SP-242

Seat No.	

Total No. of Pages : 2

T.Y. B.Tech. (Computer Science and Engineering (AIML) (Semester - V) (CBCS) Examination, December - 2023

INFORMATION SECURITY (OE-1)

Sub. Code : 92007

9917

Day and Date : Friday, 08 - 12 - 2023 **Total Marks : 70**

Time : 10.30 a.m. to 01.00 p.m.

Instructions :
1) **Question no. 6 is compulsory.**
2) **Solve any four questions from Q. No. 1 to Q. No. 5.**
3) **Assume suitable data wherever necessary.**
4) **Figures to the right indicate full marks.**

Q1) a) Explain Secure Electronic Transaction. **[8]**

b) What are the three pillars of cryptography? **[7]**

9917

Q2) a) Write RSA algorithm. **[8]**

b) What is Diffie-Hellman Key Exchange algorithm? **[7]**

Q3) a) Explain Secure Electronic Transaction. Using Playfair cipher encrypt the plaintext "instruments" using 'MONARCY' keyword **[8]**

b) What is IP Security Architecture? **[7]**

9917

Q4) a) How we achieve authentication, confidentiality and Confidentiality and authentication using PGP. **[8]**

b) Explain Digital signature authentication mechanism also explain two approaches. **[7]**

P.T.O.

Q5) a) Explain Password management scheme. **[8]**

b) Write the difference between transport and tunnel mode. **[7]**

Q6) Write a short note on (Any 2) : **[10]**

a) Transposition Techniques

b) Pretty Good Privacy

c) Kerberos

▽▽▽▽

9917

9917

9917