HW2 of Introduction to Information Security 2015

1. Implement DES. (Please don't call the existing library, implement it by yourself!)

2. Use your DES as the encryption and decryption (加解密都要) in ECB, CBC, OFB and CTR modes. Do the cipher on both R.G.B arrays separately and continuously (1.將 RGB 分開後，各自加解密; 2.不管 RGB，將讀入的資料連續取 64bit 來加解密). Please ignore the header information (標頭檔不用加解密). Test your code with the bmp file attached in moodle and save the results (bmp file) of the block cipher modes. (That means you have to learn how to read/write bmp file.)
   In addition, record the execution time of each block cipher modes.
   This website may help you with handling bmp files
   http://olife.iteye.com/blog/1028198

   If you can use the parallel computing skill in the models, you will get extra points. (Parallel computing is introduced by operation system class in the 3rd year, if you are freshman or sophomore, it's ok to ignore this part.)

   Please upload your result (doc or pdf file) to moodle and do the registration with your student ID as the account of this website (http://git.connectivity.tw/), then create the group with your partner and upload your code to this website.

Student assistant will test your code with the following parameters:
KEY: 1010111110101111101011111010111110101111101011111010111110101111 (10101111*8)
IV: 1111101011111010111110101111101011111010111110101111101011111010 (11111010*8)
and the attached bmp file.