Duration: 3 Hours **[Max Marks: 80]**

N.B. : (1) Question No 1 is Compulsory.
(2) Attempt any three questions out of the remaining five.
(3) All questions carry equal marks.

		Marks
Q.1		
a.	In an RSA System, given N=221, e=7. Calculate Private key d.	**5**
b.	Describe different types of Denial of service attacks.	**5**
c.	Explain SSH protocol stack in brief.	**5**
d.	Describe RC5 algorithm with an example.	**5**
Q.2		
a.	Explain different Block Cipher modes of Operation.	**10**
b.	Define Malware. Explain at least five types with example.	**10**
Q.3		
a.	What is Network Management Security? Explain SNMP V3.	
b.	What is an Intrusion Detection System? Explain its types in detail.	**10**
Q.4		
a.	How does IPSec help to achieve authentication and confidentiality? Justify the need of AH and ESP.	**10**
b.	Explain in detail with diagram, how Kerberos can be used for authentication.	**10**
Q.5		
a.	Explain Playfair cipher with example.	**10**
b.	Explain Security Attacks and Security Mechanisms in detail.	**10**
Q.6	Write Short Notes on **ANY FOUR** of the following:	**20**
a.	Keyed and Keyless transposition	**5**
b.	Principle elements of NAC	**5**
c.	VPN	**5**
d.	Different types of protocol offered by SSL	**5**
e.	Public Key Infrastructure (PKI)	**5**
f.	Types of firewall	**5**

****

X525Y71262EX525Y71262EX525Y71262EX525Y71262E