## EE 720: Introduction to Number Theory and Cryptography (Spring 2018) Instructor: Sarayanan Vijayakumaran

Instructor: Saravanan Vijayakumaran Indian Institute of Technology Bombay

Date: January 23, 2018

Assignment 2: 10 points

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] 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