Homework 2

David Miller & Hannah McLaughlin
CIS 5371: Cryptography

February 20, 2018

Problem 1. *Bob has a blockcipher $E : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$, but hes unhappy with the short key length k. He wants to double the key length by constructing a blockcipher $F : \{0,1\}^{2k}\{0,1\}^n \rightarrow \{0,1\}^n$ on top of E, but he doesnt want to use the 3DES-2 construction, since its too slow for him. So Bob tries the following construction: $F_{K_1,K_2}(x) = E_{K_1}(x \oplus K_2)$. Give a key-recovery attack on Bobs construction, using $\mathcal{O}(2^k)$ time, but only $\mathcal{O}(1)$ space and queries.*

Let Q_0, Q_1 be the querries O^1 and 1^l to the oracle, respectively. From this we obtain ciphertexts c_0 and c_1

$$Q_0 = 0^l \Rightarrow\ c_0 \leftarrow E_{K_1}(K_2) \tag{1}$$

$$Q_1 = 1^l \Rightarrow\ c_1 \leftarrow E_{K_1}(1 \oplus K_2) \tag{2}$$

such that K_1, K_2 are the unknown keys we are trying to recover. Algorithm 1 leverages these queries to recover K_1, K_2.

Algorithm 1 Key-Recovery Attack

```
for $k' \in \mathcal{K}$ do
    $k_2' \leftarrow E_{k'}^{-1}(Q_0)$
    $x \leftarrow E_{k'}^{-1}(Q_1)$
    if $x \oplus\ k_2' = 1^l$: then
        $K_1 \leftarrow k'$ , $K_2 \leftarrow k_2'$ return
    end if
end for
```

The for loop will iterate at most $|\mathcal{K}| = 2^k$ times, resulting in $\mathcal{O}(2^k)$ time complexity. Algorithm 1 overwrites two temporary variables for each $k' \in \mathcal{K}$ and stores the keys when correctly determined which results in $\mathcal{O}(1)$ space complexity. Since we make just two queries to the oracle we achieve $\mathcal{O}(1)$ query complexity. The algorithm is essentially a brute force approach by iterating over all possible K_1 values since we get K_2 "for free" by knowing how the encryption relies on K_2.

Problem 2. *Alice has a function family $F : \{0,1\}^k \times \{0, 1\}^n \rightarrow \{0,1\}^n$ that she intends to use as a PRF. However, this F has a serious weakness: for any fixed key K, if we pick a random message $x \leftarrow \{0, 1\}^n$, then the first byte of $F_K(x)$ will be 0^8 with probability $\frac{1}{128}$, instead of the desired probability $\frac{1}{256}$. Adversary Eve wants to break the PRF security of F. Of course its trivial to have advantage $\frac{1}{128} - \frac{1}{256} = \frac{1}{256}$ using just a single random query. However, being greedy, Eve aims for more. Give an efficient PRF attack (of multiple queries) to achieve advantage at least 0.99. For your analysis, you can use the following tool:*

Hoeffding's inequality: Let $X_1, \ldots, X_m$ be independent and identically distributed random variables, each in $\{0,1\}$ and each taking on the value 1 with probability p. Let $\overline{X} = \frac{1}{n}$ $(X_1 + \cdots + X_n)$ be the "empirical mean" of the observations, which has the expected value $\mathbb{E}[X] = p$. Then for any real number $t \geq 0$,

$$\Pr[|\overline{X} - p| \geq t] \leq 2e^{-2nt^2}$$

To achieve an advantage of at least 0.99, we will use Hoeffding's inequality.

We know

$$Adv_A = Pr[Real \Rightarrow 1] - Pr[Random \Rightarrow 1] \quad (1)$$
$$0.99 \leq (1 - 2e^{-2nt^2}) - 2e^{-2nt^2} \quad (2)$$

We must solve for n, or the number of queries made to the oracle, to give an efficient PRF attack.

$$0.99 \leq 1 - 2e^{-2nt^2} - 2e^{-2nt^2} \quad (3)$$
$$0.99 - 1 \leq -2e^{-2nt^2} - 2e^{-2nt^2} \quad (4)$$
$$-0.01 \leq -4e^{-2nt^2} \quad (5)$$
$$\frac{-0.01}{-4} \geq e^{-2nt^2} \quad (6)$$
$$\ln\frac{0.01}{4} \geq -2nt^2 \quad (7)$$
$$-\ln\frac{4}{0.01} \geq -2nt^2 \quad (8)$$
$$-\ln(400) \geq -2nt^2 \quad (9)$$
$$\frac{\ln(400)}{2t^2} \leq n \quad (10)$$

Now we find a t value so that there is no intersection between the closed t-neighborhoods of $\frac{1}{128}$ and $\frac{1}{256}$, where the closed t-neighborhood of a point x is the set $\overline{B_t(x)} = \{y \mid |y - x| \leq t\}$. We use the midpoint formula to help us choose it.

$$\frac{\frac{1}{128} - \frac{1}{256}}{2} = \frac{3}{512} \quad (11)$$

For $t = \frac{3}{512} - \frac{1}{256} = \frac{1}{128} - \frac{3}{512} = \frac{1}{512}$ we have the $\overline{B_t(\frac{1}{128})} \cap \overline{B_t(\frac{1}{256})}$ is the singleton $\{\frac{3}{512}\}$. Therefore any value less than $t = \frac{1}{512}$ will do. Letting $t = \frac{2}{1025}$ we get that
Therefore $n \geq 786{,}848$ queries to achieve an advantage of at least 0.99. To solve this, we keep a counter variable that counts the number of queries where the first byte is equal to 0^8 and have the queries x_i uniformly and independently distributed for $i = 1, \ldots, n$.

Algorithm 2 Breaking PRF Security

```
counter ← 0, $t$ ← 2/1025, $n$ ← 786848
for $i = 1$ to $n$ do
    if first byte of $F_k(x_i) = 0^8$: then
        counter ← counter + 1
    end if
end for
if $|1/128 - \text{counter}/n| \leq t$ then return 1
else return 0
end if
```

From Algorithm 2, we have that counter/$n = \frac{1}{n}(y_1 + \cdots + y_n)$ where $y_i = 1$ if the first byte was 0^8 and 0 otherwise. Therefore, Algorithm 2 returns 1 if we determined that we are in the real room with a confidence level of 99%.