PAPER ID-310320

Roll No: | | | | | | | | | | | | | |

MCA
(SEM III) THEORY EXAMINATION 2025-26
CRYPTOGRAPHY & NETWORK SECURITY

TIME: 3 HRS **M.MARKS: 70**

Note: Attempt all Sections. In case of any missing data; choose suitably.

SECTION A

1. Attempt *all* questions in brief. **02 x 7 = 14**

Q no.	Question	CO	Level
a.	Define cryptanalysis and steganography with examples.	CO1	K2
b.	What is the difference between stream cipher and block cipher?	CO1	K2
c.	Explain Feistel structure in modern block ciphers.	CO2	K3
d.	What is Fermat's theorem? Give its application in cryptography.	CO2	K3
e.	Define Message Authentication Code (MAC).	CO3	K1
f.	Explain Diffie–Hellman key exchange.	CO4	K4
g.	What is a firewall? Mention any two types of firewalls.	CO5	K1

SECTION B

2. Attempt any *three* of the following: **07 x 3 = 21**

a.	Explain classical encryption techniques: substitution and transposition ciphers with suitable examples.	CO1	K2
b.	Describe the structure and working of Advanced Encryption Standard (AES).	CO2	K4
c.	Explain SHA-1 hash algorithm and discuss its security limitations.	CO3	K3
d.	Describe Kerberos authentication protocol with neat diagram.	CO4	K4
e.	Explain SSL architecture and discuss the importance of digital certificates.	CO5	K5

SECTION C

3. Attempt any *one* part of the following: **07 x 1 = 07**

a.	Discuss Shannon's concepts of confusion and diffusion. How do they enhance encryption security? Give examples from DES.	CO1	K2
b.	Explain the working of Triple DES with diagram. Compare it with DES in terms of security.	CO2	K3

4. Attempt any *one* part of the following: **07 x 1 = 07**

a.	Explain RSA algorithm with an example showing key generation, encryption, and decryption.	CO2	K4
b.	Discuss discrete logarithm problem (DLP). Why is it important for public-key cryptography?	CO2	K4

5. Attempt any *one* part of the following: **07 x 1 = 07**

a.	Describe the structure of digital signature and explain ElGamal digital signature scheme in detail.	CO3	K3
b.	What is a hash function? Explain birthday attack with an example.	CO3	K2

6. Attempt any *one* part of the following: **07 x 1 = 07**

a.	Explain symmetric key distribution techniques. Discuss Key Distribution Center (KDC) method.	CO4	K4
b.	What is Public Key Infrastructure (PKI)? Explain X.509 certificate structure.	CO4	K4

PAPER ID-310320

Roll No: | | | | | | | | | | | | |

MCA
(SEM III) THEORY EXAMINATION 2025-26
CRYPTOGRAPHY & NETWORK SECURITY

TIME: 3 HRS **M.MARKS: 70**

7. Attempt any *one* part of the following: 07 x 1 = 07

a.	Explain the components of IP Security (IPSec) architecture. Discuss AH and ESP in detail.	CO5	K5
b.	What is intrusion detection? Explain virus, worm, and Trojan with suitable examples.	CO5	K1