**VI Semester B.C.A. Examination, May 2017**
**(CBCS) (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 information security ?

2. What is data integrity ?

3. Who is cryptanalyst ?

4. Define symmetric key cryptography.

5. What is FIPS ?

6. What is permutation process in cryptography ?

7. What is co-prime ? Give examples.

8. What is integer factorization ?

9. Define stream cipher.

10. What is payload ?

11. What is a session ?

12. What is IPSec ?

## SECTION – B

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

13. Explain symmetric key encryption model with a neat diagram.

14. Explain various security mechanisms.

15. Explain Euclid's algorithm with example.

16. Explain transpositional Cipher with an example.

**P.T.O.**

17. Explain CBC mode of operation.

18. Explain digital signature process with a neat diagram.

19. Explain PGP services.

20. Compare SSL and TLS protocols.

## SECTION – C

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

21. a) Explain key elements of public key encryption.                    8
    b) Differentiate equality and congruence with examples.              7

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

23. a) Explain Fermat's theorem of primality test.                       7
    b) Explain RSA algorithm with one example.                           8

24. a) Write a short note on Whirlpool hash function.                    7
    b) Explain Diffie-Helman key agreement.                              8

25. a) Write a short note on IKE.                                        7
    b) Explain the modes of IPSec.                                       8

## SECTION – D

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

26. Explain one round of processing in AES.

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

————————————