ENEE/CMSC/MATH 456
Feistel Class Exercise

1. Consider a *two*-round Feistel Network with input length ℓ, key length n and round functions $F_k(\cdot)$, where $F: \{0,1\}^n \times \{0,1\}^{\ell/2} \to \{0,1\}^{\ell/2}$ is a pseudorandom function. Prove that the output of the Feistel Network is *not* a pseudorandom permutation (PRP).

   See attached sheet for the structure of a Feistel Network.

2. **Challenge** Consider a *three*-round Feistel Network with input length ℓ, key length n and round functions $F_k(\cdot)$, where $F:\{0,1\}^n \times \{0,1\}^{\ell/2} \rightarrow \{0,1\}^{\ell/2}$ is a pseudorandom function. Prove that the output of the Feistel Network is *not* a strong pseudorandom permutation (sPRP).

   See attached sheet for the structure of a Feistel Network.

   Hint: The sequence of queries needed is:

   1. Forward direction on (L_0||R_0), getting back (L_3||R_3)
   2. Backward direction on (L_3||R_3 + \Delta), getting back (L'_0||R'_0)
   3. Forward direction on (L_0 + \Delta||R_0), getting back (L''_3||R''_3)

      There will be a relationship between R_0, L_3, R'_0 and L''_3

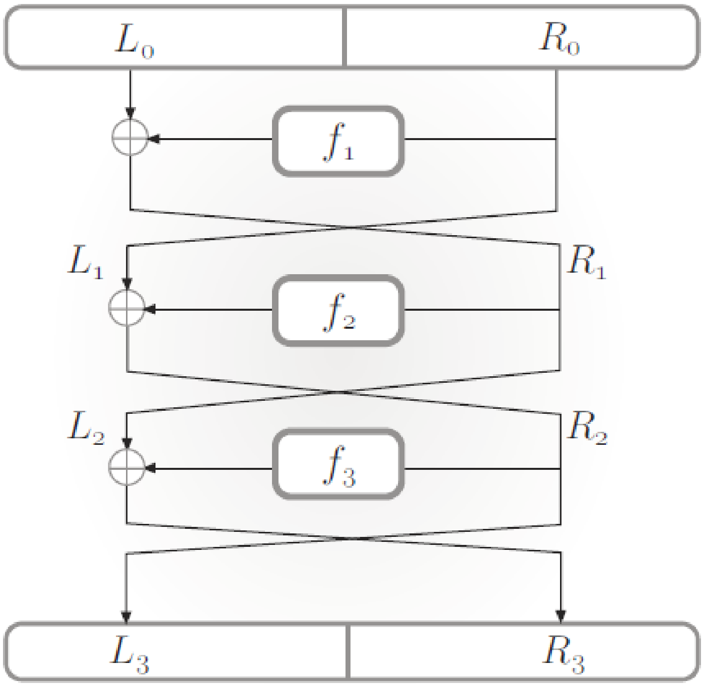

FIGURE 6.4: A 3-round Feistel network.