EMAIL Security

1. What are the five principal services provided by PGP?
2. Why does PGP generate a signature before applying compression?
3. Why is R64 conversion useful for an e-mail application?
4. What is MIME?
5. What is S/MIME?
6. The first 16 bits of the digest in PGP are transmitted in the clear.

    a. To what extent does this compromise the security of the hash algorithm?
    b. To what extent does it in fact perform its intended function, namely, to help determine if the correct RSA key was used to decrypt the digest?

7. In the PGP scheme, what is the expected number of session keys generated before a previously created key is produced?
8. In PGP, what is the probability that a user with N public keys will have at least one duplicate key ID?
9. Why does PGP use CFB rather than say CBC?
10. List three limitations of RFC 822 that motivated the creation of MIME.
11. What is the purpose of *Content-Type* header in MIME?
12. What is the difference between base64 and quoted-printable MIME transfer encodings
13. What are the four functions of S/MIME?
14. What is the digital signature algorithm that must be supported by all S/MIME agents?