PAPER ID-310613

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

MCA
(SEM III) THEORY EXAMINATION 2024-25
CRYPTOGRAPHY & NETWORK SECURITY

TIME: 3 HRS **M.MARKS: 100**

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

SECTION A

1. Attempt *all* questions in brief. **2 x 10 = 20**

Q no.	Question	CO	Level
a.	What is Cryptography? Explain types and features of Cryptography.	1	2
b.	Between symmetric and asymmetric encryption which method is more convenient and why?	1	2
c.	Define Model of network security.	1	2
d.	What are the three aspects of security?	1	2
e.	What is public key distribution?	4	4
f.	Define firewall design principles.	5	1
g.	What is Euler's theorem?	3	1
h.	What is Birthday Attack?	3	2
i.	Describe the terms Triple DES.	1	2
j.	What do mean by steganography? How it differs from cryptography?	1	2

SECTION B

2. Attempt any *three* of the following: **10 x 3 = 30**

a.	Explain following components of encryption algorithm with examples. 1. Plain text 2. Encryption algorithm 3. Secret key 4. Cipher text 5. Decryption algorithm	1	2
b.	Define Euler's theorem and it's application also Find gcd (24140, 16762), gcd (1970, 1066) using Euclid's algorithm?	2	3
c.	Perform encryption and decryption using RSA Alg. For the following. P=17; q=11; e=7; M=88	2	3
d.	Explain the attacks related to Digital Signature.	4	4
e.	What is a message authentication code? What characteristics are needed in a secure hash function?	5	1

SECTION C

3. Attempt any *one* part of the following: **10 x 1 = 10**

a.	Explain in detail about DES and Triple DES.	1	2
b.	Explain the following terms :— i. Masquerading ii. Passive Attack iii. Stream Cipher. iv. Message Integrity v. Stenography	1	2

4. Attempt any *one* part of the following: **10 x 1 = 10**

a.	Explain Fermat's theorem. What is Euler's totient?	2	4
b.	Describe the principle of differential cryptanalysis.	1	2

PAPER ID-310613

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

MCA
(SEM III) THEORY EXAMINATION 2024-25
CRYPTOGRAPHY & NETWORK SECURITY

TIME: 3 HRS **M.MARKS: 100**

5. Attempt any *one* part of the following: 10 x 1 = 10

a.	Describe the Digital Signature Algorithm (DSA) of Digital Signature Standard.	4	4
b.	What are the requirements of a good hash and MAC?	3	2

6. Attempt any *one* part of the following: 10 x 1 = 10

a.	With DSS, if same message is signed at different occasions, the signatures of the message differ. Why? Explain with suitable example.	3	3
b.	Explain the PGP message generation process. Why does PGP generate a signature before compression while message encryption is applied after compression ?	5	1

7. Attempt any *one* part of the following: 10 x 1 = 10

a.	Write short notes on any **two** of the following: — (a) Pretty Good Privacy (PGP) (b) Firewall (c) Viruses.	4	4
b.	What do you understand by digital certificate? What is a chain of certificates ? How is a X.509 certificate revoked ?	5	1