

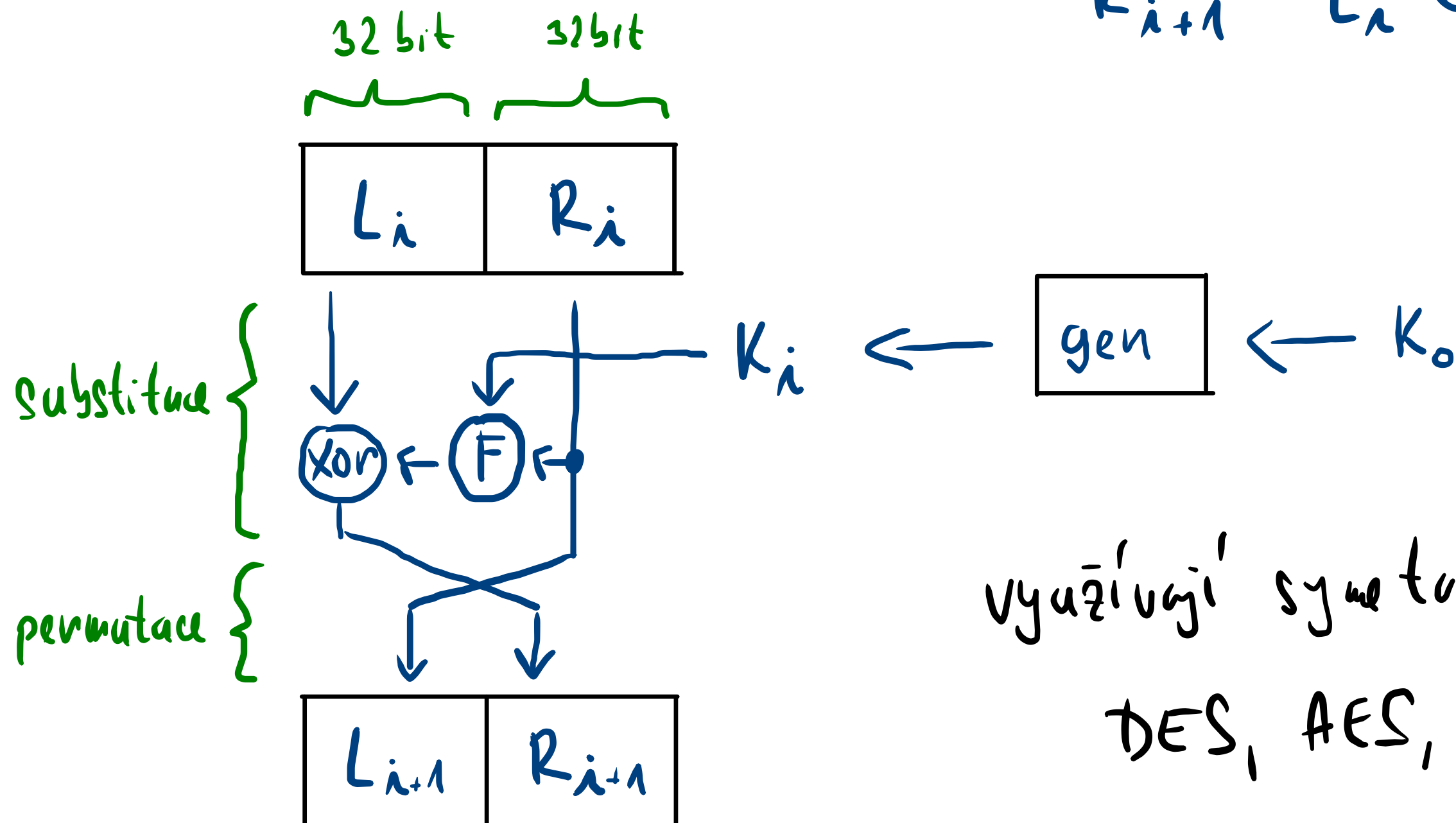
Příklad

9. Nakreslit a popísat Feistelovu šifru, napísat algoritmus který to používá.

- Princip blokových symetrických šifer
- Vstup rozdělén na bloky o 64 bitech
↳ vstup rozpušen

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

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



využívají symetrické algoritmy
DES, AES, ...