Roll No. .....

Total Page No. : 3

51N2305 /

51N2305 /

B.TECH. V SEMESTER (NEW SCHEME)
MAIN/BACK EXAMINATION 2024-25
COMPUTER SCIENCE & ENGINEERING
(CYBER SECURITY)

(5CY4-05) - Cryptography and Information Security

Time : 3 Hours] **[Max. Marks :** 70

[Min. Passing Marks :

Instructions to Candidates :

Part-A : Short Answer Type Questions (up to 25 words) 10 × 2 = 20 marks. All 10 questions are compulsory.

Part-B : Analytical/Problem Solving questions 5 × 4 = 20 marks. Candidates have to answer 5 questions out of 7.

Part-C : Descriptive/Analytical/Problem Solving questions 3 × 10 marks = 30 marks. Candidates have to answer 3 questions out of 5.

Schematic diagrams must be shown wherever necessary. Any data you feel missing may suitably be assumed and stated clearly. Units of quantities used/ calculated must be stated clearly.

Use of the following supporting materials is permitted during examination. (Mentioned in form no. 205).

1_____

Part-A

1. Explain plain text and cipher text.
2. What are transposition techniques ?
3. Explain the purpose of S-Boxes in DES ?
4. Is Diffie-Hellman key exchange protocol is vulnerable ? Explain ?
5. What are the properties of digital signature ?
6. What is HMAC ?
7. What is IEEE802.11 standard ?
8. What is wireless security ?
9. What is the purpose of S/MIME ?
10. What is internet key exchange ?

Part-B

1. 'Passive attacks are very difficult to detect' Justify this statement.
2. Explain the design principles of block cipher technique ?
3. What is the problem that Kerberos addresses ?
4. Write the four SSL protocols.
5. What are the services provided by IP Security ?
6. What is meant by one-way property in hash function ?
7. Difference between Substitution Cipher technique and Transposition Cipher technique.

Part-C

1. Differentiate between passive attacks and active attacks.

2. Which four tasks are performed in each round of AES Cipher ? Explain.

3. Perform decryption and encryption using RSA algorithm with p=3, q=11, e=7 and N=5.

4. Give the structure of HMAC. Explain the applications of HMAC.

5. Explain IP Security protocols in detail.

****