Code No.: 9A05709/R09

III B.Tech. II Semester Regular and Supplementary Examinations Set-2

April/May - 2013

INFORMATION SECURITY

(Information Technology)

Time: 3 Hours Max. Marks: 70

*Answer any **FIVE** Questions*

*All Questions carry **equal** marks*

- - -

1. Discuss in detail the substitution ciphers and the transposition ciphers.

2. Write notes on the following,
   (a) Code red worm
   (b) Trapdoors
   (c) Salami attacks.

3. Explain different crypto algorithms where public-key cryptosystems are used.

4. (a) What is digital signature? Explain the benefits of digital signatures.
   (b) Explain the approaches for dealing with replay attacks.

5. (a) What are the functions included in MIME in order to enhance security how are they done?
   (b) Why does PGP maintain key rings with every user? Explain how the messages are generated and received by

6. (a) Discuss about the documents regarding IP security protocol.
   (b) Describe any four ISAKMP payload types listing the parameters of the pay-load.

7. Discuss differences between SSL and TLS.

8. (a) Draw the figure showing VACM logic and explain.
   (b) The encryption scheme used for UNIX passwords is one way; it is not possible to reverse it. Therefore, would it be accurate to say that this is in fact, a hash code rather than an encryption of the password.