Doctored Dobbertin v2

本题主要考查选手对可调分组密码分析方法的掌握程度以及阅读论文能力。

题目描述

题目中实现了一个10轮可调AES算法，即加密函数的输入除了明文以及密钥外，还有一个额外的输入称作tweak。

服务端随机生成密钥、明文、tweak，随后进行一次加密作为挑战，接着客户端可以选取明文、tweak获取相同密钥的加密结果，接着服务端公布挑战密文和所用到的tweak，客户端需要恢复明文，即可获取flag。

求解思路

通过比对，不难发现，与hacklu CTF 2023中的原题“Doctored Dobbertin”相比，本题中修改的常量包含S盒、P盒以及常数，而选择明文攻击的次数由7次减少为1次。常规的线性、差分等手段往往需要更多数据，因此考虑其他特殊方法。

如果搜索“可调分组密码后门”，可以发现相关论文，而本题的攻击方法取自第5节。 当然求解本题并非必须阅读原论文，有经验的选手会发现题目轮常数的修改显得非常可疑：每一轮加密中，会将常数以及tweak分别加到内部状态上，那是否存在一个tweak，其满足每一轮派生出来的轮tweak与轮常数相加后刚好抵消？答案是肯定的，经过分析，可以找出来该tweak数值为 `0x846a51a2787d09d057b2bfa8a3481dae` 。接着，我们只需要发送全0的明文，最后一次轮密钥加之前，我们知道内部密文的第1/3列必然相等，2/4列必然相等，而最后一轮的轮密钥恰好有一半为0，因此我们可以提取出8个非0密钥字节，进而可以确定主密钥中的8个字节，最后只需要枚举主密钥剩下的2字节即可。