实验三 - DES

【实验目的及要求】

1. 理解Fesitel结构及DES算法的原理，并掌握加解密流程；
2. 了解弱密钥与半弱密钥；
3. 对算法进行深入理解和思考，开始尝试算法的优化与改良；
4. 必做部分DES算法的实现需要给出流程图和伪代码。

【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。

（一）必做（**需要给出流程图和伪代码**）

1、编程实现DES算法。要求对于给定密钥，可以正确实现加密与解密；

2、编程实现三重DES算法(EDE)，使用双倍密钥进行加解密。

（二）选做

1、（难度：中等）找出所有的弱密钥与半弱密钥；

**弱密钥**：若给定初始密钥，经密钥生成，有，则称K为弱密钥；

**半弱密钥：**若给定初始密钥和，两个密钥生成的子密钥对称，则称和为一组半弱密钥；

请**思考**弱密钥和半弱密钥的特殊性质给明密文之间的关系带来了什么特点，在实验报告的“测试样例及结果截图”部分通过加（解）密运算来验证这些密钥的正确性。**并在实验报告中详细说明你的算法原理和（半）弱密钥的危害。**

2、（难度：困难）对DES算法进行优化（如时间上、空间上）；

**注意：**需进行横向（与必做结果相比）对比与纵向（标准参考 **650 Mb/s** ）对比；

另外所提供论文仅供参照，希望同学们可以发散思维，创新思考。**此部分需要在实验报告中详细说明你的优化思路，并附上你的加解密速度以及测试环境。**

* “一种优化DES算法\_陈良.pdf”“DES算法软件速度优化的实现\_郑焰.pdf”内容主要围绕结构与速度的优化，如SP盒合并、比特切片、硬件上的优化；
* “基于DES算法的系统优化设计\_付秀伟.pdf”内容围绕DES算法的安全性缺陷进行了优化，有兴趣的同学可以思考学习。

【实验报告】

1、 实验布置两周内，请同学们将实验报告提交至OJ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、 请详细阅读附件中有关代码和实验报告的要求部分，报告格式见附件，且该格式仅供参考，同学们可酌情更改；

4、 以下思考题若无选做说明，均应体现在报告中。

【思考题】

1. 目前对于DES的密码分析都做了哪些工作，有什么成果。

2. DES为何不再适用于现代。