TE/IT/Sem VI (Rev)
sub- I & NS

ws Oct Sacn- 10 19

Con. 6146-10.

(REVISED COURSE)

(3 Hours)

30/11/10

GT-7677

[Total Marks : 100

N.B.: (1) Question No.1 is **compulsory**.
    (2) Attempt any **four** out of remaining **six** questions.
    (3) Assume suitable data if necessary and state the assumptions clearly.

Q1. (a) What are the attacks in information transfer? Also write the security services used to prevent these attacks.   05
  (b) How AES is better than DES?   05
  (c) Compare ACL with C-List   05
  (d) Explain Session Hijacking.   05

Q2. (a) Explain RSA cryptosystem in detail.   10
  (b) Explain Network layer attacks. Discuss Packet Sniffing in detail   10

Q3. (a) What is symmetric key cryptography? Explain A5/1 algorithm.   10
  (b) Discuss Denial of Service Attack with its causes, preventive and reactive measures.   10

Q4. (a) Discuss various categories of malware and ways to detect them.   10
  (b) Explain different types of firewalls. At which layer of Internet Protocol stack do each operate?   10

Q5. (a) Explain Cryptographic hash function and explain Tiger hash in detail   10
  (b) What are the security policies used by banks during the time of disaster   10

Q6. (a) Discuss different biometric means used for Authentication. Compare them with password authentication.   10
  (b) Compare Signature based and Anomaly based IDS with suitable examples.   10

Q7. Write notes on any **three** of the followings: 20
  (i) Knapsack cryptosystem
  (ii) Covert channel
  (iii) Risk Analysis
  (iv) Web Server vulnerabilities.