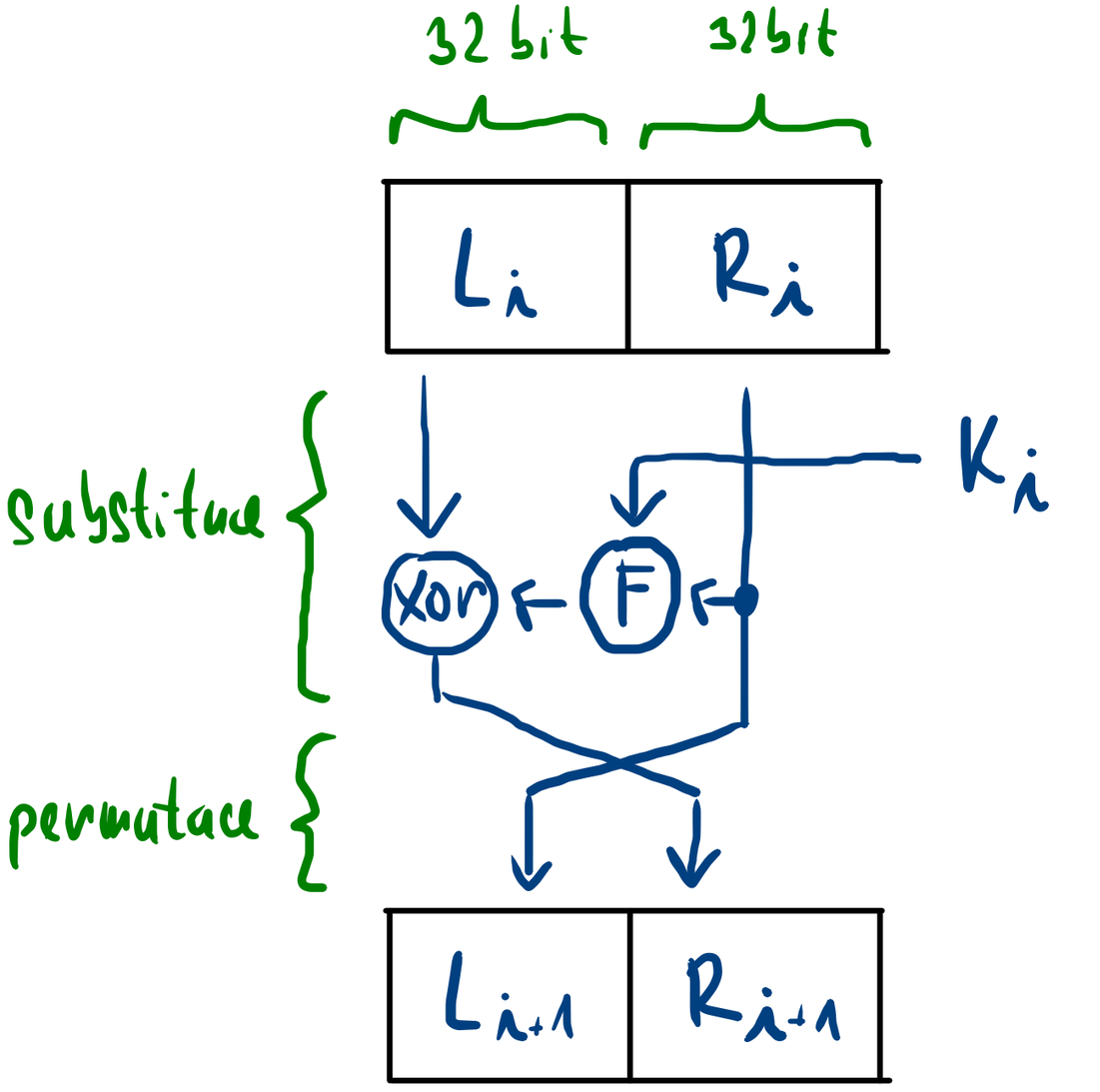
Příklad

9. Nakresliť a popísať Feistelovu šifru, napísať algoritmus ktorý to používa.

- Princip blokových symetrických šifer
- Vstup rozdělen na bloky o 64 bitech
  - ↳ vstup rozpůlen

$$L_{i+1} = R_i$$

$$R_{i+1} = L_i \otimes F(R_i, K_i)$$



využívají symetrické algoritmy

DES, AES, ...