# CS 427, Assignment 1

Cody Malick
malickc@oregonstate.edu

January 20, 2017

## 1

We can find the value of $k$ by xoring $m$ and $c$

$m \oplus c:$

110101100010110
100111011011111

010010111001001

Then, $k = 010010111001001$. We can use this info to then xor the value of $m'$ with the value of $k$:

$m' \oplus k:$

010010111001001
001000000101111

011010111100110

Then our encrypted $m'$, lets call it $c' = 011010111100110$

## 2

We can show that these two libraries are not interchangable by inspecting the distribution of each library:

$\mathcal{L}_1$ has a probability distribution of $\{0,1\}^\lambda - 0^\lambda$

$\mathcal{L}_2$, on the other hand, has a probability distribution of $\{0,1\}^\lambda$

This makes it quite obvious that there is a difference between the two distributions. Specifically, that $\mathcal{L}_2$ can produce the key consisting of only 0's, while $\mathcal{L}_1$ cannot. While a key consisting of only zeroes isn't ideal, it is a difference in behavior which Eve can exploit. In an example case:

If calling program $prog(m_1)$ which calls $\mathcal{L}_1$ or $\mathcal{L}_2$, the adversary Eve can't choose the function, but she can choose the message $m_1$. In the case of $\mathcal{L}_2$, it simply returns a random ciphertext $c \leftarrow \{0,1\}^\lambda$, while $\mathcal{L}_1$ returns an OTP encrypted ciphertext with a random key without the possibility of an all zero key. The probabilities of $\mathcal{L}_1$ and $\mathcal{L}_2$ are as follows (where $P(x)$ is the probability of x):

$P(\mathcal{L}_1) = \frac{1}{2^\lambda - 1}$
$P(\mathcal{L}_2) = \frac{1}{2^\lambda}$

Because the probabilities differ, there is a case where Eve can find a difference in behavior, specifically that $\mathcal{L}_1$ cannot produce an all zero key.

# 3

We can show these two functions, $\mathcal{L}_1, \mathcal{L}_2$ are interchangable by slowly changing bits of $\mathcal{L}_1$ to look like $\mathcal{L}_2$. Our end goal is to show that $\mathcal{L}_1$ values in the same range that $\mathcal{L}_2$ does:

1. change $\mathcal{L}_2$ to include: $c = c \bmod n$
   This doesn't change the calling function as the modulus function is the size of $\mathbb{Z}$, leaving the library behavior unchanged

2.

3.

# 4