[45101]
SPECIAL DRIVE-DEC./JAN.-2023
M.C.A. DEGREE EXAMINATIONS
FOURTH SEMESTER
Paper - I : INFORMATION SECURITY AND CRYPTOGRAPHY
(2016-17 and 2017-18 Admitted Batches)

Time : 3 Hours **Maximum Marks: 75**

SECTION - A

Answer ALL questions. **(4×15=60)**

1. a) Use Hill cipher to encrypt the text DEF. The key to be used is $\begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 8 & 7 \end{bmatrix}$.

b) What is Steganography? Explain its features.

(OR)

c) With help of an example explain how can we find out GCD of two numbers using Euclid algorithm.

d) Explain the conventional security model used for information security.

2. a) Explain Sub key generation Process in Simplified DES algorithm.

b) Describe Feistel Cipher Structure with respect to its design features.

(OR)

c) P and Q are two prime numbers. P=7, and Q=17. Take public key E=5. If plain text value is 6, then what will be cipher text value according to RSA algorithm? Explain in detail.

d) What are the requirements of digital signature?

3. a) What are the various virus counter measures?

b) Discuss about Secure Hash algorithm.

(OR)

c) Explain about certificate based authentication and password management.

4. a) What is a Firewall? Explain its design principles and types with example.

b) Give IP Security architecture with neat diagram.

(OR)

c) What are different services provided by the SSL Record Protocol? Which parameters define session state and connection state.

SECTION - B

Answer any FIVE from the following. **(5×3=15)**

5. a) What are the types of security attacks?

b) Compare substitution ciphers with transposition ciphers.

c) What is avalanche effect in DES?

d) Evaluate Euler's totient function Φ (37).

e) Define linear and differential cryptanalysis.

f) How encapsulating security payload help in IP security?

g) What are the limitations of firewalls?

h) What is bio-metric authentication?
