EE 720: Introduction to Number Theory and Cryptography (Spring 2018) 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] 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] Let $negl_1$ and $negl_2$ be negligible functions. Prove that the function $negl_3$ defined by $negl_3(n) = negl_1(n) + negl_2(n)$ is negligible.

Solution: Write your answer here