Quiz 1 Solutions

Problem 1 [30 points] Let $m \geq 1$ be an integer, and let D_m denote the set $\{1, \ldots, m-1\}$. Consider the symmetric encryption scheme in which the key is a randomly chosen element of D_m, the message space is also D_m, and the encryption of message $M \in D_m$ under key $K \in D_m$ is $M \cdot K \bmod m$, meaning obtained by multipling the integers M and K and then taking the remainder modulo m. For $m = 4$, is this encryption scheme perfectly secure? Why or why not?

The simplest way to get a handle on what is going on here is to make a table whose row K, column M entry is $\mathcal{E}_K(M)$:

$K =$

	$M =$ 1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Let $C = 0$ and $M_1 = 1$, $M_2 = 2$. Then

$$\begin{aligned} \Pr\left[\mathcal{E}_K(M_1) = 0\right] &= 0 \\ \Pr\left[\mathcal{E}_K(M_2) = 0\right] &= \frac{1}{3} \end{aligned}$$

Above, the probability is over K chosen at random from D_m. Thus the first probability is the number of 0 entries in column 1 of the table divided by the number of rows (3), while the second probability is the number of 0 entries in column 2 of the table divided by the number of rows (3). Since the probabilities are not equal, the scheme is not perfectly secure.

Problem 2 [70 points] Define F: $\{0,1\}^{256} \times \{0,1\}^{384} \to \{0,1\}^{256}$ as follows. A key $K = K_1 \,\|\, K_2$ is a pair of 128-bit strings and an input $x = x[1]x[2]x[3]$ consist of three 128-bit blocks. Then

$F_{K_1||K_2}(x)$
$y_1 \leftarrow \mathsf{AES}_{K_1}(x[1] \oplus x[2])$
$y_2 \leftarrow \mathsf{AES}_{K_2}(x[2] \oplus x[3])$
Return $y_1||y_2$

Above $a||b$ denotes the concatenation of strings a and b. (For example, $01||00 = 0100$.)

1. **[10 points]** Is F a block cipher? Why or why not?

A block cipher is a map E: $\{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^L$ where $\ell = L$ and E_K is a permutation for every $K \in \{0,1\}^k$. Here we have $\ell = 384 \neq 256 = L$ so F is not a block cipher. Indeed, E_K cannot be a permutation because its domain $\{0,1\}^{384}$ is larger than its range $\{0,1\}^{256}$.

2. **[30 points]** Give the best key recovery attack that you can on F. Say how many AES and AES^{-1} computations and input-output examples your attack uses. Your score depends on these quantities.

Let $(x[1]x[2]x[3], y_1||y_2)$ be an input-output example under target key $K = K_1 \,\|\, K_2$. Exhaustive key search takes 2^{256} time, because the length of the target key $K_1||K_2$ is $128+128 = 256$ bits. But we can search for the two halves of the key separately, as follows.

Let $T_1, \ldots, T_N$ denote a listing of AES keys, where $N = 2^{128}$. Then the attack is as follows:

for $i = 1, \ldots, N$ **do**
  If $\mathsf{AES}_{T_i}(x[1] \oplus x[2]) = y_1$ then
    $L_1 \leftarrow T_i$
  If $\mathsf{AES}_{T_i}(x[2] \oplus x[3]) = y_2$ then
    $L_2 \leftarrow T_i$
Return $L_1||L_2$

The attack returns a key consistent with the input-output example. To increase the chance of getting the target key one could test the candidate keys under a second input-output example.

The attack uses $2 \cdot 2^{128} = 2^{129}$ AES applications.

3. **[30 points]** Give the best PRF-attack you can on F. Say what is the advantage achieved by your adversary, what is its running time, and how many oracle queries it makes. The number of points you get depends on these quantities.

A weakness of the construct we can exploit is that

$$F_{K_1 \,\|\, K_2}(0^{128}||1^{128}||0^{128}) = F_{K_1 \,\|\, K_2}(1^{128}||0^{128}||1^{128}) \; .$$

This leads to the following.

Adversary A
  $a \xleftarrow{\$} \mathbf{Fn}(0^{128}||1^{128}||0^{128})$
  $b \xleftarrow{\$} \mathbf{Fn}(1^{128}||0^{128}||1^{128})$
  If $(a = b)$ then return 1 else return 0

The advantage of A is by definition

$$\mathbf{Adv}^{\mathrm{prf}}_F(A) \;\; = \;\; \Pr\left[\mathrm{Real}^A_F \Rightarrow 1\right] - \Pr\left[\mathrm{Rand}^A_{\{0,1\}^{256}} \Rightarrow 1\right] \; .$$

In Game Real_F we will have $a = F_{K_1 \,\|\, K_2}(0^{128}1^{128}0^{128})$ and $b = F_{K_1 \,\|\, K_2}(1^{128}0^{128}1^{128})$ where $K_1 \,\|\, K_2$ is the target key chosen by the **Initialize** procedure. By the above observation we will have $a = b$, so

$$\Pr\left[\text{Real}_F^A \Rightarrow 1\right] = 1 \ .$$

In Game Rand_F the responses a, b will be independent random 256-bit strings so

$$\Pr\left[\text{Rand}_{\{0,1\}^{256}}^A \Rightarrow 1\right] = \Pr\left[a = b\right] = 2^{-256} \ .$$

So

$$\mathbf{Adv}_F^{\text{prf}}(A) = 1 - 2^{-256} \ .$$

The number of oracle queries made by A is 2 and its running time is a small constant.
