差分分析：

思路：对于 8 位的输入，有 256*256 大小的差分表，有 256 种输入差分和输出差分，分别对每种{△X,△Y}对计数，计入差分表中。

线性分析：

思路：对于每一个 8 位的输入，有 0 个 xi 到 8 个 Xi，共 256 种的组合方式参与 X⊕Y=0 的运算，相应的，Y 也有 256 种选中。因此，对每个输入 X，Xi 与 Yi，共 256*256 种的异或结果进行统计，异或结果为 0 的，在表项中+1，总共有 256*256*256 次计数。最后，把每项减去 128。

作业二： Why a final key mixing is required by a cipher?

如果没有及经过最后一轮 keymixing，攻击者可以直接通过 Sbox 后的输出，推测出上层的输入。