# INTE2401/2402 Lab 7

In this lab, we aim to design a webpage encrypting/decrypting text files (.txt) and generate the hash-based message authentication code with the Stanford JavaScript AES library. The Stanford JavaScript AES library can be downloaded at (<https://github.com/bitwiseshiftleft/sjcl/blob/master/sjcl.js>). User guide is provided at (<http://bitwiseshiftleft.github.io/sjcl/doc/>).

Q. Implement a JavaScript program of text files encryption and decryption with AES by using Stanford JavaScript AES library, including the following steps.

1. Design an webpage for the functions below;
2. Read a local text file (.txt) and display the content;
3. Input an 128-bits AES key in hexadecimal format (32 hexadecimal digits), encrypt/decrypt the file with the key, and display the encrypted file content;
4. Input an message, and generate the hash-based message authentication code;
5. Display the encrypted file, message authentication code;
6. Save the encrypted file and message authentication code as a new file in local.

Sample webpage:

