Total No. of Questions : 8] *[Total No. of Printed Pages : 2*

Roll No ....

CS-703(A)-CBGS

B.Tech., VII Semester

Examination, December 2020

Choice Based Grading System (CBGS)

Cryptography and Information Security

Time : Three Hours

Maximum Marks : 70

Note: i) Attempt any five questions.

ii) All questions carry equal marks.

1. a) Explain the concept of Cryptanalysis and Brute force attack. 7

b) Explain Fermat's little theorem with an example. 7

2. a) Explain RC4 cipher with the help of suitable example. 7

b) Define encryption and decryption in RSA algorithm using suitable example and how to determine the strength of RSA algorithm. 7

3. a) Explain the compression of Secure Hash Algorithm. 7

b) Explain Chinese Remainder Theorem. Using CRT find 'X' from the equations. 7

$$X \cong 7 \bmod 13 \quad \text{and} \quad X \cong 11 \bmod 12$$

4. a) Describe the steps in finding the message digest using SHA-512 algorithm. What is the order of finding two messages having the same message digest? 7

b) Define the generation and verification of the digital signature using Digital Signature standard algorithm. 7

5. a) Explain about SSL Handshake protocol. 7

   b) What are the different servers used in Kerberos? Explain the role of each one. 7

6. a) Explain about IPSec architecture and security association. 7

   b) Define elliptic curves and explain their application in cryptography. 7

7. a) Discuss the design of Firewall. What is its use? 7

   b) Discuss various spoofing and foot printing tools. 7

8. Write short notes: 14

   i) Steganography

   ii) UDP Flood

   iii) Lan Scanner Tools

******