



**B.Tech VII Semester Regular/Supplementary Examinations, November 2022**

**INFORMATION SECURITY**  
**(Professional Elective)**  
(Information Technology)

**Maximum Marks: 70**

Date:05.12.2022 Duration: 3 hours

- Note: 1. This question paper contains two parts A and B.  
2. Part A is compulsory which carries 20 marks. Answer all questions in Part A.  
3. Part B consists of 5 Units. Answer any one full question from each unit which carries 10M.  
4. Each question carries 10 marks and may have a, b, c, d as sub questions.

**Part-A**

All the following questions carry equal marks

(10x2M=20 Marks)

- 1 What is symmetric key cryptography.
- 2 Why is asymmetric cryptography bad for huge data? Specify the reason.
- 3 What is digital signature?
- 4 What is Meet in the Middle attack?
- 5 List the properties (requirements) of a hash function.
- 6 How digital signature is different from conventional?
- 7 List out the Encapsulating Security Payload (ESP) packet fields.
- 8 Differentiate Transport and Tunnel mode in IPsec.
- 9 Define Intruder. Name the three different classes of intruder.
- 10 What is worm? Give few examples.

**Part-B**

Answer All the following questions.

(5X10M=50Marks)

- 11 Apply the following substitution techniques: [10M]
- (i) Caesar Cipher: plain text: "hello how are you" ( shift 4 )
  - (ii) Playfair Cipher: plain text: "instruments"
  - (iii) One Time Pad Cipher: Plain text: todayholiday" Key: NCBTUQMOFHAI.

OR

- 12 Explain the different types of attacks and security mechanism. [10M]
- 13 Explain working principles of DES encryption and decryption in detail. [10M]

OR

- 14 Solve: Why ECC is better than RSA? However, why it is not used wisely used? Defend it. [10M]

- 15 What is hash function. Explain the HMAC in detail. [10M]

OR

- 16 Solve: Suggest and explain about an authentication scheme for mutual authentication between the user and the server which relies on symmetric encryption. [10M]
- 17 Explain in detail about PGP and S/MIME. [10M]
- OR
- 18 Explain the architecture of IP Security in detail. [10M]
- 19 Demonstrate any two advanced anti-virus techniques in detail. [10M]
- OR
- 20 Illustrate how does screened host architecture for firewalls differ from screened subnet firewall architecture? Which offers more security for information assets on trusted network? Explain with neat sketch. [10M]