

Paper Id: 113711

Roll No:

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

**B. TECH.**  
**(SEM VII) THEORY EXAMINATION 2019-20**  
**CRYPTOGRAPHY & NETWORK SECURITY**

Time: 3 Hours

Total Marks: 100

**Note:** Attempt all Sections. If require any missing data; then choose suitably.**SECTION A**

- 1. Attempt all questions in brief. 2 x 10 = 20**
- Define cipher text with the help of an example.
  - Categorize Passive and Active attack.
  - State Fermat's theorem.
  - Write any two applications of RSA algorithm.
  - What type of security goals are used in cryptography?
  - Explain briefly two approaches of Digital Signature.
  - List any two applications of X.509 Certificates.
  - Write a simple Authentication dialogue used in Kerberos.
  - Define S/MIME.
  - What are the protocols used to provide IP security?

**SECTION B**

- 2. Attempt any three of the following: 10x3=30**
- Draw the block diagram of DES encryption. Also Explain strength of DES in brief.
  - What are the securities of RSA? Perform encryption and decryption using RSA algorithm for  $p = 17, q = 11, e = 7, m = 88$
  - Explain SHA-512 algorithm with a neat diagram.
  - Give the structure of PGP message generation. Explain with a diagram.
  - Write short notes on any two of the following:  
 (i) Secure Socket Layer, (ii) Modes of IP Sec, (iii) Intrusion Detection.

**SECTION C**

- 3. Attempt any one part of the following: 10x1=10**
- Differentiate between following:  
 (i) Block cipher and Stream Cipher  
 (ii) Steganography and Cryptography  
 (iii) Authentication and Authorization
  - Explain Shannon's theory of confusion and diffusion in terms of information security.
- 4. Attempt any one part of the following: 10x1=10**
- Illustrate the concept of Chinese remainder theorem. By using Chinese Remainder Theorem solve the simultaneous congruence  $X \equiv 2 \pmod{P}$  for all  $P \in \{3, 5, 7\}$
  - What is the application of public key cryptosystems? Discuss the applications for public key cryptosystems.
- 5. Attempt any one part of the following: 10x1=10**
- Describe signing and verification in Digital Signature Algorithm.
  - What are the requirements of a Message Authentication code (MAC)? Discuss the logical structure, components and algorithmic steps of MD5 algorithm.
- 6. Attempt any one part of the following: 10x1=10**
- Explain Diffie-Helman key exchange technique with an example.
  - What is Kerberos? Discuss the principle differences between version 4 and version 5 of Kerberos.
- 7. Attempt any one part of the following: 10x1=10**
- List the participants in SET (Secure Electronic Transaction) system? Describe in brief the sequence of events that are required for a transaction.
  - What are different types of firewall? Also discuss viruses and related threats to system security