

<b>R09</b>
------------

**Code No: C7804****JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD****M. Tech I Semester Examinations March/April-2011****INFORMATION SECURITY - I****(COMPUTER NETWORKS & INFORMATION SECURITY)****Time: 3hours****Max.Marks:60**

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

- - -

- 1.a) Discuss about the Security attacks, Services and Mechanisms. [12]  
 b) Explain a Model for Internet work Security.
- 2.a) State and Prove Fermat's Theorem.  
 b) Using Fermat's Theorem, find  $3^{201} \pmod{11}$ . [12]
3. Explain the key expansion process of Data Encryption standard (DES) Algorithm. [12]
- 4.a) Explain Diffie-Helman key exchange algorithm.  
 b) Consider a Diffie-Hellman scheme with a common prime  $q=11$  and a primitive root  $\alpha=2$ . If user A has public key  $Y_{A=9}$ , what is A's private key  $X_A$ ? [12]
- 5.a) Explain the importance of Secure Hash Function.  
 b) Write short notes on Message Digest. [12]
6. What are Kerberos and explain its requirements. [12]
- 7.a) What is the function of SNMP Proxy?  
 b) What threats is USM Designed to Country? [12]
- 8.a) Discuss about Firewall Design Principles.  
 b) Write short notes on the following:  
 i) Reference monitor          ii) Capability ticket. [12]

--ooOoo--