Sl. No. 100005

No. of Printed Pages : **2**

GS-757

VI Semester B. VOC Examination, May/June - 2019

INFORMATION TECHNOLOGY

603 : Cryptography and Network Security

(CBCS) (Fresh) (2018-19 & Onwards)

Time : 3 Hours Max. Marks : 100

Instructions to Candidates : *Answer* ***all*** *the sections.*

SECTION - A

Answer **any ten** questions. Each question carries **two** marks. **10x2=20**

1. What is the need of network security ?
2. Define confidentiality and authentication with an example.
3. Define encryption and decryption.
4. What is asymmetric key cryptography ?
5. What is co-prime ? Give examples.
6. Find GCD (12, 60).
7. Define cryptographic hash function.
8. List the security services provided by a digital signature.
9. What is cardinality of prime ?
10. What is Hijacking ? State its purpose.
11. What is S/MIME ?
12. What is E-Commerce Security ?

P.T.O.

SECTION - B

Answer **any five** Questions. Each Question carries **ten** marks. **5x10=50**

13. (a) Explain the techniques of security goals in detail.
(b) Explain Extended Euclidean Algorithm.

14. (a) Explain the Feistel structure with a neat diagram.
(b) Explain playfair cipher with an example.

15. (a) Explain Electronic codebook mode (ECB).
(b) List the duties of KDC.

16. (a) What are the five principle services provided by PGP ?
(b) Write a note on steganography.

17. (a) Explain Round function of DES Algorithm.
(b) Explain different types of attacks on encrypted messages.

18. (a) What is the difference between block ciphers and stream cipher ?
(b) Explain RSA algorithm with an example.

19. (a) Explain the various process of factorization.
(b) Write a short note on :
(i) Trusted centre
(ii) Certification authority
(iii) Controlled trusted centre.

20. (a) Explain whirlpool cipher.
(b) Write a note on digital signature.

- o 0 o -