Information_Security_Exercise4

1.

$$L_i = R_{i-1} \tag{1}$$
$$R_i = L_{i-1} \oplus F(k_i, R_{i-1}) \tag{2}$$
$$R_{i-1} = R_{i-1}^{'} \oplus 111...11 \tag{3}$$

From (1)(3), we get

$$L_i = R_{i-1}^{'} \oplus 111...11 \Rightarrow L_i \oplus 111...11 = R_{i-1}^{'} \tag{4}$$

i.e.

$$L_i^{'} = R_{i-1}^{'} \tag{5}$$

Also we know that there is XOR in F function.

$$k_i \oplus R_{i-1} = (k_i^{'} \oplus 111...11) \oplus R_{i-1} = k_i^{'} \oplus R_{i-1}^{'} \tag{6}$$

Consider the given hint, we can get

$$R_i^{'} = (L_i \oplus F(k_i^{'}, R_{i-1}^{'}) = L_i^{'} \oplus F(k_i^{'}, R_{i-1}^{'}) \tag{7}$$

Finally, from (5)(7) we can prove

$$Y^{'} = E_{k^{'}}(X^{'})$$

2.

All keys for 16 rounds will be the same if k = all 0's. Decryption process is the same as the encryption process, except we apply the keys in reverse order. But since all the keys is the same, we get

$$E_k(P) = D_k(P)$$

This is the proof.

Method: Do not use weak key, like k = all 1's, or 0101 0101 0101 0101(hexadecimal).