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] Prove that the Vigenére cipher using period t is perfectly indistinguishable when used to encrypt messages of length t. 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

2. [5 points] When the one-time pad is used with the all-zeros key, i.e. $k = 0^l$, we have $\mathtt{Enc}_k(m) = m \oplus k = m$. This means that the plaintext will be sent as it is. To prevent this, suppose we modify the one-time pad to use only non-zero keys, $k \neq 0^l$. The key generation algorithm `Gen` picks key k uniformly from the set $\{0,1\}^l \setminus \{0^l\}$ which has cardinality $2^l - 1$. Is this modified scheme still perfectly secret? Justify your answer either with a proof or a counterexample.

   Solution: Write your answer here