CS 427/519: Homework 1

Due: Friday January 20, 10pm; typed and submitted electronically.

1. I asked Alice to encrypt
   \[ m = 110101100010110 \]
   using one-time pad, and I saw that the result was
   \[ c = 100111011011111 \]
   If Alice encrypts
   \[ m' = 001000000101111 \]
   using the same one-time pad key as before, what would be the result? Above all, show how you derived the answer.

2. Let \( 0^\lambda \) denote the string of \( \lambda \) zeroes. In one-time pad, if \( 0^\lambda \) is chosen as the key, then Alice ends up sending her plaintext in the clear! This can’t be good!
   
   So let’s imagine that Alice always avoids choosing \( 0^\lambda \) as her key. In other words, she modifies the KeyGen algorithm so that instead of choosing \( k \) uniformly from \( \{0,1\}^\lambda \), she chooses uniformly from \( \{0,1\}^\lambda \setminus \{0^\lambda\} \) (the set of all strings other than the all-zeroes string).
   
   Show that this is a bad idea, as far as our security definition is concerned. Show that the following two libraries are not interchangeable:

   \[
   \begin{array}{c}
   \mathcal{L}_1 \\
   \text{VIEW}(m):
   \begin{align*}
   k &\leftarrow \{0,1\}^\lambda \setminus \{0^\lambda\} \\
   c &:= k \oplus m \\
   \text{return } c
   \end{align*}
   \\
   \mathcal{L}_2 \\
   \text{VIEW}(m):
   \begin{align*}
   c &\leftarrow \{0,1\}^\lambda \\
   \text{return } c
   \end{align*}
   \end{array}
   \]

   You must explicitly give a calling program and argue that its output probabilities are different in presence of the two libraries.

   \text{Hint:} Try to think about some event that can happen in one library but not the other.

3. Show that the following two libraries are interchangeable:

   \[
   \begin{array}{c}
   \mathcal{L}_1 \\
   \text{QUERY}(x \in \mathbb{Z}_n):
   \begin{align*}
   k &\leftarrow \mathbb{Z}_n \\
   c &:= (k + x) \mod n \\
   \text{return } c
   \end{align*}
   \\
   \mathcal{L}_2 \\
   \text{QUERY}(x \in \mathbb{Z}_n):
   \begin{align*}
   c &\leftarrow \mathbb{Z}_n \\
   \text{return } c
   \end{align*}
   \end{array}
   \]

   (Refer to chapter 0 for questions about any of this notation.)

grad. Let \( \Sigma \) be an encryption scheme with keyspace \( \mathcal{K} \) and plaintext space \( \mathcal{M} \). Prove that if \( |\mathcal{K}| < |\mathcal{M}| \) then the scheme cannot have one-time secrecy.