Tutorial-XIV (SSL, TLS/PGP)

1. What is the length of the key material if the cipher suite is one of the following?
(i) SSL_RSA_WITH_NULL_MD5
(ii) SSL_RSA_WITH_NULL_SHA

2. Show the formula/diagram for the following:
(i) Key material in SSL
(ii) MAC in SSL
(iii) Hash calculation for Certificate Verify message in SSL
(iv) Data expansion in TLS
(v) PRF in TLS

3. (i)Answer the following questions about tag values in PGP:
a. Can a packet with a tag value of 1 contain another packet?
b. Can a packet with a tag value of 6 contain another packet?

(ii) What types of a packet should be sent in PGP to provide the following security services:
a. Confidentiality
b. Message integrity
c. Authentication