[Nov-23]

GITAM (Deemed to be University)
[CSEN2071]
GST/GSS/GSB/GSHS Degree Examination

III Semester

CRYPTOGRAPHY AND NETWORK SECURITY

(Effective for the admitted batch 2021-2022)

Time: 2 Hours **Max. Marks: 30**

Instructions: All parts of the unit must be answered in one place only.

SECTION-A

1. **Answer all the questions.** **(5×1=5M)**

   a) What is denial of service attack?

   b) Interpret the working of cipher feedback mode.

   c) Prove a | b and b | a if a=$\pm$b.

   d) Infer about man in middle attack.

   e) What is the difference between a TLS connection and a TLS session?

SECTION-B

Answer the following: **(5×5=25M)**

UNIT-I

2. Let message = “graduate”, Key = “word”, Solve by using Playfair Cipher algorithm.

OR

3. What is Attack? Infer the different types of attacks?

UNIT-II

4. Summarize the structure of AES with diagram and describe the steps involved in encryption process.

OR

5. Briefly explain the design principles of block cipher.

UNIT-III

6. Deduct encryption and decryption using the RSA algorithm, for the following:

   p=3; q=11, e=7; M=5

OR

7. State and prove the division algorithm.

UNIT-IV

8. Elaborate with suitable diagrams the applications of hash function.

OR

9. Discuss the steps used in SHA-512 with a block diagram.

UNIT-V

10. Interpret the steps for preparing an signedData of MIME entity.

OR

11. Outline the rules to be followed by an sending agent for content encryption purpose.