Jeremy Cross
200319513

ENSE 350 Lab 2 Report

Building an RSA Cryptosystem

1) creates a public and private key

The first part of the algorithm takes a p and q value and creates n and phi using the proper equations. It then takes an e value and checks to see whether it is coprime to phi. If not then it increments e until it is. There is now a public key with both an e and n value. The next step is to create a private key with a d and n value. In order to find d, we can use the pulveriser method to find the values of x and y in e*x + phi*y = 1 where x is the value of d. Once we have d then we have our private key.

2) Encryption

When given a message m the encryption component of the algorithm will encrypt the message. This can be done with a repeated squaring function that takes in m, e, and n and calculates m^e mod n.

3) Decryption

Decrypting the message m can be done the same way as encrypting. The repeated squaring function can be used again but instead the values of m', d, and n can be sent in to calculate m'^d mod n. This Decrypts the message back to its original state.