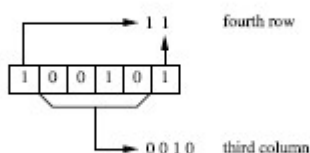


FAST NATIONAL UNIVERSITY
School of Computing
Spring 2021

| | |
|---------------|---|
| Course Title: | Computer Organization and Assembly Language |
| Task: | Assignment #5 |
| Due Date: | 16 th May, 2021 |
| Weightage: | 3% |

Q1. In this assignment, you have to implement the s-boxes which are an essential part of the Data Encryption Standard (DES). Each s-box is a lookup table that maps a 6-bit input to a 4-bit output. An example of how to convert the input to output is as follows:

The S-box input $b = (100101)_2$ indicates the row $11_2 = 3$ (i.e., fourth row, numbering starts with 00_2) and the column $0010_2 = 2$ (i.e., the third column). If the input b is fed into S-box 1, the output is $S_1(37 = 100101_2) = 8 = 1000_2$.



Example of the decoding of the input 100101_2 by S-box 1

All of these s-boxes are listed in tables below.

S-box S_1

| S_1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|-------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 0 | 14 | 04 | 13 | 01 | 02 | 15 | 11 | 08 | 03 | 10 | 06 | 12 | 05 | 09 | 00 | 07 |
| 1 | 00 | 15 | 07 | 04 | 14 | 02 | 13 | 01 | 10 | 06 | 12 | 11 | 09 | 05 | 03 | 08 |
| 2 | 04 | 01 | 14 | 08 | 13 | 06 | 02 | 11 | 15 | 12 | 09 | 07 | 03 | 10 | 05 | 00 |
| 3 | 15 | 12 | 08 | 02 | 04 | 09 | 01 | 07 | 05 | 11 | 03 | 14 | 10 | 00 | 06 | 13 |

S-box S_2

| S_2 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|-------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 0 | 15 | 01 | 08 | 14 | 06 | 11 | 03 | 04 | 09 | 07 | 02 | 13 | 12 | 00 | 05 | 10 |
| 1 | 03 | 13 | 04 | 07 | 15 | 02 | 08 | 14 | 12 | 00 | 01 | 10 | 06 | 09 | 11 | 05 |
| 2 | 00 | 14 | 07 | 11 | 10 | 04 | 13 | 01 | 05 | 08 | 12 | 06 | 09 | 03 | 02 | 15 |
| 3 | 13 | 08 | 10 | 01 | 03 | 15 | 04 | 02 | 11 | 06 | 07 | 12 | 00 | 05 | 14 | 09 |

S-box S_3

| S_3 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|-------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 0 | 10 | 00 | 09 | 14 | 06 | 03 | 15 | 05 | 01 | 13 | 12 | 07 | 11 | 04 | 02 | 08 |
| 1 | 13 | 07 | 00 | 09 | 03 | 04 | 06 | 10 | 02 | 08 | 05 | 14 | 12 | 11 | 15 | 01 |
| 2 | 13 | 06 | 04 | 09 | 08 | 15 | 03 | 00 | 11 | 01 | 02 | 12 | 05 | 10 | 14 | 07 |
| 3 | 01 | 10 | 13 | 00 | 06 | 09 | 08 | 07 | 04 | 15 | 14 | 03 | 11 | 05 | 02 | 12 |

FAST NATIONAL UNIVERSITY
School of Computing
Spring 2021

S-box S_4

| S_4 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|-------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 0 | 07 | 13 | 14 | 03 | 00 | 06 | 09 | 10 | 01 | 02 | 08 | 05 | 11 | 12 | 04 | 15 |
| 1 | 13 | 08 | 11 | 05 | 06 | 15 | 00 | 03 | 04 | 07 | 02 | 12 | 01 | 10 | 14 | 09 |
| 2 | 10 | 06 | 09 | 00 | 12 | 11 | 07 | 13 | 15 | 01 | 03 | 14 | 05 | 02 | 08 | 04 |
| 3 | 03 | 15 | 00 | 06 | 10 | 01 | 13 | 08 | 09 | 04 | 05 | 11 | 12 | 07 | 02 | 14 |

S-box S_5

| S_5 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|-------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 0 | 02 | 12 | 04 | 01 | 07 | 10 | 11 | 06 | 08 | 05 | 03 | 15 | 13 | 00 | 14 | 09 |
| 1 | 14 | 11 | 02 | 12 | 04 | 07 | 13 | 01 | 05 | 00 | 15 | 10 | 03 | 09 | 08 | 06 |
| 2 | 04 | 02 | 01 | 11 | 10 | 13 | 07 | 08 | 15 | 09 | 12 | 05 | 06 | 03 | 00 | 14 |
| 3 | 11 | 08 | 12 | 07 | 01 | 14 | 02 | 13 | 06 | 15 | 00 | 09 | 10 | 04 | 05 | 03 |

S-box S_6

| S_6 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|-------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 0 | 12 | 01 | 10 | 15 | 09 | 02 | 06 | 08 | 00 | 13 | 03 | 04 | 14 | 07 | 05 | 11 |
| 1 | 10 | 15 | 04 | 02 | 07 | 12 | 09 | 05 | 06 | 01 | 13 | 14 | 00 | 11 | 03 | 08 |
| 2 | 09 | 14 | 15 | 05 | 02 | 08 | 12 | 03 | 07 | 00 | 04 | 10 | 01 | 13 | 11 | 06 |
| 3 | 04 | 03 | 02 | 12 | 09 | 05 | 15 | 10 | 11 | 14 | 01 | 07 | 06 | 00 | 08 | 13 |

S-box S_7

| S_7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|-------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 0 | 04 | 11 | 02 | 14 | 15 | 00 | 08 | 13 | 03 | 12 | 09 | 07 | 05 | 10 | 06 | 01 |
| 1 | 13 | 00 | 11 | 07 | 04 | 09 | 01 | 10 | 14 | 03 | 05 | 12 | 02 | 15 | 08 | 06 |
| 2 | 01 | 04 | 11 | 13 | 12 | 03 | 07 | 14 | 10 | 15 | 06 | 08 | 00 | 05 | 09 | 02 |
| 3 | 06 | 11 | 13 | 08 | 01 | 04 | 10 | 07 | 09 | 05 | 00 | 15 | 14 | 02 | 03 | 12 |

S-box S_8

| S_8 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|-------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 0 | 13 | 02 | 08 | 04 | 06 | 15 | 11 | 01 | 10 | 09 | 03 | 14 | 05 | 00 | 12 | 07 |
| 1 | 01 | 15 | 13 | 08 | 10 | 03 | 07 | 04 | 12 | 05 | 06 | 11 | 00 | 14 | 09 | 02 |
| 2 | 07 | 11 | 04 | 01 | 09 | 12 | 14 | 02 | 00 | 06 | 10 | 13 | 15 | 03 | 05 | 08 |
| 3 | 02 | 01 | 14 | 07 | 04 | 10 | 08 | 13 | 15 | 12 | 09 | 00 | 03 | 05 | 06 | 11 |

In this assignment, your task is to implement these s-boxes in Assembly language as a subroutine and share its code.