PAPER ID-410749

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

MCA
(SEM III) THEORY EXAMINATION 2021-22
CRYPTOGRAPHY & NETWORK SECURITY

Time: 3 Hours ***Total Marks: 100***

Note: 1. Attempt all Sections. If require any missing data; then choose suitably.

SECTION A

1. Attempt *all* questions in brief.

Q no.	Question	Marks	CO
a.	Differentiate block cipher and stream cipher.	2	1
b.	Differentiate substitution and transposition cipher.	2	1
c.	What is prime and relative prime number in cryptography?	2	2
d.	Differentiate MAC and Hash.	2	3
e.	What do you mean by product cipher?	2	1
f.	Describe birthday attack.	2	4
g.	What do you mean by authentication?	2	3
h.	Which algorithm can be used to check message authenticity whether it is changed or altered in between the communication.	2	3
i.	Why triple DES is used not double?	2	1
j.	What do you mean by Email security?	2	5

SECTION B

2. Attempt any *three* of the following:

Q no.	Question	Marks	CO
a.	What is Brute-Force attack? Explain with an example.	10	1, 2
b.	Solve the following equations: - (a) $3^{12} \bmod 11$ (b) $8^{-1} \bmod 17$	10	2
c.	In RSA: a. Why can't Bob choose 1 as the public key e? b. What is the problem in choosing 2 as the public key e?	10	3
d.	Distinguish between data-origin authentication and entity authentication. Explain with the help of example.	10	4
e.	What is DDoS? Explain with the help of example.	10	5

SECTION C

3. Attempt any *one* part of the following:

Q no.	Question	Marks	CO
a.	Describe criteria that are intended to increase confusion and diffusion properties.	10	1, 2
b.	How many permutations are used in a DES cipher algorithm? How many permutations are used in the round-key generator?	10	1

QP22O1P_132 | 07-Jan-2022 14:30:58 | 43.230.196.221

QP22O1P_132 | 07-Jan-2022 14:30:58 | 43.230.196.221

4. Attempt any *one* part of the following:

Q no.	Question	Marks	CO
a.	In a RSA system, the public key of a given user is e=31, n=3599. What is the private key of this user?	10	3
b.	Perform encryption and decryption using the RSA algorithm, for any two of the following: (a) p=3; q=11; e=7; M=5. (b) p=5; q=11; e=3; M=9. (c) P=7; q=11; e=17; M=8.	10	3

5. Attempt any *one* part of the following:

Q no.	Question	Marks	CO
a.	Using fermat's theorem, find $3^{201} mod 11$.	10	2
b.	Compare and contrast features of SHA-512.	10	3

6. Attempt any *one* part of the following:

Q no.	Question	Marks	CO
a.	Define the RSA digital signature scheme and compare it to the RSA cryptosystem.	10	4
b.	In the Diffie-Hellman protocol, g = 7, p = 23, x = 3, and y = 5. a. What is the value of the symmetric key? b. What is the value of R_1 and R_2.	10	4

7. Attempt any *one* part of the following:

Q no.	Question	Marks	CO
a.	What services are provided by IPSec?	10	5
b.	What is a firewall? Discuss its different types and possible configuration.	10	5

QP22O1P_132 | 07-Jan-2022 14:30:58 | 43.230.196.221

QP22O1P_132 | 07-Jan-2022 14:30:58 | 43.230.196.221