**Assignment I**

**Cryptography and Network Security(CSE324)**

1a. Define computer security. Explain CIA triad.

b. For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity respectively. Justify your answers.

i) An organization managing public information on its web server.

ii) A law enforcement organization managing extremely sensitive investigative information.

2a. Explain the different types of security mechanisms.

b. Consider an implanted medical device that monitors & records data about a patient’s health and stores the information locally. To access the data, authorized personnel must transmit a personal identification number to the implanted device, and once authorized, electronically request specific portions of data. Give examples of confidentiality, integrity and availability requirements associated with the system, and in each case, indicate the degree of importance of the requirement.

3a. What are the challenges of computer security? Explain.

b. It is required to encrypt the message “COMPUTER SCIENCE STUDENTS ”. Use the key as “MIGHTY”. Design the Playfair cipher and give the encrypted message.

4a. What is a threat? How is it different from an attack? Explain the different types of security attacks.

b. Give an example to explain how Hill cipher can be broken.

5a. Draw a matrix that shows the relationship between security services and mechanisms.

b. Using Vigenere Cipher encrypt the word “cryptographic system” using the key ALERT. Also decrypt the obtained cipher text.

6a. What is an autokey system? How is it different from a one time pad? Give an example for each.

b. Encipher the message “notification” using rail fence cipher of depth 3. What is the drawback of this method? Illustrate how it can be strengthened.