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 in ECB, CBC, OFB and CTR models. Test your code with the bmp file attached in moodle and save the results of the encryption models. (That means you have to learn how to read/write bmp file.) In addition, record the execution time of each encryption model.
   This website may help you with handling bmp files
   http://olife.iteye.com/blog/1028198

   If you can use the parallel computing skill in CTR model, 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.)

Student assistant will test your code with the following parameters:
KEY: 1010111110101111101011111010111110101111101011111010111110101111 (10111111*8)
IV: 1111101011111010111110101111101011111010111110101111101011111010 (11111010*8)
and the attached bmp file.