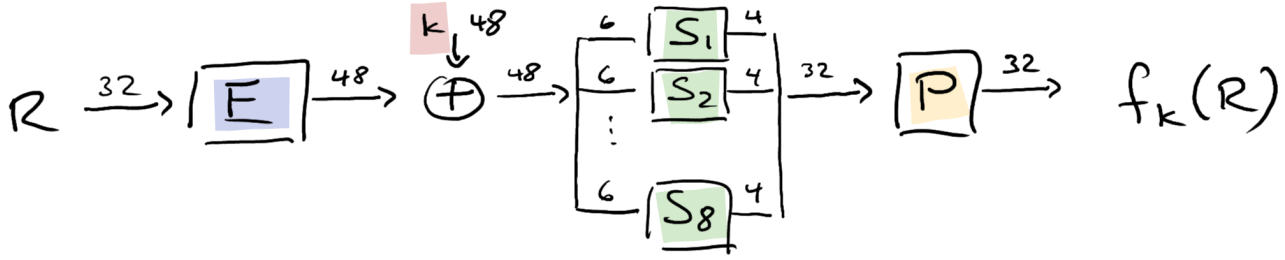
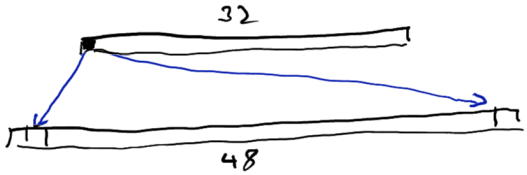
DES internals

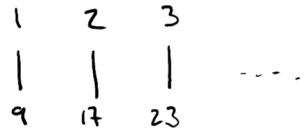
round function $f_k(R)$



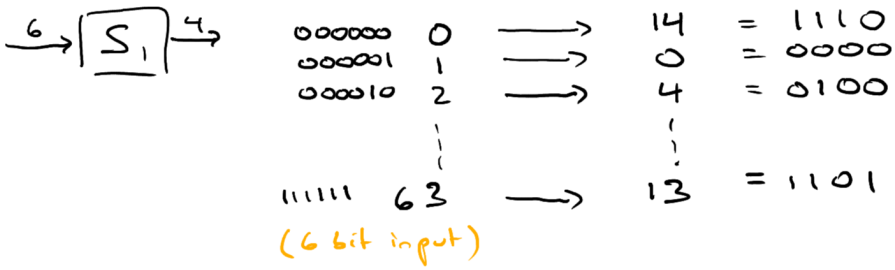
E-box expansion



P-box permutation



S-box substitution "heart of DES"



- carefully designed
  - 1994 : S-box design criteria published
  - protect against differential cryptanalysis
- must be nonlinear
- if 1 input bit changes, at least 2 output bits change