

B.Tech IV Year II Semester (R09) Regular & Supplementary Examinations April 2016

**INFORMATION SECURITY**

(Common to ECE & ECC)

Time: 3 hours

Max. Marks: 70

Answer any FIVE questions  
All questions carry equal marks

\*\*\*\*\*

- 1 (a) Explain the four classes of threats.  
(b) Differentiate between symmetric cryptography and asymmetric cryptography.
- 2 Write notes on the following:  
(a) Boot-sector viruses.  
(b) Internet worms.  
(c) Brian viruses.
- 3 (a) Discuss the basic uses of Message Authentication Code.  
(b) Explain key distribution using Public key Cryptography.
- 4 (a) Explain the Arbitrated Digital Signature Technique where the arbiter does not see the message and that uses conventional cryptography.  
(b) Explain the Arbitrated Digital Signature Technique where the arbiter does not see the message and that uses public-key encryption.
- 5 (a) What are the services provided by PGP services?  
(b) Explain the reasons for using PGP.  
(c) Why E-mail compatibility function in PGP needed?
- 6 (a) Discuss the purpose of SA selectors?  
(b) Enumerate on the five default ISAKMP exchange types.
- 7 Explain in detail about SSL record protocol operation.
- 8 (a) What is a firewall? Explain the capabilities that are within the scope of a firewall?  
(b) What are the measures that may be used for intrusion detection?

\*\*\*\*\*