

Encryption:

$$LE_1 = RE_0$$

$$RE_1 = LE_0 \oplus F(CRE_0, k_1)$$

$$LE_2 = RE_1$$

$$RE_2 = LE_1 \oplus F(CRE_1, k_2)$$

$$\vdots$$

$$LE_0 = RE_{i-1}$$

$$RE_i = LE_{i-1} \oplus F(CRE_{i-1}, k_i)$$

Decryption:

$$LD_0 = RE_{16}$$

$$RD_0 = LE_{16}$$

$$LD = RD_0$$

$$RD_1 = LD_0 \oplus F(RD_0, k_{16})$$

$$LD = RD_1$$

$$RD_2 = LD_1 \oplus F(RD_1, k_{15})$$

$$\vdots$$

$$LD = RD = RE_0 \rightarrow LD_p = RD_{p-1} = RE_0$$

$$RD_{16} = LD_{15} \oplus F(RD_{15}, k_1) = LE_0 \Rightarrow RD_p = LD_{p-1} \oplus F(RD_{p-1}, k_p)$$

$$RD_{17} = LE_0, \quad LD_{17} = RE_0$$