CS381 Exercise 4

Name: Zhang Yupeng
Student ID: 5130309468

1. Let M' be the bitwise inversion of M. Prove that, for DES， if $Y = E_k(X)$, then $Y' = E'_k(X')$ (Hint: $(A \bigoplus B)' = A' \bigoplus B$.)

A	B	$A \bigoplus B$	$(A \bigoplus B)'$	$A' \bigoplus B$	$A' \bigoplus B$
0	0	0	1	1	1
0	1	1	0	0	0
1	0	1	0	0	0
1	1	0	1	1	1

We can see the table above, if the plaintext and key for an encryption are complemented, then the inputs to the first XOR are also complemented. The output, then, is the same as for the uncomplemented inputs. Further down, we see that only one of the two inputs to the second XOR is complemented, therefore, the output is the complement of the output that would be generated by uncomplemented inputs.

2. prove that for DES, if key k is all 0, then $E_k = D_k$. Can you find a method to avoid this problem?
For the F function of DES, $F(R_n, K_{n+1}) = 0$
We have:

$$L_{n+1} = R_n, R_{n+1} = L_n \bigoplus F(R_n, K_{n+1}) = L_n \bigoplus 0 = L_n$$

Thus

$$L_{n+2} = R_{n+1} = L_n; R_{n+2} = L_{n+1} = R_n$$

Therefore,

$$L_{16} = L_0; R_{16} = R_0$$

So, the encryption is all the same as the decryption.
To avoid the case, we should use strong key instead of this very weak key.