Department of Compute Science.
MCA, Semester-IV

Assignment #2
Cryptography and Network Security

❖ **Last date of online submission : April 18,2020**

1. What was the original and final set of criteria used by NIST to evaluate candidate AES ciphers?

2. List the parameters (block size, key size, and the number of rounds) for the three AES versions.

3. How many transformations are there in each version of AES? How many round keys are needed for each version?

4. Compare DES and AES. Which one is bit-oriented? Which one is byte oriented?

5. Define state in AES? How many states are there in each version of AES?

6. Which of the four transformations defined for AES change the contents of bytes? Which one does not change the contents of the bytes?

7. Compare the substitution in DES and AES. Why do we have only one substitution table(S-box) in AES, but several in DES?

8. Compare the permutations in DES and AES. Why do we need expansion and compression permutations in DES, but not in AES?

9. Compare the round keys in DES and AES. In which cipher is the size of the round key the same as the size of the block?

10. Why do you think the mixing transformation (MixColumns) is not needed in DES, but is needed in AES?