SANSKRITI UNIVERSITY	**SANSKRITI UNIVERSITY** Mathura, Uttar Pradesh	**Enrol. No:**

Semester End Examination - January 2022
Course Code : CSE 403 Course Name : Cryptography & Network Security
School of Engineering & Information Technology
Programme: B.Tech (CSE)(Regular & Lateral) **Semester: VII**

Time: 3 hrs **Max. Marks 100**

PART – A (10 questions X 2 marks = 20 Marks)
Answer ALL the Questions

1. Attempts all parts. All parts carry equal marks. Write answer of each part in short.

a. Define the term Intruder. **[2]**
b. Define Active Attack. **[2]**
c. Explain Passive Attack in short. **[2]**
d. Give the full form of S/MIME and PGP. **[2]**
e. What is key size in DES algorithm? **[2]**
f. Explain the functionality of key generator. **[2]**
g. Define Private key. **[2]**
h. Define Public key. **[2]**
i. Explain Virus in short. **[2]**
j. Write the full form of AH and ESP. **[2]**

PART – B (4 questions X 5 marks = 20 Marks)
(Answer all questions)

2. Explain TLS in brief. **[5]**
3. Explain in Groups and Prime Numbers in brief. **[5]**
4. Explain the Feistel structure in detail. **[5]**
5. Explain Conventional encryption model in detail. **[5]**

PART – C (3 questions X 10 marks = 30 Marks)
Answer Three out of Four Questions

6. Explain Chinese Remainder Theorem in detail. **[10]**
7. Discuss Euclid's algorithm in detail. **[10]**
8.(a) Explain SHA algorithm in detail. **[10]**
(b) For the keyword MONARCHY and message =JAZZ .Solve it by Play fair cipher.
9.(a) Explain EL Gamal encryption. **[10]**
(b) What is the purpose of X. 509 Standard?

PART – D (2 questions X 15 marks = 30 Marks)
Answer Two out of Three Questions

10. Discuss Active Attack and Passive Attack in detail along with its types. **[15]**
11. Explain Shannon's theory of Confusion and Diffusion in detail. **[15]**
12.(a) Discuss on Stream ciphers and Block ciphers. **[15]**
(b) Explain SSL security in detail.