1. Consider a two-round Feistel Network with input length $\ell$, key length $n$ and round functions $F(\cdot)$, 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 pseudorandom permutation (PRP).

See attached sheet for the structure of a Feistel Network.

Solution:

1. Query $L_0||R_0$, get back $F_k(R_0) + L_0||*$ (we don't care what's on the right)
2. Query $L_0 + \Delta||R_0$, get back $F_k(R_0) + L_0 + \Delta||*$
3. XOR the two left hand sides. If you get back $\Delta$, then output 0. Otherwise output 1.

The probability of outputting 1 when the oracle is a 2-round Feistel is 1. The probability of outputting 1 when the oracle is a random permutation is approximately $1/2^{\ell/2}$. The difference is clearly non-negligible. Thus, this is a valid attack on the security of the 2-round Feistel.
2. **Challenge** Consider a three-round Feistel Network with input length $\ell$, key length $n$ and round functions $F^{n \times 0,1^{\ell/2}} \rightarrow 0,1^{\ell/2}$ 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 $L''_3$

Solution: When we query $(L_0 || R_0)$, we get back $(L_3 || R_3)$.

When we query the backward direction on $(L_3 || R_3 + \Delta)$, we get $L'_2 = R'_1 = L_2 + \Delta$, and $L'_1 = R'_0 = L_3 + f(L_2 + \Delta)$, where $L_2 = L_0 + f(R_0)$

When we query the forward direction on $(L_0 + \Delta || R_0)$, we get back $L''_3 = R_0 + f(L_2 + \Delta)$.

So we have the relationship: $R'_0 + L_3 = R_0 + L''_3$.

If the above relationship occurs, the distinguisher outputs 1. The probability of outputting 1 when the oracle is 3-round Feistel is 1. The probability of outputting 1 when the oracle is a random permutation is approx. $1/2^{\ell/2}$. 
**FIGURE 6.4:** A 3-round Feistel network.