(2 ½ Hours)   **[Total Marks: 75]**

N.B.   1) All questions are compulsory.
2) Figures to the right indicate marks.
3) Illustrations, in-depth answers and diagrams will be appreciated.
4) Mixing of sub-questions is not allowed.

Q. 1   Attempt ANY FOUR from the following: **(20M)**
(a)   Define computer security. What are the objectives of computer security?
(b)   What is an active attack in security? State various types of active attacks.
(c)   Write a note on Steganography.
(d)   Encrypt the following message using Rail Fence Algorithm with key size = 4.
Plaintext = they are attacking from the north.
(e)   Explain Electronic Code Book(ECB) mode in cryptography.
(f)   Differentiate substitution and transposition techniques.

Q. 2   Attempt ANY FOUR from the following: **(20M)**
(a)   Write a note on public key cryptosystem.
(b)   Describe X.509 certificate format.
(c)   Assume Alice and Bob wish to communicate secretly. Compute the shared
secret key using Diffie Hellman Key Exchange.
[Prime number $p = 7$, generator $g = 3$, Alice's private key = 2, Bob's private
key = 4]
(d)   How does HMAC algorithm work?
(e)   Discuss the concept of a digital signature. Explain its types.
(f)   Explain kerberos processing in detail.

Q. 3   Attempt ANY FOUR from the following: **(20M)**
(a)   What is a firewall? State and explain various types of firewall.
(b)   Explain the importance of web security.
(c)   What is S/MIME (Secure/Multipurpose Internet Mail Extensions)? Define its
key features.
(d)   Describe IP security architecture.
(e)   State and explain any 5 types of virus.
(f)   Write a note on honeypots.

Q. 4   Attempt ANY FIVE from the following: **(15M)**
(a)   Define terms :
   i.   Cryptanalysis
   ii.   Brute Force Attack
(b)   What is message authentication code?
(c)   State any two common forms of malicious code.
(d)   Using Caesar cipher with key size = 3, encrypt the message "hide the gold and
defend east wall"
(e)   What are the three properties of Hash function?
(f)   Explain the life cycle of viruses.

****

40170

C8FBDCA165F35CDA4C2D2BBCD1811A57