BLG 351E – Microcomputer Laboratory
Experiment 3

Introduction

The main purpose of this experiment is to gain more experience in assembly programming of MC6802. To this end, you are expected to implement the bit-wise encryption algorithm using the preliminary information according to the points indicated in the experiment part.

Preliminary Information: Bit-wise Encryption

Encryption operations are frequently used to ensure the security of the data in computer/communication systems. In this experiment, we will implement a simple encryption technique, namely bit-wise encryption, by manipulating the bits of the data (plain text). When manipulating the bits of the plain text, XOR and permutation operations are widely used and the cipher text is generated. Decryption of the cipher text makes use of the same operations here to get the original plain text back. However, the operations performed during the encryption are run backwards.

The bit-wise encryption algorithm you are expected to implement works on 8-bit plain text as follows:

1. The first 4-bits and the last 4-bits of the plain text are permutated
   (e.g., ABCDEFGH → EFGHABCD)
2. The resulting text from the first step is divided into 4 groups and bits are permutated in each group (e.g., EFGHABCD → FEHGBADC)
3. As the final step, the resulting text from the second step is XORed with an 8-bit key to produce the cipher text. (e.g., cipher text = FEHGBADC XOR KLMNOPQR)

Part 1

You are expected to implement the bit-wise encryption algorithm explained in the Preliminary Information Section. Your program should start from the address **$4000**. It will read the plain text from the memory location **$10**. The encryption key will be stored in the address **$11**. After the encryption operation, your program is expected to write the cipher text to the memory location **$12**.

Do not overwrite your program for Part 1 on the kit while implementing Part 2.

Part 2

You are expected to implement a decryption program for the bit-wise encryption algorithm. Your program should start from **$4100** and read the cipher text from the memory location **$12**. It will use the encryption key that is stored in the address **$11**. After the decryption operation, your program is expected to write the plain text to the memory location **$13**.

$0010	Plain text
$0011	Encryption key
$0012	Cipher text
$0013	Plain text

Encryption — Decryption
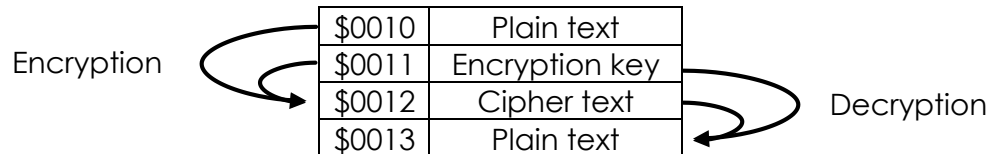
Report

Your report should contain your observations and your programs with explanations for the experiment.