CS 427/519: Homework 1

Due: Friday January 19, 10pm; typed and submitted electronically.

1. Consider the following variant of one-time pad, which uses \( \mathbb{Z}_n \) instead of \( \{0, 1\}^\lambda \). Refer to chapter 0 for questions about any of this notation.

\[
\begin{align*}
\mathcal{K} &= \mathbb{Z}_n & \text{KeyGen:} & k \leftarrow \mathbb{Z}_n & \text{return } k \\
M &= \mathbb{Z}_n & \text{Enc}(k, m): & \text{return } (k + m) \mod n \\
C &= \mathbb{Z}_n & \text{Dec}(k, c): & \text{??}
\end{align*}
\]

(a) What must \( \text{Dec} \) be in order for the scheme to satisfy correctness?

(b) Show that the scheme has uniformly distributed ciphertexts. In other words, show that the following two libraries are interchangeable:

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

\[
\begin{align*}
\mathcal{L}_2 & \text{ QUERY}(x \in \mathbb{Z}_n): & c \leftarrow \mathbb{Z}_n \\
& & \text{return } c
\end{align*}
\]

2. Show that the following libraries are not interchangeable. Describe an explicit distinguishing calling program, and compute its output probabilities when linked to both libraries:

\[
\begin{align*}
\mathcal{L}_{\text{left}} & \text{ QUERY}(m_L, m_R \in \{0, 1\}^\lambda): & k \leftarrow \{0, 1\}^\lambda \\
& & c := k \oplus m_L \\
& & \text{return } (k, c)
\end{align*}
\]

\[
\begin{align*}
\mathcal{L}_{\text{right}} & \text{ QUERY}(m_L, m_R \in \{0, 1\}^\lambda): & k \leftarrow \{0, 1\}^\lambda \\
& & c := k \oplus m_R \\
& & \text{return } (k, c)
\end{align*}
\]

3. Consider the following encryption scheme. It supports plaintexts from \( M = \{0, 1\}^\lambda \) and ciphertexts from \( C = \{0, 1\}^{2\lambda} \). Its keyspace is:

\[
\mathcal{K} = \left\{ k \in \{0, 1, \_\}^{2\lambda} \mid \text{k contains exactly } \lambda \text{ } \_ \text{ characters} \right\}
\]

To encrypt plaintext \( m \) under key \( k \), we “fill in” the \( \_ \) characters in \( k \) using the bits of \( m \).

Show that the scheme does not have one-time secrecy, by constructing a program that distinguishes the two relevant libraries from the one-time secrecy definition.

Example: Below is an example encryption of \( m = 1101100001 \).

\[
\begin{align*}
k &= 1\_\_0\_\_11010.1_0.0\_\_ \\
m &= 11 \ 01 \ 1 \ 0 \ 0 \ 001 \\
\Rightarrow \text{Enc}(k, m) &= 11100111010100000001
\end{align*}
\]

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

For full credit, construct an explicit distinguisher between the one-time secrecy libraries.