School of Computing Science and Engineering
Master of Computer Applications
Mid Term Examination - May 2024

Duration : 90 Minutes
Max Marks : 50

Sem II - E1PAA201T - Cryptography

General Instructions
Answer to the specific question asked
Draw neat, labelled diagrams wherever necessary
Approved data hand books are allowed subject to verification by the Invigilator

1) What are the different types of attack models? Explain all. — K2 (2)

2) Discuss Kerckhoff's Principle of the cryptosystem. — K1 (3)

3) Explain co-prime number with example. — K2 (4)

4) What is double transposition cipher? Describe with example. — K2 (6)

5) What are the different types of cyber attacks? — K3 (6)

6) Define the cryptosystem assuming the standard symbol. — K3 (9)

7) Apply the Hill cipher algebraically with it encryption and decryption operations. — K4 (8)

8) With the help of an example explain Totient function (phi function), give defination & application also. — K4 (12)

OR

How Expantion & compression function are related to DES algorithm. — K4 (12)