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

V Semester

CRYPTOGRAPHY AND NETWORK SECURITY
(Effective for 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=05)

   a) Outline the various objectives of computer security.

   b) Differentiate between stream and block cipher

   c) Find Residues of 6 when n = 8

   d) What are the primary requirements of the digital signature? Explain

   e) List S/MIME Message Content Types

Section-B

Answer the following: (5×5=25)

UNIT-I

2. Solve by using Playfair cipher algorithm. The message   CO1 PO2 L6 'MY BALLOON' using the key 'MONACHRY'.

OR

3. Illustrate the various security mechanisms.

UNIT-II

4. Summarize the functionality of single round of DES with a neat diagram and number of bits in each flow of data.

<div align="center">**OR**</div>

5.   How can the same key be reused in triple DES? Illustrate.

<div align="center">**UNIT-III**</div>

6.   Find an integer that has a remainder of 3 when divided by 7 and 13, but is divisible by 12.

<div align="center">**OR**</div>

7.   Elaborate diffie hellman key exchange algorithm with example.

<div align="center">**UNIT-IV**</div>

8.   Infer about the various elements of X.509 Certificate.

<div align="center">**OR**</div>

9.   Explain the techniques used for distribution of keys.

<div align="center">**UNIT-V**</div>

10.   Summarize the four message related services that S/MIME provides.

<div align="center">**OR**</div>

11.   Interpret the steps for preparing an enveloped Data of MIME entity.

<div align="right">[VS/123]</div>