R09

Code No: C7804

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
M. TECH I SEMESTER EXAMINATIONS APRIL/MAY-2012
INFORMATION SECURITY - I
(COMPUTER NETWORKS & INFORMATION SECURITY)

Time: 3hours **Max.Marks:60**

Answer any five questions
All questions carry equal marks

\- - -

1. What is the difference between passive and active security threats? Write notes on security services.

2.a) What is the purpose of the S-boxes in DES?
b) State Fermat's theorem. Using Euler's function, find $\Phi(21)$ and $\Phi(37)$.

3. Write notes on Random Number Generators and their significance in security.

4. Explain AES algorithm.

5. Explain WHIRLPOOL algorithm.

6.a) What are the properties a digital signature should have?
b) Explain digital signature algorithm.

7.a) Give a brief account on Trusted Computing Base.
b) What is the role of compression in the operation of a virus?

8. Write short notes on any two of the following:
a) ECC.
b) OS Security Functions.
c) Race Conditions.

* * * * * *