实验四-AES

【实验目的及要求】

1、 通过本次实验，熟练掌握 AES-128 加解密流程；

2、 了解 AES-192 与 AES-256 加解密流程；

3、 了解 S 盒的生成原理；

4、 通过尝试 AES 的攻击，了解常用的攻击方法；

5、 必做部分需要给出 AES 算法的流程图和伪代码。

【实验步骤】

在完成必做项的基础上，从选做项任选若干项完成。

注：1）编程实现密码算法需同时实现加密和解密；

2）之后实验中可能会需结合 AES 算法实现工作模式，建议留出调用接口。

（一）必做

（1）利用有限域上的计算，编程实现 AES 的 S 盒和逆 S 盒，即给定一个 S 盒的输入，通过有限域的计算而非查表，计算出 S 盒的输出，或者通过计算得到整个 S 盒的表。

（2）使用（1）中输出的 S 盒编程实现 AES-128 加解密（包括加密函数、解密函数、密钥扩展函数）。

（二）选做

1、难度：一般

（1）编程实现 AES-192 与 AES-256 加解密（可用一个循环判断密钥长度然后扩展，没必要分开写三个文件，请注意部分密钥扩展的不同）。

2、难度：困难

（2）根据参考文献【1】第 2 节，编程实现 AES 的差分错误攻击（故障注入攻击）（选做该题时需要在报告中写出这种攻击方式的原理、过程以及流程图）。

【思考题】

1、比较 AES 与 DES 的异同，AES 相比于 DES 有哪些改进。

2、（选做）破解不包含 S 盒的 AES（即不做字节代替），并使用伪代码或者代码给出破解流程

TIPS:

① 考虑除 S 盒外的计算有什么样的代数特征。

② 利用这样的代数特征，考虑能不能换一种方式对行移位和列混淆进行表示。

③ 考虑在这样的攻击下至少需要多少组明密文对才能执行攻击。

【实验报告】

1、 实验布置两周内，请同学们将实验报告提交至0J平台对应位置，逾期者酌情扣分；

2、 对于每个算法，报告中应含有函数调用关系图、测试样例及运行结果截图，部分算法需要流程图/伪代码；并且记录自己本次实验的收获感想，和对实验不足之处的建议；

3、 报告格式见附件二；且该格式仅供参考，同学们可酌情更改。

4、 请注意：所有实验中，并不是做困难难度的实验的难度系数一定高于难度为中等；**难度系数由实验自身难度和具体实现情况以及程度决定；**如果只能敷衍完成，同学们不如选择在更简单的选做题上创新。

【参考文献】

[1]孙维东,俞军,沈磊.对称加密算法 AES 和 DES 的差分错误分析[J].复旦学报(自然科学版),2013,52(03):297-302.