Assignment #4– Understanding Crypto Basics Deadline: 5th Nov' 2019

1. (a) Write AES (Rindael) algorithm as discussed in class.
 (b) Discuss the diffusion and confusion properties achieved by AES
 (c) Execute the AES code and discuss the avalanche property exhibited by AES

2. Let IIT Patna wish to transfer all the files\ documents digitally. Prepare a case study and summarize through a table highlighting the following.

   ➔ Define the security threats
   ➔ Security Services required to address that threat
   ➔ Cryptographic mechanisms required with proper justification.