Feistel Cryptosystem

March 28, 2021

0.1 A simple three-round Feistel cryptosystem

The block size is 8 and key length is 12. The number of rounds $NR = 3$. For each length-12 bit string $\kappa = k_1 k_2 \cdots k_{12}$, representing a system key, the key scheduling algorithm will take the ith keys ($i = 1, 2, 3$) to be the following 4-bit srings:

$\kappa^1 = k_1 \cdots k_4 \oplus k_5 \cdots k_8$

$\kappa^2 = k_5 \cdots k_8 \oplus k_9 \cdots k_{12}$

$\kappa^3 = k_9 \cdots k_{12} \oplus k_1 \cdots k_4$

The round key function $f_{\kappa^i}(R)$ is simply obtained by XORing an inputted 4-bit string R with the round key κ^i.

0.2 Assignment 1:

Write a program with syntax Ctext = FeistelSystem3(Ptext, Key) that will perform the three-round Feistel system encryption process.