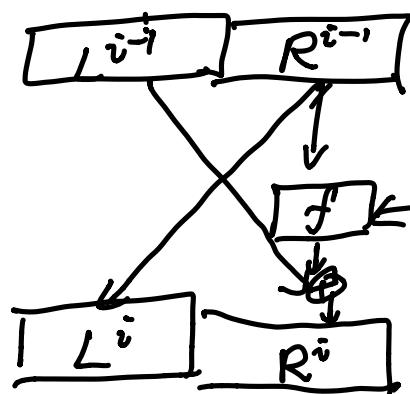ECE 471/571 SPN, DES

Feistel cipher
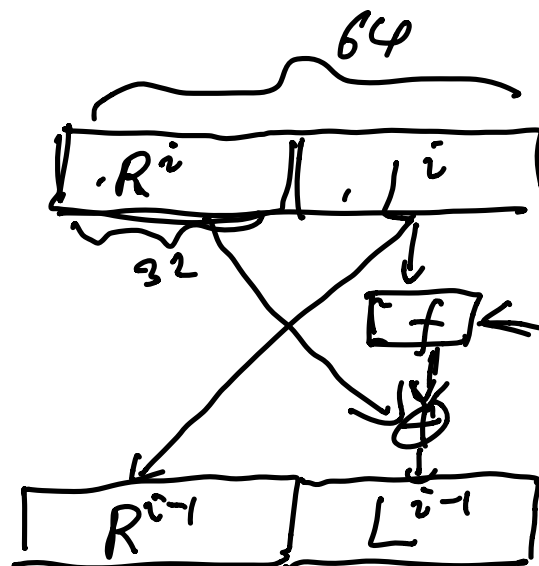
Enc.



$$L^i = R^{i-1}$$

$$R^i = L^{i-1} \oplus f(R^{i-1}, k^i)$$

Dec.



$$R^{i-1} = L^i$$

$$L^{i-1} = R^i \oplus$$

$$f(R^{i-1}, k^i)$$

$$\neq f(L^i, k^i)$$

for the solution of the SPN question on tophat,
please see the notes published in

weekly materials → scanned lecture
notes (2019)

in   2/4/2019.