

**CS 772/872: Computer and Network Security
Fall 2009**

Homework #4

Due: October 29, 2009

Points 20

This homework deals with PGP. gpg (GNU PGP) is now installed on our Unix systems (e.g., cash, dilbert., ...). You can do `man gpg` to get more details. Using gpg do the following.

1. List the features that PGP offers (just to make sure you have read about PGP)
2. Create a public key/private key
3. Generate a symmetric key
4. Encrypt this file (hw4.pdf) using symmetric file
5. Sign the file
6. Receive my public key
7. Send your public key to mukka@cs.odu.edu
8. Send your symmetric key using my public key
9. Send the encrypted and signed file to me (mukka@cs.odu.edu)
10. Receive my encrypted file
11. Decrypt the file I have sent.
12. Modify the file that I have sent, encrypt, and send it back to me.
13. Verify my signature
14. Receive public keys from others and list all public keys (using GPG)
15. Sign my public certificate and send it back to me.

Submit the source code, the object code, the input data, and the output.