FirstRanker.com
Firstranker's choice
www.FirstRanker.com www.FirstRanker.com

R15

Code No: 824AE

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
MCA IV Semester Examinations, March/April - 2022
INFORMATION SECURITY

Time: 3 Hours **Max.Marks:75**

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

1.a) Explain the operations, requirements and components of Network security model.
b) Differentiate between Active Attacks and Passive Attacks. [8+7]

2.a) Use *Playfair cipher* with the key "COMPUTER" to encrypt the message "INFORMATION SECURITY".
b) Discuss about different poly-alphabetic cipher substitution techniques. [8+7]

3.a) Explain cipher block modes of operations with suitable diagrams.
b) Give the structure of AES. Explain how Encryption/Decryption is done in AES. [7+8]

4.a) Alice and Bob agreed to use RSA algorithm for the secret communication. Alice securely choose two primes, p=5 and q=11 and a secret key d=7. Find the corresponding public key. Bob uses this public key and sends a cipher text 18 to Alice. Find the plain text.
b) Illustrate man in the middle attack on Diffie-Hellman key exchange algorithm. [8+7]

5.a) What are the Security Requirements of message authentication?
b) Discuss the various principles involved in private and public key cryptography. [8+7]

6.a) Explain the authentication procedures defined by X.509 certificate.
b) What is Kerberos? What are the main features of Kerberos Version 5? [7+8]

7.a) How does PGP provide confidentiality and authentication service for e-mail and file storage applications? Draw the block diagram and explain its components.
b) What are the services provided by IPSec? Where can be the IPSec located on a network? [8+7]

8.a) Write briefly about the signature based Intrusion Detection Systems.
b) Discuss about the various types of firewalls. [8+7]

---oo0oo---

www.FirstRanker.com