1、代码思路：

x'=(x1,x2…) ,x''=(x1'',x2''…)对应于 **y'=(y1,y2…), y''=(y1'',y2''…)**

x'^x''=*x; y'^y''=*y

差分分析：计算所有可能的***x** 的值（通过遍历所有（**x',x''**）对），以及相应的***y**（通过查找 **S** 盒），然后将结果记录入表中得到 **DDT**

线性分析：遍历所有可能的 **xi^yj=0(i,j=1～n** 中的任意几个**)**式子，然后每个式子遍历整个 **S** 盒得到这个式子**=0** 的概率并记录入表中得到 **LAT**

2、最后一轮中的 **key mixing** 不能去掉是因为 **S** 盒是可逆的，如果没有 **key mixing** 做保护可以直接通过 **S** 盒的输出逆向得到 **S** 盒的输入，这样最后一个 **S** 盒也失去了意义，相当于整个加密体系少了一轮加密，密码的强度降低了。