

Mathematics of Coding and Cryptography Worksheet 6

Suppose you have access to a 3-round machine using the simplified DES algorithm we have discussed in class (with the same S-boxes and expander we have been using). Suppose you enter two inputs

$$LR = 000000111111 \quad \text{and} \quad L^*R^* = 101010111111$$

into the machine, and the respective outputs are

$$111011011010 \quad \text{and} \quad 010100111000.$$

What is the key?