20PCSET3CN3

SHRIMATHI DEVKUNVAR NANALAL BHATT VAISHNAV COLLEGE FOR WOMEN
(AUTONOMOUS)
(Affiliated to the University of Madras and Re-accredited with 'A+' Grade by NAAC)
Chromepet, Chennai - 600 044.
M.Sc. Comp Sci - END SEMESTER EXAMINATIONS APRIL - 2024
SEMESTER - III

20PCSET3CN3 - Cryptography and Network Security

Total Duration : 2 Hrs. 30 Mins. Total Marks : 60

Section B

Answer any **SIX** questions $(6 \times 5 = 30$ Marks)

1. Illustrate Transposition cipher techniques.
2. Sketch and explain Public-key cryptosystems.
3. What are the requirements for a hash function?
4. Explain the overview of Kerberos.
5. Sketch and explain DES algorithm.
6. Consider an RSA cryptosystem with p = 17, q = 13, and e = 35. What is the value of d and n?
   • Let (e, n) be the public key of Alice. If we use it to encrypt a message m = 78, what is the ciphertext C?
   • Let (d, n) be the private key of Alice. If she receives a ciphertext C = 65, what is the original message m?
   • If you receive a message m = 93 from Alice and her digital signature 188, do you think that this message indeed comes from her?
7. Explain the necessity of Authentication requirements in the context of communication across a network.
8. Examine he concept of Electronic Mail Security.

Section C

I - Answer any **TWO** questions $(2 \times 10 = 20$ Marks)

9. Explain the following
   a) Active attacks b) Passive attacks
10. How do you apply AES cipher to do encryption and decryption? Explain.
11. Distinguish between RSA and Diffie-Hellman algorithm.
12. Examine the requirements of Digital signatures.

II - Compulsory question $(1 \times 10 = 10$ Marks)

13. Examine the IP security architecture, benefits, and its applications.

******