

## ENTS 689i: Network Immunity

### Problem Set #1

Due: September 25, 2008

1. Chapter 2, Problem 2
2. Chapter 2, Problem 10
3. Chapter 2, Problem 16
4. Chapter 2, Problem 17
5. Chapter 2, Problem 22
6. Chapter 10, Problem 21
7. Chapter 10, Problem 22
8. GNU Privacy Guard (GPG)
  - a. Download and install GNU's GPG product. For Windows, the installation files can be located here: <ftp://ftp.gnupg.org/gcrypt/binary/gnupg-w32cli-1.4.9.exe>
  - b. Generate a key for yourself by running (accept all the default values) and export it into a file:
    - i. `"\progra~1\gnu\gnupg\gpg --gen-key"`
    - ii. `"\progra~1\gnu\gnupg\gpg --export -a MyName > key.txt"`
  - c. Create a file with your name in it and encrypt it using symmetric key "ents689i":
    - i. `"echo MyName > symmetric.txt"`
    - ii. `"\progra~1\gnu\gnupg\gpg -c symmetric.txt"`
  - d. Download my public key: <http://www.cs.umd.edu/~clancy/tcc.umd.edu.txt>
    - i. Save it into a file
    - ii. Import it into your GPG keyring
    - iii. `"\progra~1\gnu\gnupg\gpg --import -a tcc.umd.edu.txt"`
  - e. Create another file with your name in it, sign it with your private key, and encrypt it using my public key:
    - i. `"echo MyName > public.txt"`
    - ii. `"\progra~1\gnu\gnupg\gpg -c public.txt"`
    - iii. `"\progra~1\gnu\gnupg\gpg -e -u MyName -r tcc@umd.edu public.txt"`
  - f. Email the following files to [tcc@umd.edu](mailto:tcc@umd.edu) with subject line "ENTS689i HW1":
    - i. key.txt
    - ii. symmetric.txt.pgp
    - iii. public.txt.pgp