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.

$\mathcal{K} = \mathbb{Z}_n$ $\mathcal{M} = \mathbb{Z}_n$ $\mathcal{C} = \mathbb{Z}_n$	KeyGen: $k \leftarrow \mathbb{Z}_n$ return k	Enc(k, m): return $(k + m) \% n$	Dec(k, c): ??

   (a) What must 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:

$\mathcal{L}_1$	$\mathcal{L}_2$
QUERY$(x \in \mathbb{Z}_n)$: $k \leftarrow \mathbb{Z}_n$ $c := (k + x) \% n$ return c	QUERY$(x \in \mathbb{Z}_n)$: $c \leftarrow \mathbb{Z}_n$ return c

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:

$\mathcal{L}_{\text{left}}$	$\mathcal{L}_{\text{right}}$
QUERY$(m_L, m_R \in \{0,1\}^\lambda)$: $k \leftarrow \{0,1\}^\lambda$ $c := k \oplus m_L$ return (k, c)	QUERY$(m_L, m_R \in \{0,1\}^\lambda)$: $k \leftarrow \{0,1\}^\lambda$ $c := k \oplus m_R$ return (k, c)

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

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

   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 $m = 1101100001$.

```
          k = 1__0__11010_1_0_0___
          m =  11 01      1 0 0 001
⇒ Enc(k, m) = 11100111010110000001
```

grad. Let Σ 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.

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