

Assignment – 5

Date: October 03, 2018

Submission Deadline: October 24, 2018

All assignments will be marked out of 20. No assignment will be evaluated after the deadline.

1. Implement Data Encryption Standard (DES). (Refer to appropriate text for detailed specifications.)
 - a. For implementation you may skip the initial permutation (and its inverse permutation at the end).
 - b. Implement both encryption and decryption functions.
 - c. You may assume the plaintext to be a random string of bits, divide it into blocks to encrypt.
 - d. Select the key to be any bitstring of length 56 bits.