106132

No. of Printed Pages : **2**

# GS-644

VI Semester B.C.A. Examination, May/June - 2019

## COMPUTER SCIENCE

## BCA 603 : CRYPTOGRAPHY AND NETWORK SECURITY

(CBCS) (F+R)(2016-17 & Onwards)

Time : 3 Hours | Max. Marks : 100

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

### SECTION - A

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

**1.** Define Cryptography.

**2.** Distinguish between active and passive attacks.

**3.** Define Integrity and Non-repudiation.

**4.** Find the GCD of 16 and 48.

**5.** Define Padding in block cipher.

**6.** Define Resedue class.

**7.** Estimate the block size of MD5.

**8.** Define S/MIME.

**9.** What is Kerberos ?

**10.** Define the Diffie - Hellman protocol.

**11.** List any 2 applications of X.509 certificate.

**12.** Define Hijacking.

### SECTION - B

Answer **any five** questions. Each question carries **five** marks. **5x5=25**

**13.** Compare steganography and watermarking. 5

**14.** State and explain the principles of public key cryptography. 5

**15.** With a neat diagram explain the general structure of DES. 5

**P.T.O.**

16. Explain Transposition cipher with an example. 5

17. State the important properties of public key encryption scheme. 5

18. Why SHA more secure than MD5 ? 5

19. Briefly explain the architecture of SSL. 5

20. Explain Tunnel mode of IPSec. 5

## SECTION - C

Answer **any three** questions. Each question carries **fifteen** marks. **3x15=45**

21. (a) Briefly explain the model of conventional cryptosystem. 8

(b) Find det.A if $A = \begin{bmatrix} 9 & 0 & -2 \\ -3 & -5 & 2 \\ 2 & 0 & 6 \end{bmatrix}$ 7

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

(b) Explain the rules of play fair cipher with an example. 7

23. (a) Explain the procedure for RSA cryptosystem. 10

(b) Differentiate between Symmetric and Asymmetric key Cryptography. 5

24. (a) Explain the working of Digital Signature with a neat diagram. 8

(b) How does PGP provide confidentiality and authentication service for e-mail ? Explain. 7

25. (a) List and explain the four protocols of SSL. 8

(b) Explain X.509 certificate. 7

## SECTION - D

Answer **any one** question. Each question carries **ten** marks. **1x10=10**

26. Discuss in detail block cipher modes of operations. 10

27. List and explain the properties of Hash functions. 10

- o 0 o -