

2015

Time : 3 hours

Full Marks : 80

Candidates are required to give their answers in their own words as far as practicable.

The questions are of equal value.

Answer any five questions in which Q. No. 1 is compulsory.

1. Choose the correct answer of the following :

   (a) Which one of the following computer network is built on the top of another network ?

   (i) Prior network

   (ii) Chief network

   (iii) Prime network

   (iv) Overlay network

   (b) What is Data Encryption Standard (DES) ?

   (i) Block cipher

   (ii) Stream cipher

(iii) Bit cipher

(iv) None of the mentioned

(c) Which one of the following is a cryptographic protocol used to secure HTTP connection ?

(i) Stream Control Transmission Protocol (SCTP)

(ii) Transport Layer Security (TLS)

(iii) Explicit Congestion Notification (ECN)

(iv) Resource Reservation Protocol

(d) These are the features present in IPv4 but not in IPv6 :

(i) Fragmentation

(ii) Header checksum

(iii) Options

(iv) All of the mentioned

(e) DHCP uses UDP port _____ for sending data to the server ?

(i) 66

(ii) 67

(iii) 68

(iv) 69

(f) Which one of the following algorithm is not used in asymmetric-key cryptography ?

(i) RSA algorithm

(ii) Diffie-hellman algorithm

(iii) Electromic code book algorithm

(iv) None of the mentioned

(g) Socket-style API for windows is called :

(i) Wsock

(ii) Winsock

(iii) Wins

(iv) None of the mentioned

(h) Sniffers can be deployed in :

(i) Wired environment

(ii) Wi-Fi

(iii) Ethernet LAN

(iv) All of the mentioned

2. Explain DES and purpose of S-Box in DES in detail.

3. Demonstrate the Euclidean Algorithm with the extended Euclidean Algorithm.

4. What is a message authentication code ? Differentiate between authentication code and one-way hash function.

5. Explain, in detail, about MAC algorithms and its requirement.

6. Demonstrate the Fermat's and Euler's theorems important roles in public key cryptography.

7. Explain IP security with diagram. Describe the benefits and services of IP security.

8. What are the types of Malicious Software ? Describe some worm countermeasures.

9. Illustrate and briefly define the parameters that define an Secure Socket Layer session connection and session state.