SE – 346

VI Semester B.C.A. Examination, September 2020
(CBCS – F+R Scheme)
(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. **(10×2=20)**

1. Define cryptography.
2. Define Hashing.
3. What is data integrity ?
4. What is Affine cipher ?
5. What is Brute force attack ?
6. Define Residue class.
7. What is co-prime ? Give example.
8. What is trapdoor one-way function ?
9. What is Kerberos ?
10. What is message padding ?
11. Define digital signature.
12. Define Hijacking.

SECTION – B

Answer **any five** questions. **(5×5=25)**

13. Discuss the classification of security goals.
14. Find GCD(2740, 1760) using Euclidean algorithm.

15. Write a neat diagram and explain the general structure of DES.

16. Explain transpositional cipher with an example.

17. Explain CBC mode of operation.

18. Explain Fermat's little theorem.

19. Briefly explain the architecture of SSL.

20. Explain the practical applications of watermarking.

SECTION – C

Answer **any three** questions. **Each** question carries **15** marks.

21. a) Explain the types of cryptanalysis attacks. **(8+7)**
    b) List four properties of divisibility.

22. a) Draw the block diagram of DES algorithm. Explain briefly. **(8+7)**
    b) Write a short note on multiple DES.

23. a) Explain the rules of play fair cipher with an example. **(8+7)**
    b) Differentiate between symmetric and asymmetric key cryptography.

24. a) State and explain Chinese remainder theorem with an example. **(8+7)**
    b) Discuss different attacks on RSA.

25. a) Explain Public Key Infrastructure (RKI) in detail. **(8+7)**
    b) Differentiate between MIME and S/MIME.

SECTION – D

Answer **any one** question. **(1×10=10)**

26. Discuss in detail block cipher modes of operations.

27. Explain SHA-512 algorithm with a neat diagram.
