Department of Computer Science and Engineering
CS6004 - Cyber Forensics
Question Bank (2017-18 ODD)

Unit 1. NETWORK LAYER SECURITY &TRANSPORT LAYER SECURITY

Part-A

1. What are the basic components of the IPsec security?
2. What is the security service provided by IPsec ?
3. What are the seven doc of IPsec?
4. What are the three parameters used to identify SA?
5. Name the two databases for processing IP traffic ?
6. Differentiate two modes of SA.
7. What is function of IPsec AH ?
8. Draw the AH format used in IPsec protocol ?
9. What is anti-replay ?
10. What is the function of IPsec ESP ?
11. Draw the AH format used in IPsec protocol ?
12. How secret key is established between sender and receiver using Deffie Hellman algorithm?
13. What is anti-clogging?
14. What is replay attack ?
15. Name the five default exchange types of ISAKMP ?
16. Draw the two layers of protocols used in SSL ?
17. What is need of Change Cipher spec protocol?
18. List the alert messages defined in SSL alert protocol?
19. How security is provided by TLS protocol ?
20. List the input and output of pseudo random function in TLS?
21. List the alert messages defined in TLS alert protocol ?

Part - B

1. Explain overall operation of HMAC computation used in IPsec ?
2. Explain the documents that describe the set of IPsec protocols.
3. How is AH employed in transport and tunnel mode ?
4. Draw the AH format and explain its fields in details.
5. Draw the ESP format and explain its fields in details.
6. How is ESP employed in transport and tunnel mode ?
7. Draw the ISAKMP header format? Explain.
8. Discuss the five default exchange types of ISAKMP.
9. List and discuss the Payload types and processing of ISAKMP ?
10. Discuss the two defined specification in SSL?
11. Discuss the overall operation of SSL record protocol ?
12. Discuss the overall operation of SSL handshake protocol ?
13. List the steps used to generate master secret key from premaster secret key ?
14. List the steps used to generate cryptographic parameters from master key ?
15. Brief the data expansion function in TLS pseudo random function.