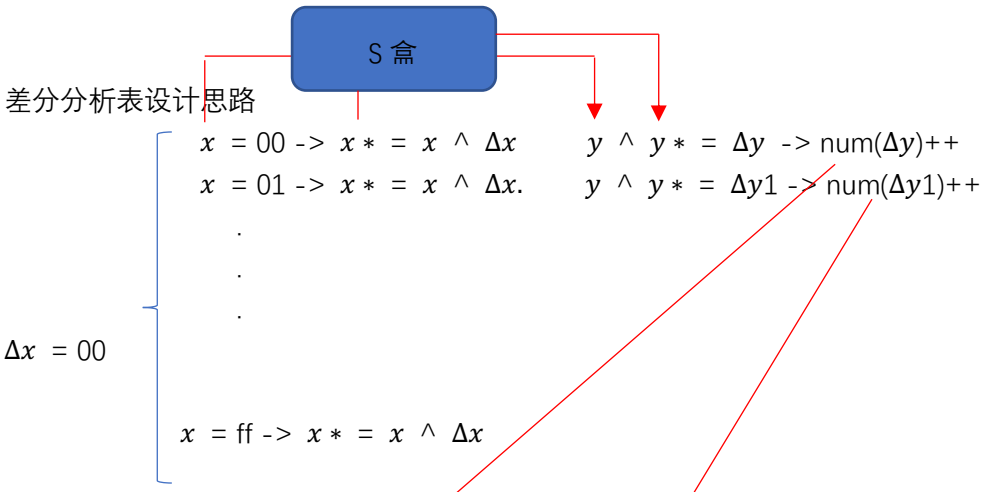
1901210447 刘嘉欣 第三次作业

1. 差分分析表设计思路



Δx \ Δy	00	01	…					fe	ff
00		num(01)							

Δx = 02

.

.

.

Δx = ff

如此将Δx从 0 遍历到 255，对每一个Δx，可以计算出 255 个Δy，对应于 DDT 表的每一项。每一轮Δx可以完成表项的一行。

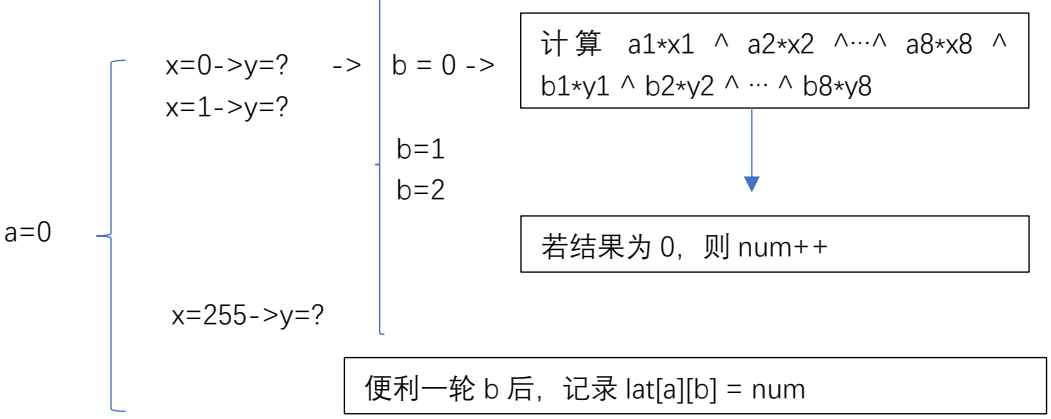
2. 线形分析表设计思路

构造多项式：

a1*x1 ^ a2*x2 ^…^ a8*x8 = b1*y1 ^ b2*y2 ^ … ^ b8*y8

其中 x1x2…x8 位为八位数字 x 的每一位，a，b，y 同

对于每一个 a，有 255 对 x，y；而对于每一对 x，y，有 b(0,255)：



a=1

a=255

对于每一个 a 从 0 遍历到 255，每一轮遍历下来完成 LAT 表的一行。

3. 为什么最后需要异或轮密钥

这是为了消除明文的统计特征。若没有这一步，攻击者得到密文后便可通过 s 盒，利用差分分析或者线性分析解密，使得密码更容易被破解。