Time: 3 Hours **Max. Marks: 80**

INSTRUCTIONS
(1) Question 1 is compulsory.
(2) Attempt any **three** from the remaining questions.
(3) Draw neat diagrams wherever necessary.

Q1 **5 marks each**

a) Distinguish between passive and active security attacks
b) Differentiate between virus and worm
c) Explain SSH protocol stack in brief
d) Write short note on :Email Security

Q2 **10 marks each**

a) Discuss classical encryption techniques with example
b) Explain different types of denial of service attacks

Q3 **10 marks each**

a) What are Block cipher modes. Describe any two in detail
b) Given modulus n=221 and public key e=7 find the values of p,q,phi(n) and d using RSA encrypt M=5

Q4 **10 marks each**

a) Discuss various NAC enforcement methods
b) Design sample digital certificate and explain each field of it

Q5 **10 marks each**

a) Show how a Kerberos protocol can be used to achieve single sign on in distributed systems
b) Explain the different types of protocol offered by SSL

Q6 **10 marks each**

a) Why there is a need of a firewall?Explain the different types of firewalls
b) How does IPSec help to achieve authentication and confidentiality?Justify the need of AH and ESP

X532Y5D0D7FX532Y5D0D7FX532Y5D0D7FX532Y5D0D7F