

CBCS Scheme

USN

--	--	--	--	--	--	--	--	--	--

16/17SCS253

Second Semester M.Tech. Degree Examination, June/July 2018 Information and Network Security

Time: 3 hrs.

Max. Marks: 80

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

Module-1

- 1 a. Discuss the simplified model of conventional cryptosystem with neat diagram. (04 Marks)
b. Explain the features of play fair cipher. (04 Marks)
c. Perform the hill cipher encryption and decryption for the plaintext "PAYMOREMONEY"

by using key $K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$. (08 Marks)

OR

- 2 a. Explain the Feistel cipher encryption and decryption with diagram. (08 Marks)
b. Describe the general depiction of DES encryption algorithm with neat diagram. (08 Marks)

Module-2

- 3 a. Discuss the applications and requirements for public key cryptography. (08 Marks)
b. Perform the encryption and decryption using RSA algorithm for the following :
i) $p = 3, q = 11, e = 7, M = 5$
ii) $p = 5, q = 11, e = 3, M = 9$. (08 Marks)

OR

- 4 a. What are Abelian groups? Explain the geometric description of addition in Elliptic curves. (08 Marks)
b. User A and B use the Diffie-Hellman's key exchange technique with a common prime $q = 71$, and primitive root of $\alpha = 7$. Compute the following :
i) If user A has private key $X_A = 5$, compute Y_A
ii) If user B has private key $X_B = 12$, compute Y_B . (08 Marks)

Module-3

- 5 a. Discuss the techniques involved in distribution of public keys. (08 Marks)
b. Give the format of X.509 certificate with neat diagram. (08 Marks)

OR

- 6 a. Differentiate between Kerberos version 4 and 5. (04 Marks)
b. Explain decentralized key control. (04 Marks)
c. With the aid of diagram describe the key distribution scenario. (08 Marks)

Module-4

- 7 a. Give the general IEEE802 MPDU format. (04 Marks)
b. Explain the IEEE 802.11 network components and architectural model. (04 Marks)
c. Describe the IEEE 802.11i phases of operations briefly. (08 Marks)

OR

- 8 a. Explain SSL architecture and SSL record protocol. (08 Marks)
b. Describe the SSH protocol stack with neat diagrams. (08 Marks)

Module-5

- 9 a. Explain any two PGP cryptographic functions. (08 Marks)
b. Describe the IP security applications and benefits with the help of IP security scenario. (08 Marks)

OR

- 10 a. What are the services of PGP? Explain. (04 Marks)
b. Explain the various fields of MIME content types. (04 Marks)
c. Describe the encapsulation security payload (ESP) IP security format with neat diagrams. (08 Marks)

* * * * *