

**R09**

**Code No: D0509, D5809, D4003**

**JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD**

**M.Tech II - Semester Examinations, March/April 2011**

**INFORMATION SECURITY**

**(COMMON TO COMPUTER SCIENCE, COMPUTER SCIENCE &  
ENGINEERING, INFORMATION TECHNOLOGY)**

**Time: 3hours**

**Max. Marks: 60**

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

- - -

1. a) Explain various types of Security Services.  
b) Explain various types of Security Attacks.  
c) Explain various types of Security Mechanisms. [4+4+4]
2. a) Discuss in detail Simple-DES(Data Encryption Standard) algorithm.  
b) Explain various modes of operations of block ciphers. [6+6]
3. a) Explain the procedure involved in Rivest-Shamir-Adleman (RSA) public-key encryption algorithm.  
b) Explain the procedure involved in ELGAMAL public-key encryption algorithm. [6+6]
4. a) Explain about Hash and Message Authentication Code(HMAC).  
b) What are the Approaches of Message Authentication? [6+6]
5. a) Explain the Digital Signature algorithm.  
b) Explain the X.509 authentication procedures. [6+6]
6. a) List and explain the Pretty Good Privacy(PGP) services.  
b) What are the five header fields defined in Multipurpose Internet Mail Extensions (MIME)? Explain it? [6+6]
7. a) Explain about the Internet Protocol(IP) Security Architecture?  
b) Explain the significance of dual signature in Secure Electronic Transaction (SET). [6+6]
8. a) What are the differences between Simple Network Management Protocol Version 1(SNMPV1) and Simple Network Management Protocol version3 (SNMPv3).  
b) What is the structure of a virus? [6+6]

\*\*\*\*\*