ENEE/CMSC/MATH 456
SPN Class Exercise

1. Present an attack and analyze the complexity of your attack to recover the all sub-keys of a *two*-round SPN (with a final key-mixing step) with the following parameters (same as picture on the attached sheet and the one in the lecture notes):
   - Block size: $\ell = 16$
   - Sub-key length: $n = 16$, the three sub-keys, k_1, k_2, k_3 are uniform, independent 16-bit keys.
   - Number of S-boxes: 4, each with 4-bit input/output

   Same structure as in the picture on the next sheet.

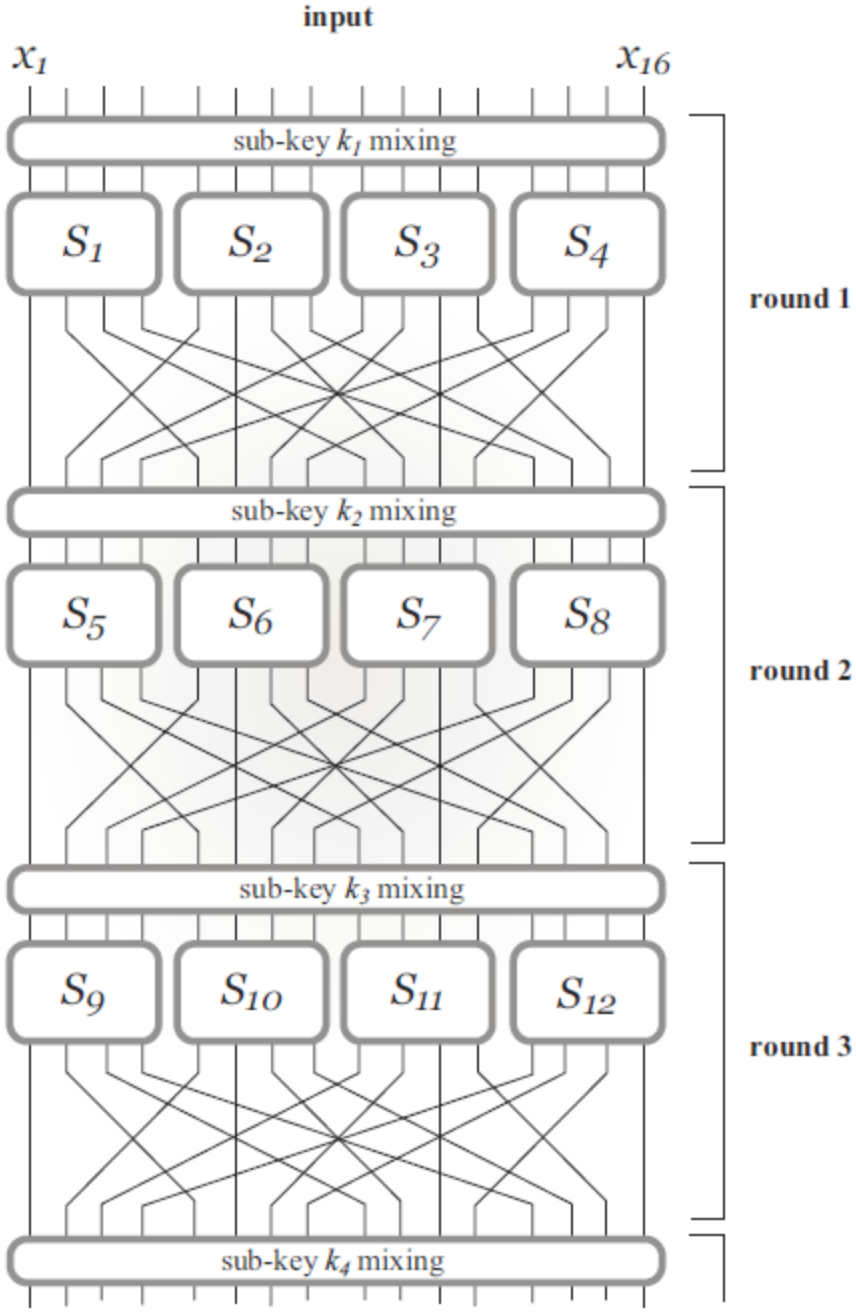

FIGURE 6.2: A substitution-permutation network.