## 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] Let  $negl_1$  be a negligible function. Prove that for any positive polynomial p, the function  $negl_2$  defined by  $negl_2(n) = p(n) \cdot negl_1(n)$  is negligible.

Solution: Write your answer here

2. [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  $\mathcal{M} = \{0, \dots, 4\}$ . Algorithm Gen chooses a uniform key from the keyspace  $\{0, \dots, 5\}$ .  $\operatorname{Enc}_k(m) = (k+m) \mod 5$  and  $\operatorname{Dec}_k(c) = (c-k) \mod 5$ .

Solution: Write your answer here