Comp7401 - Lab #2

Objective: To analyze a basic Feistel structure.

- Consider an 8-bit block cipher based on the Feistel structure (basic DES building block) with two rounds and no initial or final permutation.

- The scrambling function for round is defined as:

  $f_i(x, k) = [(2i*k)^x] \bmod 15$; **Where: i = 1, 2; k = 7 ∀ k**

  Plaintext (x) = 00101000

1. **Encryption cycle**

   (a). Generate the ciphertext after the 2 rounds
   (b). Draw the diagram of the Feistel Cipher network and show all the intermediate steps and results.

2. **Decryption cycle**

   (a). Work in reverse and generate the plaintext from the ciphertext after the 2 rounds
   (b). Draw the picture of the Feistel Cipher network and show all the intermediate steps and results.