SG – 633

20

VI Semester B.C.A. Examination, September/October 2021
(2016-17 and Onwards) (CBCS Scheme) (F + R)
COMPUTER SCIENCE
BCA – 603 : Cryptography and Network Security

Time : 3 Hours Max. Marks : 100

***Instruction** : Answer **all** the Sections.*

SECTION – A

Answer **any ten** questions. **Each** question carries **two** marks : **(10×2=20)**

1. Define Network Security.

2. What is ciphertext ?

3. State the major difference between symmetric and asymmetric key.

4. What is block cipher ?

5. List any two Hashing algorithms.

6. What is Public Key Infrastructure (PKI) ?

7. What is data integrity ?

8. What is S/MIME ?

9. What are the protocols used in SSL ?

10. Define Man-in-the-Middle attack.

11. What is pay load ?

12. What are the two modes of operation in IPSec ?

SECTION – B

Answer **any five** questions. **Each** question carries **five** marks : **(5×5=25)**

13. Explain the various security mechanisms.

14. Differentiate active and passive attacks. Give examples.

P.T.O.

15. Explain Euclidean algorithm to find GCD.

16. Use additive cipher with key = 10 to encrypt the message "SUCCESS".

17. Explain ECB encryption mode of operation.

18. Explain the digital signature process.

19. What is key distribution center ? State its types.

20. Write a note on Secure Socket Layer.

SECTION – C

Answer **any three** questions. **Each** carries **fifteen** marks : **(3×15=45)**

21. a) Write a note on the attacks that threaten various security goals. **8**

    b) How do you find the inverse of a matrix ? Explain with an example. **7**

22. a) Explain the general structure of DES with a neat diagram. **10**

    b) Compare AES and DES. **5**

23. a) State and explain Chinese Remainder theorem with an example. **10**

    b) Describe security of RSA system. **5**

24. a) Write a note on secure Hash Function SHA 512. **8**

    b) Explain the X.509 certificate structure. **7**

25. a) Explain the security policy database. **8**

    b) Write a note on watermarking. **7**

SECTION – D

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

26. Explain in detail the round function of AES. **10**

27. Write a note on :

    a) S-MIME. **5**

    b) Brute-force attack. **5**
