Department of Compute Science.
MCA, Semester-IV

Assignment #1
Cryptography and Network Security

- **Last date of online submission : April 10,2020**
- **Maximum Marks : 10**

1. Define the three security goals.

2. Distinguish between passive and active security attacks .Name some passive and active security attacks.

3. What is the OSI security architecture? Explain.

4. What are the essential ingredients of a symmetric cipher?

5. What are the two basic functions used in encryption algorithms? Explain.

6. Differentiate between block cipher and stream cipher ?

7. What are the two general approaches to attack a cipher?

8. A cipher text has been generated with an affine cipher. The most frequent letter of the ciphertext is 'F' , and the second most frequent letter of the ciphertext is 'C' . Break this code.

9. A small private club has only 100 members . Answer the following questions:
   a. How many secret keys are needed if all members of the club need to send secret messages to each other?
   b. How many secret keys are needed if everyone trusts the president of the club? If a member needs to send a message to another member, she first sends it to the president; the president then sends the message to the other member.
   c. How many secret keys are needed if the president decides that the two members who need to communicate should contact him first. The president then creates a temporary key to be used between the two. The temporary key is encrypted and send to both members.

10. Some archeologists found a new script written in an unknown language. The archeologists later found a small tablet at the same place that contains a sentence in the same language with the translation in Greek. Using the tablet, they were able to read the original script. What type of attack did the archeologists use?