(Pages : 3) **N – 6667**

Reg. No. : .....

Name : .....

Eighth Semester B.Tech. Degree Examination, May 2022

(2008 Scheme)

08.803 : CRYPTOGRAPHY AND NETWORKS SECURITY(R)

Time : 3 Hours Max. Marks : 100

SECTION – A

Answer **all** questions. **Each** question carries **4** marks.

1. What is the difference between a block cipher and a stream cipher? Give one example of each.
2. Encrypt the sentence cryptographic techniques' using Vignere cipher with key a 'cryptanalysis'.
3. What parameters determine the actual algorithm of a Feistel cipher?
4. What is Euler's totient function ($\varphi(n)$)? Write all numbers which are relatively prime to 15.
5. What is a message authentication code?
6. What is the purpose of the state array?
7. How SSL connection is different from SSL session?
8. What is man in the middle attack of Diffie-Hellman key exchange algorithm?
9. Write any four security requirements of Cryptographic Hash Functions.
10. What are *Enveloped data*, *signed data and clear-signed data* in the context of S/MIME?

(10 × 4 = 40 Marks)

P.T.O.

SECTION – B

Answer **one full** question from each module. Each question carries **20** marks.

Module – I

11. (a) How Monoalphabetic ciphers differ from Polyalphabetic ciphers? Explain with one example from each. **6**

(b) Draw diagrams showing encryption and decryption in Cipher Feedback (CFB) mode of DES. **7**

(c) Describe Mixcolumns operation of AES. **7**

OR

12. (a) What are transposition ciphers. Illustrate with an example. **4**

(b) What are the different primitive operations in IDEA. Explain the encryption process of IDEA. **10**

(c) Explain the operation performed in S Box of DES. **6**

Module – II

13. (a) Explain the different operations by which 128 bit hash value is generated from a message by MD5 algorithm. **10**

(b) Write RSA algorithm. Perform encryption and decryption using the RSA algorithm for $p - 5$; $q = 11$; $e = 3$; $M = 9$. **10**

OR

14. (a) Explain how signing and verification is performed in Digital Signature algorithm. **10**

(b) Explain how a common key is established between communicating parties using Diffie-Hellman Algorithm? **10**

Module – III

15. (a) What steps are involved in SSL Record Protocol transmission? **10**

(b) List the applications of IPSec. What are the benefits of IPSec. **10**

OR

16. (a) What are the firewalls? What are different types of firewall? **10**

(b) Distinguish between transport mode and tunnel mode operation in IP security? **10**

(3 × 20 = 60 Marks)