CBCS SCHEME

USN | | | | | | | | | | |

18SCS322

Third Semester M.Tech. Degree Examination, Jan./Feb.2021
Information & Network Security

Time: 3 hrs. Max. Marks:100

Note: ***Answer any FIVE full questions, choosing ONE full question from each module.***

Module-1

1 a. Explain polyalphabetic ciphen substitution techniques, with example. **(10 Marks)**

b. Explain in detail, DES encryption and decryption. **(10 Marks)**

OR

2 a. Illustrate Caesar cipher substitution technique for the plain text "Meet me after toga party". **(05 Marks)**

b. Describe the following in detail:
(i) Avalanche effect. (ii) Timing attack.
(iii) Block cipher principles. (iv) Feistel cipher structure. **(10 Marks)**

c. Describe playfair cipher key features and perform encryption and decryption for the plain text "WORLD" with key "SECURE". **(05 Marks)**

Module-2

3 a. Describe RSA algorithm, its computational aspects and security in RSA. **(10 Marks)**

b. What is PRNG based RSA? Explain the Diffie-Hellman key exchange algorithm. **(10 Marks)**

OR

4 a. Perform encryption and decryption using RSA algorithm for:
p = 3, q = 11, e = 7 and M = 5. **(08 Marks)**

b. Explain with example Elgamal cryptosystem. **(12 Marks)**

Module-3

5 a. Give X.509 certificate format with neat diagram. **(10 Marks)**

b. Differentiate briefly Kerbero's version 4 and kerbero's version 5. **(10 Marks)**

OR

6 a. Illustrate different techniques involved in distribution of public keys. **(10 Marks)**

b. Describe in detail Remote user authentication principles. **(10 Marks)**

Module-4

7 a. Explain wireless security threats. **(08 Marks)**

b. Describe IEEE 802.11 wireless LAN overview. **(12 Marks)**

OR

8 a. Explain SSL architecture and SSL record protocol. **(10 Marks)**

b. Describe SSH protocol stack with neat diagram. **(10 Marks)**

Module-5

9 a. Describe S/MIME functionality and S/MIME certificate processing. **(10 Marks)**

b. Explain Encapsulating security format (ESP) format in detail. **(10 Marks)**

OR

10 a. Explain any 2 PGP cryptographic functions. **(10 Marks)**

b. Illustrate IP security policy for:
(i) Security association. (ii) Security association database. **(10 Marks)**

* * * * *