CSC 439/539 Advanced Information Security, Spring 2013
Question Bank: Module 3 – Email Security

1) Explain how would use PGP for:
   a. Authentication.
   b. Confidentiality
   c. Confidentiality and Authentication

For each case, you need to explain the order in which the message is packaged at the sender side and how it is extracted at the receiver side. You can explain in words as a sequence of actions or illustrate using a flow diagram.

2) What specific algorithms are used by PGP for:
   a. Hashing
   b. Encryption for confidentiality
   c. Public-key encryption
   d. Compression
3) What is the significance and unique characteristic of the PGP Session key? Also, explain how it is generated at the sender side.
4) What is Key ID in the context of PGP? Explain how PGP lets the sender to efficiently notify the public keys that were used for encryption and to be used for decryption.
5) Explain the structure of the message transmitted using S/MIME?
6) Briefly explain the working of the DKIM standard? What is its primary difference when compared to PGP and S/MIME?