**Code No: 127DY** **R15**

**JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD**
**B. Tech IV Year I Semester Examinations, May/June - 2019**
**INFORMATION SECURITY**
**(Information Technology)**

**Time: 3 Hours** **Max. Marks: 75**

**Note:** This question paper contains two parts A and B.
Part A is compulsory which carries 25 marks. Answer all questions in Part A. Part B consists of 5 Units. Answer any one full question from each unit. Each question carries 10 marks and may have a, b, c as sub questions.

**PART- A**

**(25 Marks)**

| | | |
|---|---|---|
| 1.a) | Define steganography. | [2] |
| b) | Differentiate between transposition chipper and substitution chipper? | [3] |
| c) | Define linear crypt analysis? | [2] |
| d) | Define the principle elements of a public key cryptosystem. | [3] |
| e) | Give the requirements for message authentication? | [2] |
| f) | Evaluate what are the security services provided by digital signature. | [3] |
| g) | Give the applications of IPSecurity. | [2] |
| h) | Examine whether ESP includes a padding field. | [3] |
| i) | List three classes of intruder. | [2] |
| j) | Discuss about password management. | [3] |

**PART-B**

**(50 Marks)**

2. Apply Vigenere cipher; encrypt the word “explanation” using the key “leg”. [10]

**OR**

3. Explain in detail about various security mechanisms. [10]

4. Evaluate using Diffie-Hellman key exchange technique. Users A and B use a common prime q=11 and a primitive root alpha=7 (a) If user A has private key XA=3.What is A’s public key YA? (b) If user B has private key XB=6.What is B’s public key YB? (c) What is the shared secret key? [10]

**OR**

5. Explain the various types of block chipper design principles. [10]

6. Explain the process of deriving eighty 64-bitwords from1024 bits for processing of a single blocks and also discus single round function in SHA-512 algorithm. Show the values of W16, W17, W18 andW19. [10]

**OR**

7. Compare and generalize the features of SHA and MD5 algorithm. Formulate the objectives of HMAC candidate security features. [10]

8. Describe about the architecture of IP security. [10]

**OR**

9. Analyze the Cryptographic algorithms used in S/MIME and Explain S/MIME certification processing. [10]

10.a) Explain the design principles of firewall.
b) Explain about secure electronic transaction. [5+5]

**OR**

11. List the different protocols of SSL. Explain in detail Handshake protocol. [10]

**--ooOoo--**