Vidya Vikas Education Trust's
Universal College of Engineering
Gujarati Linguistic Minority Institution

Date: 14/05/2021	Internal Assesment Test: 1	Branch: Computer
Semester: 6	Subject: Cryptography & System Security	Marks: 20

Q1 Attempt any 5 from 6 **(10 Marks)**

a. What is authentication header(AH) ? How does it protect against replay attacks ?
b. Explain working of DES detailing the Fiestel structure
c. What are the system security goals ? Explain why the balance among different goals is needed
d. What is denial of service attack ?
e. What are different security goals ?
f. What are block cipher algorithmic modes ? Describe any two modes

Q2 Attempt any 1 from 2 **(5 Marks)**

a. Explain structure of DES
b. Define the goals of security and specify mechanisms to achieve goal

Q3 Attempt any 1 from 2 **(5 Marks)**

a. List the functions of the different protocols of SSL. Explain the handshake protocol
b. Explain any one of block ciphers with example

****