UG – 422

25

VI Semester B.C.A. Examination, September/October 2022
(CBCS) (F + R) (2016 – 17 and Onwards)
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. Name any two active attacks.
2. Define monoalphabetic cipher.
3. Define block cipher.
4. Differentiate steganography and water marking.
5. What is Avalanche effect ?
6. What is residue class ?
7. Define trapdoor one-way function.
8. Write any two attacks on RSA.
9. What is Kerberos ?
10. Define S/MIME.
11. What is blind signature ?
12. List two protocols which provide security for emails.

SECTION – B

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

13. Explain various security mechanisms. **5**
14. Explain play fair cipher with an example. **5**
15. What is cryptographic hash function ? Explain its properties. **5**

P.T.O.

16. Write a note on steganography. **5**

17. Compare AES and DES. **5**

18. Explain Fermat's little theorem. **5**

19. What is PKI ? What are main duties of PKI ? **5**

20. Explain the two modes of operation in IPSec. **5**

SECTION – C

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

21. a) Explain any three types of cryptoanalytic attacks. **8**

    b) Explain extended Euclidean algorithm with an example. **7**

22. a) Explain the four stages of AES algorithm. **8**

    b) Explain multiple DES. **7**

23. a) Explain any two probabilistic algorithms for primality testing. **8**

    b) State and explain Chinese Remainder theorem with an example. **7**

24. a) Explain Whirlpool Cipher. **8**

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

25. a) Explain the protocols in SSL. **8**

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

SECTION – D

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

26. Explain RSA cryptosystem. **10**

27. Explain security policy inbound and outbound processing. **10**
