**Code: 9A05709**

B.Tech III Year II Semester (R09) Supplementary Examinations December/January 2015/2016
**INFORMATION SECURITY**
(Information Technology)

Time: 3 hours                                                                Max Marks: 70

Answer any FIVE questions
All questions carry equal marks
*****

1  (a)  Briefly describe data vulnerabilities.
   (b)  Illustrate Columnar transposition cipher with an example.

2  (a)  What are the sources of viruses?
   (b)  How to identify potential covert channels? Explain.

3  (a)  Explain Diffie-Hellman key exchange algorithm with an example.
   (b)  What are the roles of public and private keys?

4  (a)  Describe various examples of replay attacks.
   (b)  Mention the difference between direct and arbitrated digital signatures.
   (c)  Why sequence numbers are not generally used for authentication and key exchange?

5  What is Kerberos? Explain how it provides authenticated service.

6  Discuss the advantages and disadvantages of Diffie-Hellman key exchange protocol? What is the specific key exchange algorithm mandated for use in the initial version of ISAKMP

7  Explain in detail about SSL record protocol operation.

8  (a)  List the characteristics of a good firewall implementation.
   (b)  Explain in detail the two broad categories of statistical anomaly detection

*****