15623

Reg. No. | | | | | | | | |

VI Semester B.CA. Degree Examination, September - 2021

COMPUTER SCIENCE

Cryptography and Network Security

(CBCS Scheme)

Time : 3 Hours **Maximum Marks : 100**

Instructions to Candidates:

Answer all sections.

SECTION - A

Answer any **10**. Each carries **2** marks. **(10×2=20)**

1. What is Cryptography?
2. Write any two differences between Symmetric and Asymmetric key system.
3. What are the properties of Divisibility.
4. Write the difference between Equality and congruence.
5. Use affine Cipher to encrypt the message "Cryptography" with key pair (7,2).
6. What do you mean by message padding?
7. Explain Trapdoor one way function.
8. List the properties of cryptographic Hash function.
9. What are the problems of symmetric key distribution.
10. Write the functions of Public Key Infrastructure (PKI).
11. Define the terms Session and session state.
12. What are the two modes of operation in IPSec?

SECTION - B

Answer any **5** each carries **5** marks. **(5×5=25)**

13. Explain the goals of cryptography.
14. With an example explain Extended Euclidean algorithm.

[P.T.O.

15. Write the difference between stream and Block Cipher.

16. Write any 5 comparisons between AES and DES.

17. Write a note on RC4 stream Cipher.

18. Explain the Knapsack cryptosystem algorithm.

19. Write the differences between conventional and Digital Signature.

20. Compare SSL and TLS.

SECTION - C

Answer any **3** each carries **15** marks. **(3×15=45)**

21. a. Explain DES Algorithm. **(10)**
    b. Write a note on play fair Cipher. **(5)**
22. a. Explain the Encryption and Decryption process in 3DES. With a neat diagram. **(8)**
    b. With a neat diagram explain the AES encryption for a single round. **(7)**
23. a. Explain the different modes of operation for modern block cipher. **(10)**
    b. Write a note on Fermat's little theorem. **(5)**
24. a. Explain in detail encryption, decryption and key generation in RSA cryptosystem. **(10)**
    b. Explain SHA - 512 function **(5)**
25. a. Explain Diffie - Hellman Key agreement. **(7)**
    b. Explain the modes of IPSec In detail. **(8)**

SECTION - D

Answer any **one.** Each carries **10** marks. **(1×10=10)**

26. Explain security mechanisms in detail? **(10)**
27. With an example, explain the chinese Remainder theorem. **(10)**
