Name:Chao Jiang
ECE5563 — Spring 2015 **HW 2** Due: Feb. 3

Problem 3.1b

In that same discussion, it was stated that for the ideal block cipher, which allows all possible reversible mappings, the size of the key is $n \times 2^n$ bits. But, if there are $2^n!$ possible mappings, it should take $\log_2 2^n!$ bits to discriminate among the different mappings, and so the key length should be $\log_2 2^n!$. However, $\log_2 2^n! < n \times 2^n$. Explain the discrepancy.

It seems to be not reasonable at first glance, but when after deeply thought about it, we find that if the key length is $\log_2 2^n!$ bits. assign each mapping a number, from 1 to $2^n!$ and maintain a table that shows the mapping for each such number. This is not convenient for use in practical, because if the n is small, it's vulnerable to a statistical analysis of the plaintext; if n is sufficiently large to mask the statistical characteristics of the source plaintext, then the table becomes huge. So we define the key consist of the ciphertext value for each plaintext block,it means that from the key we can know the mapping, so the huge table is not needed.