Brent Reinhardt

Michael Harkins Group Name: The Null Terminators

Samuel Schneider

Diffie Hellman Key Exchange

This project will take input data and will be able to encrypt and decrypt said data following the style of the Diffie Hellman Key Exchange protocol. This encryption is a very useful solution for two people to encrypt a document when communicating over an unsecure telephone line.In this encryption, two people agree to use a prime p and a primitive root: a of p. One person picks an unmentioned integer, k1, and sends to the other person ak1 **mod** p. The other person picked their own secret number, k2, and sends over ak2 **mod** p. Person 1 calculates (ak2 ) k1 **mod** p. Person 2 calculates (ak1 ) k2 **mod** p. Now both person 1 and 2 have the same key to encrypt and decrypt the document without either of them sharing which numbers they used.

This project will be broken into 3 sections for completing it:

One person will create the code that asks for the required variables and will compute the key.

Another person will create the code for encrypting the data.

The last person will create the decryption code.