实验2 公钥密码算法的研究与使用

1. **实验目的**
2. 理解非对称加密算法的基本原理。
3. 了解现有RSA算法的原理以及椭圆曲线公钥密码算法的原理与优缺点。
4. 基于C++、Java或.net中成熟的RSA或SM2等加密库实现一个非对称加密解密算法程序。
5. **实验预备知识及实验环境搭建**
   1. **实验预备知识**
6. 公钥密码算法的基本原理：查阅文献，了解公钥密码算法的发展历史和现状，了解其加密与解密算法的基本原理。理解公钥、私钥、电子签名、数字证书等基本概念。
7. 常用非对称加密算法基本原理：查阅文献，列举常用的公钥密码算法及其优缺点。
8. 编程库的调用：了解C++、Java或.net等常用语言或框架下对于公钥密码算法编程库的调用，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此类编程库。
   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。选定一种公钥密码算法，并在开发环境中设置对于该公钥密码算法的库引用，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. **公钥密码算法加密与解密的基本原理**

**实验内容**

查阅文献，并对公钥密码算法加密与解密的基本原理加以叙述。

**实验要求**

要求详细叙述以下内容：

1. 公钥密码算法的发展历史、研究现状、应用现状
2. 解释公钥、私钥、电子签名、数字证书等基本概念。
3. 比较软件数字证书与硬件数字证书在安全性、易用性、可靠性等方面的异同。

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 7714-2005《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3篇。

* 1. **公钥密码算法的基本原理**

**实验内容**

查阅文献，并对几种常用的公钥密码算法的基本原理加以叙述。

**实验要求**

要求详细叙述以下内容：

1. 列举不少于两种公钥密码算法。
2. 说明以上列举的公钥密码算法的基本原理与优缺点。
3. 说明拟在实现中采用的公钥密码算法。

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 7714-2005《文后参考文献著录规则》的格式。

要求此处引用的文献数量不少于2篇。实验报告中的所有参考文献统一编号。

* 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。采用上节所选定的公钥密码算法，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上节所选定加密算法的一种实现。要求列出该算法库的出处，并简要介绍该算法库。
3. 在开发环境中设置对于加密算法库的引用。要求在引用设置的各个步骤进行截图，并粘贴到实验报告中。
   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，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plaintext.txt文件中读取原始明文。
3. 要求程序从当前目录的publickey1.txt、publickey2.txt文件（公钥）中读取公钥，从当前目录的privatekey1.txt、privatekey2.txt文件（私钥）中读取私钥。
4. 要求程序将加密后的密文文本存储到ciphertext.txt文件中。
5. 要求程序封装生成公私密钥对的方法。生成的公钥与私钥分别存储到以上指定的文件中。
6. 要求程序能够执行加密算法。从plaintext.txt文件中读取明文文本，并将加密后的密文存储到ciphertext.txt文件中。要求程序能够将加密密钥作为参数输入。要求程序既能够采用公钥作为加密密钥，也能够采用私钥作为加密密钥。
7. 要求程序能够执行解密算法，从ciphertext.txt文件中读取密文文本，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。要求程序能够将解密密钥作为参数输入。要求程序既能够采用公钥作为解密密钥，也能够采用私钥作为解密密钥。
8. 要求将加密算法与解密算法分别封装到两个子函数中。
9. 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。
10. 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。
11. 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. 调用程序的公私密钥对生成方法，观察多次生成的公私密钥对是否相同。记录和保存最后两次生成的公私密钥对，分别存储到publickey1.txt/privatekey1.txt与publickey2.txt/privatekey2.txt文件对中。
4. 采用第1对密钥对中的私钥进行加密，观察得到的密文是否与原始明文相同；采用第1对密钥对中的公钥进行解密。观察得到的明文是否与原始明文相同。
5. 采用相同的明文和密码再次执行上述步骤，观察多次执行的结果是否相同。
6. 采用第1对密钥对中的公钥进行加密，观察得到的密文是否与原始明文相同，同时观察此次得到的密文是否与前序实验步骤中采用私钥加密得到的密文相同；采用第1对密钥对中的私钥进行解密。观察得到的明文是否与原始明文相同。
7. 采用私钥1进行加密，而后采用公钥2进行解密，观察程序是否可以顺利执行，若能够顺利执行，观察得到的明文与原始明文是否相同。分析原因。
8. 类似以上步骤，采用公钥1进行加密，而后采用私钥2进行解密，观察程序是否可以顺利执行，若能够顺利执行，观察得到的明文与原始明文是否相同。分析原因。
9. 采用私钥1进行加密，而后采用私钥2进行解密，观察程序是否可以顺利执行，若能够顺利执行，观察得到的明文与原始明文是否相同。分析原因。
10. 要求各实验步骤均进行截图记录。