# cryptology homework3

zhanxix

**1. Compute the DDT and LAT tables of ZUC S0 and S1.**

代码见：Compute_DDT_and_LAT_table.cpp

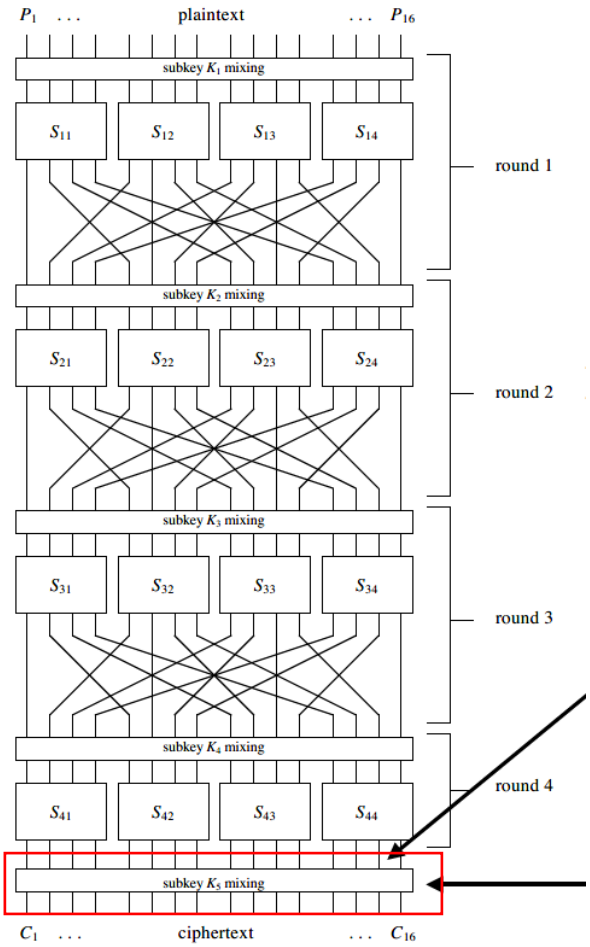
因为不确定自己的算法是否正确，因此首先使用了老师上课 PPT 上面所用的 Basic SPN 的 S 盒进行测试，即函数 test_Compute_DDT 和函数 test_Compute_LAT。

输出的差分分布表为 DDT-testS.txt，线性分布表为 LAT-testS.txt。通过比对，发现计算正确。

接下来，用与 test 相同的方法（不过由于 S 盒大小不同，因此做了些许修改）计算了祖冲之密码的 S0 盒和 S1 盒的相应表，即函数 Compute_DDT 和 Compute_LAT。

S0 的差分分布表为 DDT-S0.txt，线性分布表为 LAT-S0.txt。S1 的差分分布表为 DDT-S1.txt，线性分布表为 LAT-S1.txt。

**2. Answer why a final key mixing is required by a cipher (you can take Basic SPN as an example) ?**




如图所示，之所以需要最后一轮的密钥混合（轮密钥加），是因为：如果没有这最后一

轮的密钥混合（图中箭头所指，红框部分），那么攻击者就能直接得到最后一轮 S 盒的输出。那么唯一的非线性组件 S 盒就暴露在攻击者面前，攻击者可以在不知道密钥的情况先直接开始对最后一轮的解密。

因此，如果不进行最后一轮的密钥混合，最后一轮就形同虚设，相当于加密轮数少了一轮。