

| | | | | | | | | | | | | | | | | | | | |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| | | | | | | | | | | | | | | | | | | | |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|

Eighth Semester B.E. Degree Examination, Aug./Sept. 2020
Network Security

Time: 3 hrs.

Max. Marks:100

Note: Answer FIVE full questions, selecting atleast TWO questions from each part.

PART – A

- 1 a. What are the five categories of X800 security services and explain it. (11 Marks)
- b. Mention the basic tasks are to be considered while designing a particular security service. (04 Marks)
- c. Write the few examples of security attacks. (05 Marks)
- 2 a. Encrypt the plaintext "FRIDAY" using Hill cipher with the key $\begin{pmatrix} 7 & 8 \\ 19 & 3 \end{pmatrix}$. Show your calculation and also calculate the corresponding decryption of the ciphertext to recover the original plaintext. (10 Marks)
- b. Explain key generation for simplified DES. (06 Marks)
- c. Mention advantages and disadvantages of cipher Feedback mode. (04 Marks)
- 3 a. Perform encryption and decryption using RSA algorithm for $p = 7; q = 11, e = 17; M = 8$. (08 Marks)
- b. Explain Diffie – Hellman key exchange between user A and B using elliptic curves. (08 Marks)
- c. What are the properties of Hash functions? (04 Marks)
- 4 a. What are the properties and requirement for a digital signature? (06 Marks)
- b. Explain the two approach to digital signature standard. (09 Marks)
- c. Describe the common weakness/threat of a Direct Digital Signature Scheme. (05 Marks)

PART – B

- 5 a. Mention the different types of threats, consequences and countermeasures when using web. (08 Marks)
- b. Explain the SSL record protocol operation. (06 Marks)
- c. With the help of the block diagram, explain cardholder sends purchase request operation. (06 Marks)
- 6 a. Write the techniques used for learning passwords. (08 Marks)
- b. Draw the architecture for distributed intrusion detection and explain it. (12 Marks)
- 7 a. Explain the nature of viruses and phases. (08 Marks)
- b. Explain antivirus approach and its four generation. (08 Marks)
- c. What is network worm and mention few examples. (04 Marks)
- 8 a. What are capabilities and limitations of firewall? (10 Marks)
- b. What are the design goals for a firewall and also mention techniques that firewalls used to control access and enforce the sites security policy. (10 Marks)

* * * * *