EE 720: Introduction to Number Theory and Cryptography (Spring 2023)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Assignment 1: 20 points Date: August 11, 2023

1. [5 points] Show that the shift, substitution, and Vigenère ciphers can all be broken using a chosen-plaintext attack. What is the minimum amount of chosen plaintext is needed to recover the key for each of the ciphers?

2. [5 points] When using the one-time pad with the key $k = 0^l$, we have $\texttt{Enc}_k(m) = k \oplus m = m$ and the message is sent in the clear. It has therefore been suggested to modify the one-time pad by only encrypting with $k \neq 0^l$ (i.e., to have $\texttt{Gen}$ choose k uniformly from the set of nonzero keys of length l). Is this modified scheme still perfectly secret? Explain.

3. [10 points] Let $\Pi = (\texttt{Gen}, \texttt{Enc}, \texttt{Dec})$ be a perfectly indistinguishable private-key encryption scheme. Prove that it is perfectly secret.