[Nov-23]

GITAM (Deemed to be University)
[CSEN2071]
GST/GSS/GSB/GSHS Degree Examination
V 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 Questions: **(5×1=5)**

a) “Passive attacks are very difficult to detect”- Justify this statement.

b) Demonstrate the working of S-box.

c) Find the gcd(12378, 3054).

d) What are the attacks related to message communication?

e) Define TLS session and TLS connection

Section-B

Answer the following: **(5×5=25)**

UNIT-I

2. Evaluate encryption and decryption process in hill cipher. Consider message = “shar” and key = “hill”.

OR

3. What is monoalphabetic cipher? Examine how it differs from caesar cipher.

UNIT-II

4. Distinguish between public key and conventional encryption.

OR

5. Discuss output feedback mode and cipher block chaining mode with respective equations.

UNIT-III

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

   p=5; q=11, e=3; M=9

OR

7. User A and B exchange the key using Diffie-Hellman algorithm. Assume α=5 q=11 X_A=2 X_B=3. Find the value of Y_A, Y_B and secret key.

UNIT-IV

8. Elaborate the working of each round in SHA-512 followed by set of equations

OR

9. How to verify message authentication and confidentiality by making use of MAC

UNIT-V

10. Summarize the initial connection establishment between client and server by using handshake protocol.

OR

11. Infer various TLS attacks in detail.