[Apr-24]

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

VI Semester

CYPTOGRAPHY AND NETWORK SECURITY

(Effective from the admitted batch 2021-22)

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

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

Section-A

1. **Answer all questions:** **(5×1=5)**

a) Infer the terms : Symmetric and Asymmetric Cryptography with Example.

b) Analyze the operation performed in the Round Function of DES algorithm.

c) Find GCD ((24140, 16762) using Euclidean Algorithm.

d) Compare Conventional and Digital Signature.

e) Differentiate between SSL and TLS.

Section-B

Answer the following: **(5×5=25)**

UNIT-I

2. Elucidate the different types of Security services?

OR

3. Decrypt the Cipher Text "THTIPPNTOYENCGIRGRRSEYAIS" using the key=456213 with Columnar Transposition Technique

UNIT-II

4. Explain Triple DES by using 2 keys with diagram.

OR

5. Analyze ECB and Counter Mode of Operation with neat diagram.

UNIT-III

6. In a public-key system using RSA, you intercept the cipher text C = 52 sent to a user whose public key is e = 13, n = 143. What is the plaintext M?

OR

7. Elaborate “Man in the Middle Attack” in Diffie Hellman Key Exchange Algorithm.

UNIT-IV

8. What is HMAC function? Summarize the design objectives of HMAC.

OR

9. List the main features of SHA-512 cryptographic hash function and the compression function used.

UNIT-V

10. Write in detail about S/MIME IP Security

OR

11. What is intrusion detection? Explain intrusion detection techniques in detail.