EE 720: Introduction to Number Theory and Cryptography (Spring 2018)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Assignment 2: 10 points　　　　Date: January 23, 2018

Find the pdf file corresponding to your roll number in the directory `https://www.ee.iitb.ac.in/~sarva/courses/EE720/2018/assignments/assignment2/`. Upload the answers as a **pdf** file in Moodle. Use the tex file provided in the directory to fill in your answers. The **upload deadline** will be 11:00pm IST on Wednesday, January 31, 2018.

1. [5 points] State whether the following encryption scheme is perfectly secret or not. Justify your answer either with a proof or a counterexample.

   The message space is $\mathcal{M} = \left\{ m \in \{0,1\}^l \mid \text{the last bit of } m \text{ is } 0 \right\}$. Algorith $\texttt{Gen}$ chooses a uniform key from the keyspace $\{0,1\}^{l-1}$. $\texttt{Enc}_k(m) = m \oplus (k \| 0)$ and $\texttt{Dec}_k(c) = c \oplus (k \| 0)$.

   Solution: Write your answer here

2. [5 points] Prove that if only a single character is encrypted, then the shift cipher is perfectly indistinguishable. Prove this directly without proving the perfect secrecy of the scheme and then using the equivalence of perfect secrecy and perfect indistinguishability.

   Solution: Write your answer here