



Code No: 824AE

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

MCA IV Semester Examinations, October/ November - 2020

INFORMATION SECURITY

Time: 2 Hours

Max.Marks:75

Answer any five questions
All questions carry equal marks

1. Define Caesar cipher? Calculate the encryption and decryption for the following plain text P= "COME TO MY HOME" by using ceaser cipher with Key k=3. [15]
- 2.a) Specify and contrast all kinds of cipher techniques in the cryptography.
b) Mention the key principles of security. [7+8]
- 3.a) Differentiate between AES and DES in a brief manner.
b) Explain how key is generated in the RSA algorithm. [7+8]
- 4.a) Differentiate block cipher and stream cipher techniques.
b) Explain key distribution of symmetric key. [7+8]
- 5.a) Define authentication service. And explain x.509 authentication services in a detail.
b) Describe why Kerberos is more secure than the other security mechanisms? [7+8]
6. Describe the following terms in detail
a) Whirlpool b) knapsack algorithm. [7+8]
- 7.a) Demonstrate combining security associations.
b) Discuss about the IP security architecture in detail. [7+8]
- 8.a) Differentiate socket layer security and transport security.
b) Demonstrate techniques used to avoid guessable password. [7+8]

---oo0oo---