# INTE2401/2402 Lab 3

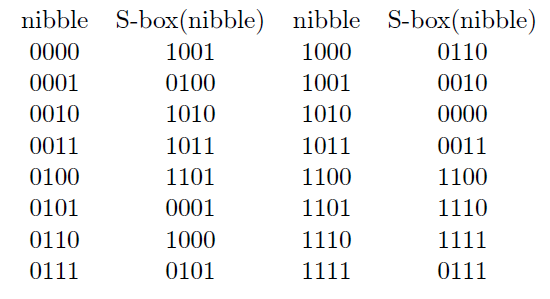
Student ID: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

In this week’s lab, we implement some building blocks of simplified AES with JavaScript. Our two tasks are implementing the protocols of substitution over nibbles and the mix columns, respectively. Noted that our philosophy is based on the **16-bit simplified AES**, namely, the input nibbles are 4-bit long. In addition, in the Task 2 (mix columns), we resort to the lookup table to obtain the result of polynomial multiplication. The lookup table is provided in this question sheet.

As usual, you may use Notepad(or other text editor) to write a JavaScript file with the extension name **.html** and then open it with Internet Explore(or other web browser).

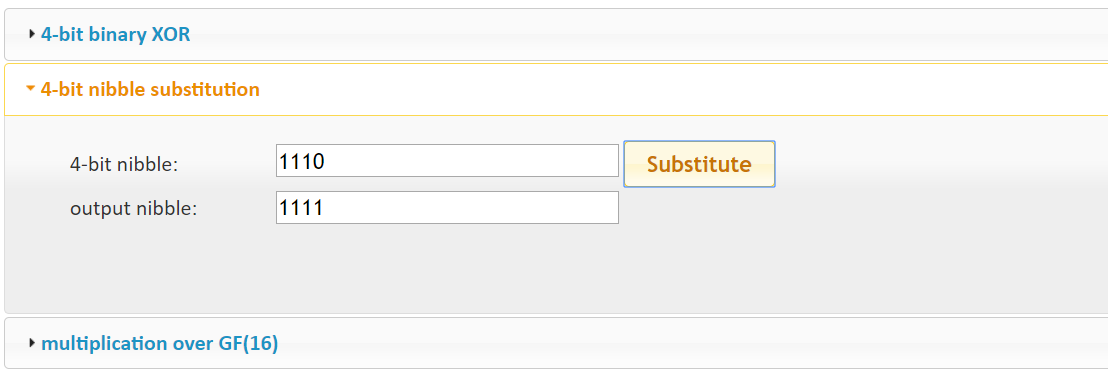
## Task 1. Implementation of Nibble Substitution based on Simplified AES

In the sense of Simplified AES, each nibble is a 4-bit binary value. The substitution is used to translate original nibble into new nibble based on the following lookup table of S-box.



Q1. Implement the substitution algorithm of a 4-bit binary number based on the protocol shown above.

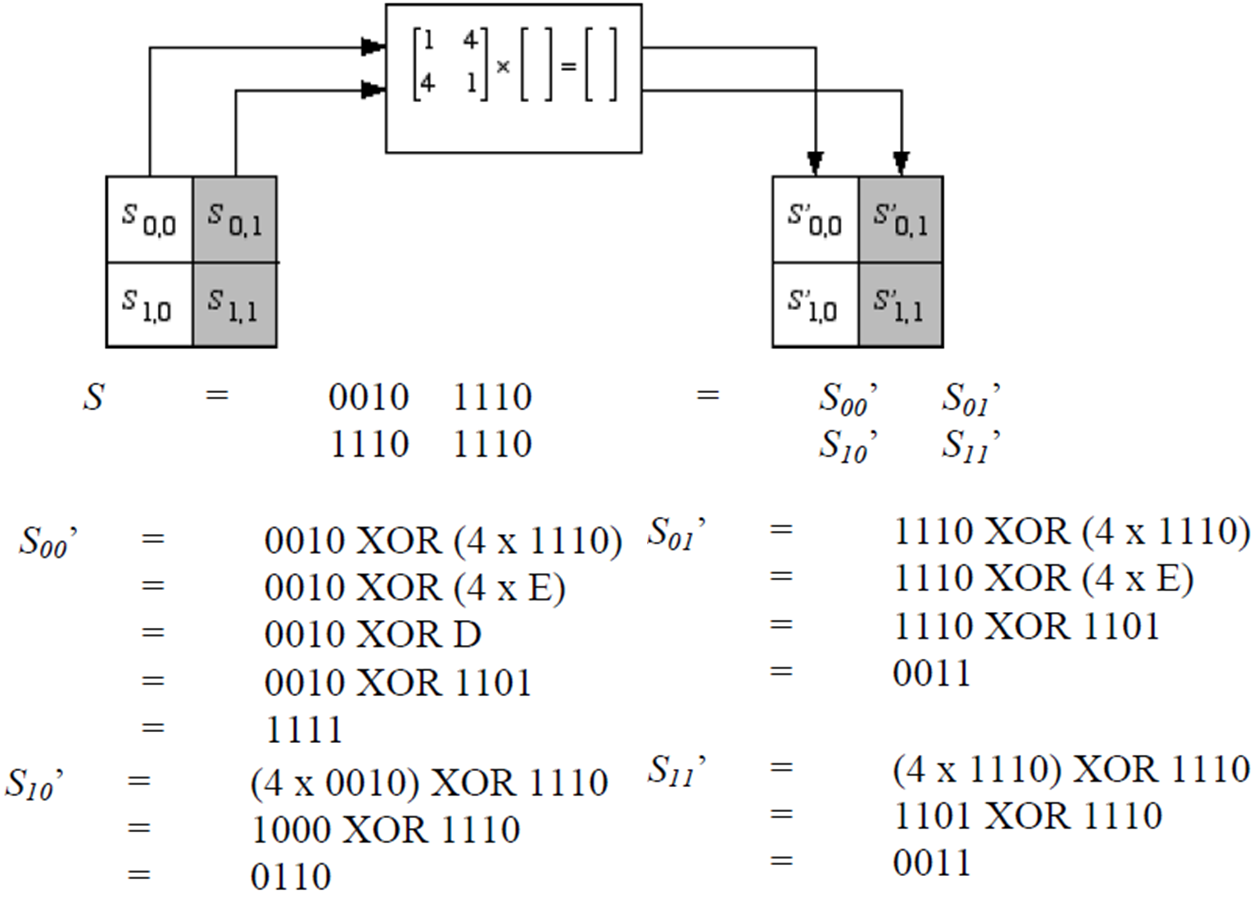
Sample form:



## Task 2. Implementation of Mix Columns

In this task, we try to implement the mix columns protocol of Simplified AES. First, let’s review the protocol based on the lecture’s slides.

1. Given a 16-bit binary input, we first split it to four 4-bit binary nibbles S0,0, S0,1, S1,0, and S1,1, and combine the nibbles as a matrix S= .
2. Given a constant matrix M=, afterward, we apply matrix multiplication with S and M using GF(16). For GF(16), the addition operation is simply an XOR, and for the multiplication operation is the **polynomial multiplication**.
3. Finally, we convert the result matrix S’= to binary string and then output it.



Having laid the protocol of mix columns above, now we use JavaScript to implement it. Noted that, the addition operation is simply an XOR operation.

For the multiplication operation, you can use the following lookup table. For example, 4\*1110=4\*E=D=13=1101.



Q2. Implement the mix columns algorithm of a 16-bit binary number based on the protocol shown above.

Example input: 0010 1110 1110 1110

Expected output: 1111 0011 0110 0011

Sample form: 