CS 6353
Unix and Network Security
Assignment 4
Due Wednesday April 20

1. (100 pts) Write a program that encrypts/decrypts data using RSA. Use the *openssl* implementation of RSA for this purpose. Include the following in your program to use openssl and rsa

   ```
   #include <openssl/ssl.h>
   #include <openssl/rsa.h>
   ```

   In your program use 1024 bit keys and encrypt/decrypt 256 byte data. Do all of the following in your program

   - Generate RSA keys.
   - Encrypt using public key and decrypt using private key. Compare the result.
   - Encrypt using private key and decrypt using public key. Compare the result.

   You need these functions in your program

   ```
   RSA_generate_key(...);
   RSA_public_encrypt(...);
   RSA_private_decrypt(...);
   RSA_private_encrypt(...);
   RSA_public_decrypt(...);
   ```

   You can use linux or solaris machines for this assignment. You can compile your program on solaris using the following format.

   ```
   g++ -o assign4 assign4.c -lcrypto -lsocket
   ```

   OpenSSL documentation for RSA is available at http://dev.openssl.org/docs/crypto/rsa.html

   Submit your program electronically using the blackboard system

   The program you submit should be your own work. Cheating will be reported to office of academic integrity. Both the copier and copiee will be held responsible.