Consider a block cipher using a Feistel structure with only 3 rounds and round function f.

1. Suppose that you are given the key K and one plaintext block ($P = L_0, R_0$). Compute the cipertext ($C = L_3, R_3$).
2. Decrypt the cipertext C you calculated in 1).

There is a trick to the encryption and decryption that you must realise for Feistel to work in practice – the blocks must be flipped after the last round, during encryption and decryption. So $L = R_3$ and $R = L_3$ at the end. Keep in mind that each round has a different key K_1, K_2 and K_3.

1.

$$\begin{aligned}
L_1 &= R_0 \\
R_1 &= f(R_0, K_1) \oplus L_0 \\
\Rightarrow L_2 &= R_1 = f(R_0, K_1) \oplus L_0 \\
R_2 &= f(R_1, K_2) \oplus L_1 \\
\Rightarrow L_3 &= R_2 = f(R_1, K_2) \oplus L_1 \\
R_3 &= f(R_2, K_3) \oplus L_2 \\
L &= R_3, R = L_3
\end{aligned}$$

2.

$$\begin{aligned}
L'_0 &= L = R_3, R'_0 = R = L_3 \\
\Rightarrow L'_1 &= R'_0 = L_3 = f(R_1, K_2) \oplus L_1 \\
R'_1 &= f(L_3, K_3) \oplus R_3 = f(R_2, K_3) \oplus f(R_2, K_3) \oplus L_2 = L_2 \\
\Rightarrow L'_2 &= R'_1 = L_2 \\
R'_2 &= f(R'_1, K_2) \oplus L'_1 = f(L_2 = R_1, K_2) \oplus f(R_1, K_2) \oplus L_1 = L_1 \\
\Rightarrow L'_3 &= R'_2 = L_1 = R_0 \\
R'_3 &= f(L_1, K_1) \oplus L_2 = f(R_0, K_1) \oplus f(R_0, K_1) \oplus L_0 = L_0 \\
\Rightarrow L &= R'_3 = L_0, R = L'3 = R_0
\end{aligned}$$