ECE 404 HW 6

Nimal Padmanabhan

February 28, 2023

1 Programming Problem

For this programming problem, we have implemented RSA encryption and decryption in two parts. For the first part, we were generated two primes p and q using the PrimeGenerator class. Next, we implemented the encryption algorithm that takes in the message plaintext, the newly generated prime number text files (p and q), and the encrypted output text file. For decryption, we read in the ciphertext as a hexstring that will be constructed into a BitVector object and use the Chinese Remainder Theorem to decrypt the encrypted message.

For part 2, we implemented two features of breaking the RSA algorithm using an e-value of 3. For the previous part, we used in an e-value of 6533. Part 2 has two sub parts: encrypting the message file with three different p and q pairs and cracking the encrypted file three public keys and private keys along with using the Chinese Remaider Theorem to deal with arithmetic with large numbers and speeding up the RSA algorithm. Towards the end of the cracking function, we only write the last half of the 256 bits since the decrypted BitVector is already padded on the left with zeroes.