实验五-SM4 及工作模式

【实验目的及要求】

1、 通过本次实验，熟练掌握 SM4 加解密流程;

2、 通过本次实验，了解并掌握各种工作模式；

3、 感受工作模式与填充方式对安全性的意义。

【实验步骤】

本次实验内容没有选做题，均为必做。

（1） 实现 SM4 算法。

（2） 使用 SM4 算法加密算法以及 PKCS#7 填充，基于 ECB 模式完成加解密。

（3） 使用 SM4 算法以及 PKCS#7 填充，基于 CBC 模式完成加解密。

注：CBC 模式完成 SM4 算法加解密需要给出流程图和伪代码。

（4） 使用 SM4 算法，基于 CTR 模式完成加解密。

（5） 使用 SM4 算法，基于 CFB 或 OFB 模式完成加解密。

注：关于 SM4 算法，详情请见附件 1。

【思考题】

1、请分析在使用 SM4 算法进行加密时，轮函数在各个阶段的运行时间占比。

2、SM4 算法与 DES、AES 算法相比有什么异同？

3、（选做）分别使用 ECB 模式和 CBC 模式加密一个 bmp 图片，观察加密后的图片文件的特征，并结合工作模式的特点说明产生该现象的原因。只需要给出加密后的图片结果以及分析即可。

注：对于 bmp 图片文件，其前 54 字节包含了图片的头信息。因此，需要拼接原图片的前 54 字节与加密后图片第 55 字节开始的所有字节，构成一个合法的 bmp 图片文件。

【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。