Assignment V

Cryptography and Network Security (CSE 324)

1a. Along with neat block diagrams explain the different ways of generating digital signatures.

b. What are the basic approaches in Bundling Security Associations in IPSec ?

2a. Give the classification of web security threats?
b. Explain message exchanges of IKEV2 Exchange protocol.

3a. What is SSL connection? Explain the connection state parameters.
b. What is the function of AH and ESP? Give the corresponding header formats.

4a. Explain the operation of SSL record protocol.
b. Explain the functions of S/MIME.

5a. Give an example and explain PGP message compression.
b. Distinguish between SSL and TLS protocols.

6a. Draw the time line diagram and explain SSL handshake protocol operation.
b. Explain the different cases in combining Security Associations