

Code : R7411206

R07**IV B.Tech I Semester (R07) Supplementary Examinations, May 2012****INFORMATION SECURITY****(Information Technology and Computer Science & Systems Engineering)****Time: 3 hours****Max Marks: 80****Answer any FIVE questions****All questions carry equal marks**

1. (a) Draw the model of network security and explain.
(b) Define active security attack. List some of the active security attacks and explain.
2. (a) What are the two general approaches of attacking a cipher?
(b) What is meant by end – to –end encryption? Explain.
(c) Explain HMAC algorithm.
3. (a) What requirements must public key crypto systems fulfill to be a secure algorithm?
(b) Write notes on Kerberos.
4. (a) Why does php generate a signature before applying compression?
(b) Explain S/M₁ME functionality.
(c) Briefly explain R64 conversion. Why R64 conversion useful for e-mail application?
5. (a) What are the benefits of IP sec?
(b) Write notes on IP sec authentication header.
(c) Briefly explain transport mode ESP.
6. (a) List and briefly define the principal categories of SET participants.
(b) Writes notes on TLS.
7. (a) What are the two common technologies to protect a password life?
(b) What are the typical phases of a virus or worm?
(c) Write short notes on SNWPV 1 community facility.
8. (a) What are the four techniques used by firewall to control access and enforce a security policy?
(b) Explain circuit level gateway.
(c) What are the two rules that a reference monitor enforces?
