PAPER ID-310118

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

MCA
(SEM-V) THEORY EXAMINATION 2020-21
CRYPTOGRAPHY & NETWORK SECURITY

Time: 3 Hours ***Total Marks: 70***

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

SECTION A

1. Attempt *all* questions in brief. 2 x 7 = 14

a.	Define symmetric key cipher.
b.	Distinguish between a stream cipher and a block cipher.
c.	Distinguish between Z and Z_n. Which set can have negative integer?
d.	Differentiate terms Cryptology and Cryptanalysis.
e.	Differentiate active and passive attack.
f.	Define term Brute-force search.
g.	Using Euler's Theorem solve $3^4 \bmod 10$.

SECTION B

2. Attempt any *three* of the following: 7 x 3 = 21

a.	Calculate greatest common divisor of (1547,560).
b.	Use a Hill cipher to encipher the message "We are the students of MCA program". Use the following key: $K = \begin{bmatrix} 03 & 02 \\ 05 & 07 \end{bmatrix}$
c.	Compare the substitution in DES and AES in detail.
d.	Explain Diffie-Hellman key exchange algorithm.
e.	Use the vigenere cipher with keyword "HEALTH" to encrypt the message "Life is full of surprises".

SECTION C

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

(a)	What is firewall? Discuss firewall design principles in detail.
(b)	Find the result of the following, using Fermat's little theorem: (i) $5^{15} \bmod 13$, (ii) $456^{17} \bmod 17$

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

(a)	Perform encryption and decryption, using RSA algorithm for p=3; q=11; e=7; M=5.
(b)	What is triple DES? Explain the term meet-in-the-middle attack.

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

(a)	What is Transposition Cipher? Illustrate with an example.
(b)	Describe the various issues in network security.

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

(a)	What do you understand by digital certificate? What is a chain of certificates? How is a X.509 certificate revoked?
(b)	What is a message authentication code? What characteristics are needed in a secure hash function?

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

(a)	What is PGP? How different is it from X.509? Give services provided by PGP and their brief description.
(b)	Explain full-service Kerberos environment. What are the principle differences between version 4 and version 5 of Kerberos?