Roll No .....

IT-8001 (CBGS)

B.E. VIII Semester

Examination, May 2019

Choice Based Grading System (CBGS)

Information Security

Time : Three Hours *Maximum Marks : 70*

Note: i) Attempt any five questions.
ii) All questions carry equal marks.

1. a) List and briefly define types of cryptanalytic attacks based on what is known to the attacker?
   b) Briefly define the playfair cipher with tacking a suitable example?

2. Encrypt the message "meet at the airport" using the Hill cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. Show your calculation and the result.

3. a) What is the primitive root of a number?
   b) What are the three broad categories of applications of public key-cryptosystems?

4. Perform the encryption and decryption using RSA algorithm
   i) $p = 3;\ q = 11;\ e = 7;\ m = 5$
   ii) $p = 11;\ q = 13;\ e = 17;\ m = 8$

5. a) Explain the concept of Kerberos? How is it useful?
   b) Explain the internet key exchange protocol.

6. Explain the phishing and format string attack. Explain with tacking suitable example.

7. a) What is penetration testing?
   b) What is firewall and its types?

8. Write a short notes (any three)
   i) Intrusion detection system
   ii) Email security
   iii) Socket secure layer
   iv) Web security and cookies

******