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

Assignment 3: 10 points Date: April 8, 2018

Upload the answers as a **pdf** file in Moodle. The **upload deadline** will be 11:00pm IST on Wednesday, April 11, 2018.

1. [5 points] Let $p = rq + 1$ where $p, q$ are primes. Then prove that

$$G = \left\{ h^r \bmod p \mid h \in \mathbb{Z}_p^* \right\}$$

   is a subgroup of $\mathbb{Z}_p^*$ of order $q$.

2. [5 points] If the decisional Diffie-Hellman problem is hard relative to a group-generation algorithm $\mathcal{G}$, then prove that the El Gamal encryption is CPA-secure.