

Duration: 3 Hours**Total Marks: 80****Instructions to the candidates, if any:-****N.B. : (1) Question No. 1 is compulsory.****(2) Attempt any three questions out of remaining five questions.**

Q. No.	Marks
Q.1 (a) Write short note on eavesdropping.	(05)
(b) Define ARP Spoofing with example, Compare it with IP Spoofing.	(05)
(c) What is X.509 certificate? Describe the steps involved in its generations	(05)
(d) List and explain various types of attacks on encrypted message.	(05)
Q.2 (a) Explain Transposition Ciphers with illustrative Example.	(10)
(b) Explain Block cipher modes of operation	(10)
Q.3 (a) Explain RSA algorithm in details with suitable example.	(10)
(b) How is security achieved in the transport and tunnel modes of ipsec? Describe the role of AH and ESP.	(10)
Q.4 (a) With a block diagram describe MD5.	(10)
(b) Explain Kerberos Protocol in detail.	(10)
Q. 5 (a) Explain Diffie Hellman Key Exchange with suitable Example.	(10)
(b) Explain firewall and its types along with its advantages and disadvantages.	(10)
Q. 6 Write short notes on (Any Four)	(20)
i) Symmetric Vs Asymmetric encryption	
ii) Principle element of NAC	
iii) SSL/TLS	
iv) Honeypot	
v) El-Gamal Algorithm	
vi) Playfair cipher	
