

**Department of Compute Science.
MCA, Semester-IV**

Assignment # 4

Cryptography and Network Security

Last date of online submission : 30.04.2020

1. List two disputes that can arise in the context of message authentication.
2. What are the properties a digital signature should have? Explain.
3. What requirements should a digital signature scheme satisfy?
4. What is the difference between direct and arbitrated digital signature?
5. In what order should the signature function and the confidentially function be applied to a message, and why?