SM – 625

VI Semester B.C.A. Examination, May/June 2018
(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. What is cryptosystem ?
2. Define Hashing.
3. What are the basic properties of divisibility ?
4. Define cipher text with an example.
5. What is Brute Force attack ?
6. Write any two applications of RSA algorithm.
7. Define Encryption and Decryption.
8. What is Trapdoor one-way function ?
9. Explain Avalanche Effect.
10. What is message padding ?
11. Define digital signature.
12. What are the protocols used to provide IP security ?

SECTION – B

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

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

P.T.O.

15. Differentiate between block cipher and a stream cipher.

16. Explain caesar cipher with an example.

17. Explain Fermat's little theorem.

18. What is primality test ? Explain in brief.

19. Explain cipher Feedback Mode.

20. Explain the practical applications of watermarking.

SECTION – C

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

21. a) Explain in detail the taxonomy of attacks with relation to security goals. **10**

    b) Discuss Extended Euclidean Algorithm. **5**

22. a) Explain steps in DES Algorithm. **10**

    b) Discuss any two modes of operations in DES. **5**

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

    b) Discuss different attacks on RSA. **5**

24. a) Explain digital signature process with its security mechanism. **10**

    b) Write a note on Kerberos. **5**

25. a) Explain Public Key Infrastructure (PKI) in detail. **10**

    b) Differenciate between MIME and S/MIME. **5**

SECTION – D

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

26. Explain Diffie-Helman key exchange technique with an example. **10**

27. a) Explain SSL Handshake protocol action. **5**

    b) Write a note on PGP services. **5**

____