2)$
 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

$$\mathbf{Adv}_{F^{(2)}}^{\text{prf}}(A) = \Pr[\mathbf{Exp}_{F^{(2)}}^{\text{prf-1}}(A) = 1] - \Pr[\mathbf{Exp}_{F^{(2)}}^{\text{prf-0}}(A) = 1] .$$

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 world 1, meaning its oracle g is a random instance of the family $F^{(2)}$. Note that, in World 1, 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 g , 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 world 0, meaning its oracle g is a random function of $2l$ bits to $2l$ bits. In that case, there is a slight possibility that g 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.
