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.

Solution: We brainstormed several solutions. The final one was as follows:
   - Obtain an input/output pair \((x,y)\)
   - Guess all possible \( k_3 \) (2^16 of them)
   - Work backward to obtain the intermediate value after the \( k_2 \) mixing step.
   - Guess the values of \( k_2 \) corresponding only to the outputs of the first S-box (2^4 of them)
   - Work backwards to obtain the intermediate value after the \( k_1 \) mixing step.
   - XOR with the appropriate bits of the input to obtain a candidate (partial) \( k_1 \) value.
   - We now have a table with \((2^20)\) candidate (partial) key tuples. We will ask for additional input/output pairs. Note that we have to work backwards from the output to obtain a partial input and that the partial input is 4-bit length. So we expect to require 5 additional input/output pairs as \((2^4)^5 = 2^{20}\).
   - In total, we have spent \( 5*2^{20} \) time. We must repeat this 4 times to obtain the rest of the key. So this would be \( 20*2^{20} = 5*2^{22} \) time.

Note this is still better than brute force search \((2^{48})\) time and better than our first attempt which did not make use of partitioning the input w.r.t S-boxes, which was \( 2^{32} \) time.
FIGURE 6.2: A substitution-permutation network.