实验1 分组加密方法的研究与使用

1. **实验目的**
2. 理解对称加密算法中的5种分组模式。
3. 掌握不同分组模式的特点。
4. 基于C++、Java或.net中成熟的对称加密库实现多种对称加密算法模式。
5. **实验预备知识及实验环境搭建**
   1. **实验预备知识**
6. 分组密码的基本原理：查阅文献，了解分组密码的几种基本分组模式。
7. 编程库的调用：了解C++、Java或.net等常用语言或框架下对于编程库的调用，掌握一种语言环境下调用编程库的方法，能够在现实环境中调用编程库。
   1. **实验环境搭建：**

选定一种编程语言或框架，搭建完整的开发环境。选定一种对称加密算法，并在开发环境中设置对于该加密算法的库引用，引用的形式可能包括头文件、静态/动态链接库等。

1. **实验要求与内容**
   1. **分组密码的基本原理**

**实验内容**

查阅文献，并对分组密码的基本原理、5种分组密码的分组模式加以叙述。

**实验要求**

要求详细叙述以下内容：

1. 分组密码的基本原理。
2. 5中分组模式的介绍，绘制各种模式的原理图，并采用表格形式对比5种分组模式的优缺点。

在报告中，需要在采用文献的位置标明参考文献序号，并在实验报告的最后列出文中所引用的所有参考文献。参考文献的标注及引用方式要求采用国家标准GB/T 7714-2015《文后参考文献著录规则》的格式。实验报告中的参考文献标注要求采用上标形式，如“张三等[1]提出了一种更为快速的加密方法，该方法通过降低随机数的生成数量提高了数据的加密效率……”参考文献的序号按文献标注在实验报告中的自然先后顺序依次增加。

要求此处引用的文献数量不少于2篇。

* 1. **环境搭建说明**

**实验内容**

选定一种语言或框架，搭建完整的开发环境。选定一种对称加密算法，寻找该算法在该语言中的一个较为成熟的算法库实现。在开发环境中设置该加密库的引用，完成程序的实现准备工作。

**实验要求**

要求完成以下内容：

1. 选定一种语言或框架，搭建完整的开发环境。要求该环境必须能够顺利完成代码的开发、调试和编译。要求描述所选定的语言，并简要说明选择该语言的原因。
2. 选定一个加密算法库，要求该算法库必须包含所选定加密算法的一种实现，并能够设置其按照不同的分组模式完成加密操作。要求在实验报告中明确给出该加密算法库的函数原型，并指出其中设置分组模式的参数。
   1. **加密及解密程序的实现**

**实验内容**

采用上节所搭建好的开发环境，引用上节选定的加密算法库，采用全部5种分组模式完成一个加密及解密程序。

**实验要求**

要求完成以下内容：

1. 实现一个加密/解密程序。要求该程序采用实验报告前述章节选定的语言和加密算法。
2. 要求程序从当前目录（程序所在目录）的plaintext1.txt和plaintext2.txt文件中读取原始明文。
3. 要求程序从当前目录的password.txt文件（加密密码）中读取密码。
4. 要求分别对明文文本实施不同模式的加密，并将加密后的密文分别存储到ciphertext-ecb.txt、ciphertext-cbc.txt、ciphertext-cfb.txt、ciphertext-ofb.txt、ciphertext-ctr.txt中（对应不同的明文，应添加编号）。
5. 要求程序能够执行解密算法，从各个ciphertext-\*.txt文件中读取密文文本，从password.txt文件（解密密码）中读取密码，进行解密，并在控制台或文本框中输出得到的明文。得到的明文同时存储至result-\*.txt文件中。
6. 要求将加密算法与解密算法分别封装到两个子函数中。
7. 要求程序运行后自动进行明文载入、密码载入、明文加密、密文存储、密文解密、解密后明文结果输出的步骤。
8. 要求在代码的关键步骤添加注释。整个程序的注释数量不得少于5处。
9. 要求提交程序的源代码、调用的库文件（列在源代码目录下）、编译完成的可执行文件、README.txt说明文档。全部文件存入文件夹下，打包为zip压缩包。
   1. **测试结果及分析**

**实验内容**

采用上节实现的程序测试加密及解密过程。

**实验要求**

要求完成以下内容：

1. 截图或采用规范的格式粘贴所采用的明文以及密码。
2. 运行程序。若程序包含界面或字符式交互过程，请截图并粘贴在实验报告中。
3. 程序执行结束后，对比5种加密分组模式得到的密文是否相同。
4. 程序执行结束后，对比输出的明文与原始明文是否相同。
5. 要求各实验步骤均进行截图记录。
6. 进阶步骤：尝试修改两个明文中的部分内容，或者修改各密文中的第二个分组，或者尝试使用不同密码对同样的明文进行加密，随后再次执行解密算法，观察得到的明文与原始明文的区别。