Homework 3

1. One round version of DES

- Input:
  - **K** (key): hexadecimal – 0 1 2 3 4 5 6 7 8 9 A B C D E F
    Binary – 0000 0001 0010 0011 0100 0101 0110 0111
    1000 1001 1010 1011 1100 1101 1110 1111
  - **T** (plaintext): F E D C B A 9 8 7 6 5 4 3 2 1 0

- Perform a round of encryption and write down the resulting ciphertext
- (Describe all of the intermediate steps to derive the result)

Homework 3

2. Show that DES decryption is, in fact, the inverse of DES encryption

- Due date
  - 2017. Oct. 2, 23:59
  - Upload your answer into the Blackboard