## 1 题目

古典算法实现文件加解密实验

## 课程设计要求

1.任务描述

利用古典算法对文本、图片、音频、视频等文件进行加解密运算

2.基本要求：

（1）复习有关古典密码体制的相关知识

（2）利用C语言设计可执行程序

1. 在设计过程中，要求设计至少两种的古典密码算法

2.课程设计题目

DES加密及解密算法

课程设计要求

1.理解体会加密算法在文件系统中的应用

2.加深对加密算法机器应用的理解

3.采用工具实现DES加密算法对文件进行加解密的基本概念与基本原理

4.用C语言实现

## 3课程设计题目

ECC加密解密的实现。

课程设计要求

（1）理解加密解密的基本思想

（2）理解 ECC加密算法的原理

1. 掌握上述加密解密算法的使用过程和实现方法

## 4课程设计题目

ECC加密解密的实现。

## 课程设计要求

（1）理解加密解密的基本思想

（2）理解 ECC签名算法的原理

（3）掌握上述加密解密算法的使用过程和实现方法

个人任务

1）字符转换

2）异常处理

3) ECC解密

## 5 RSA算法实现数字签名

1．对文件进行签名，生成一个独立于原文的签名文件；

2. 可以对文件进行签名，在文件后追加签名信息；

3．具有密钥管理的功能，比如私钥密钥和共享密钥的生成 ；

4．对私钥加密保护；

5．选择性功能：可以对 excel文档实施操作，设计一定的格式，对文档的内容进行签名，而签名的值也最终存放在 excel文档的特定标识后。说明：功能各方面越完善越好。

## 6题目

RSA短文本加密算法的实现（c语言）

## 课程设计要求

1、RSA算法实现数字签名的流程

2、对文件进行签名，生成一个独立于原文的签名文件；

3、可以对文件进行签名，在文件后追加签名信息；

4、具有密钥管理的功能，比如私钥密钥和共享密钥的生成 ；

5、对私钥加密保护；

6、选择性功能：可以对 excel文档实施操作，设计一定的格式，对文档的内容进行签名，而签名的值也最终存放在 excel文档的特定标识后。说明：功能各方面越完善越好

## 7.CA证书服务器的建立与使用--CA服务器的建立

## 课程设计内容

（1）掌握CA认证的知识，并能够使用证书完成用户身份的认证和通信过程中的安全保密。

1. 与同组同学分工合作完成设计内容。

## 8课程设计题目

利用古典算法（凯撒和维吉尼亚算法）对文本进行加解密

## 课程设计要求

（1）理解体会加密算法在文件系统中的应用

（2）加深对加密算法机器应用的理解

（3）至少使用三种古典加密算法

## 9.MD5算法短文本加密

## 课程设计要求

运用MD5算法实现对短文本的加密

# 10.课程题目：多功能加密应用软件

1.1课程设计目的

(1) 掌握密码学基础中古典加密体制的几种算法

(2) 了解并掌握古典加密算法的原理与实现

(3) 了解古典算法的特性及加解密规则

## **1.2 课程设计要求**

通过JAVA编程实现移位密码、仿射密码、维吉尼亚密码和置换密码。

# 11. CA证书服务器的建立与使用

# 12. 网络安全身份认证系统——登录及验证。

课程设计要求

登录时采用基于口令验证验证用户身份信息，采用哈希函数对用户口令进行验证，可用MD5算法或SHA-1算法，并调取数据库中的随机数生成新的散列值。

# 13. 利用DES算法对文本进行加解密运算

课程设计要求

（1）理解体会加密算法在文件系统中的应用

（2）加深对加密算法机器应用的理解

（3）分别采用不同工具实现DES加密算法对文件进行加解密的基本概念与基本原理

1. 用Java实现

## 14.课程设计题目

利用AES算法对文本进行加解密运算。

课程设计要求

（1）理解体会加密算法在文件系统中的应用。

（2）加深对加密算法机器应用的理解。

（3）分别采用不同工具实现DES、AES加密算法对文本进行加解密的基本概念与基本原理。

## 15课程设计题目

网络安全身份认证系统——注册

课程设计要求

采用哈希函数对用户口令进行验证可用MD5、SHA-1算法，并用随机数机制生成散列值，将注册信息加入数据库中，抵抗攻击者对数据库入侵以及用字典攻击破解密码。

## 16.课程设计题目

利用AES算法对文本文件进行加解密运算。

课程设计要求

（1）理解体会加密算法在文件系统中的应用。

（2）加深对加密算法机器应用的理解。

（3）分别采用不同工具实现AES加密算法对文本进行加解密的基本概念与基本原理。

（4）用JAVA 语言实现

## 17.安全的即时通讯软件(消息加解密)

课程设计要求

采用加密、数字签名技术对即时通讯软件的通信进行保护。

功能要求：

1）登录界面实现

2）聊天界面及基本通讯功能

3）采用DES加密算法对消息进行加解密

1.3 个人负责部分

实现安全即时通讯软件的加解密功能。

## 18. 题目：MD5文件加密软件

课程设计要求

运用MD5算法实现对文件的加密

## **19.题目**

**端口扫描软件（后台实现扫描及数据交互）**

课程设计要求

能够对本机或者网络安全进行设置和管理，比如可以扫描机器的漏洞，

可以存储端口扫描日志记录。

## **20．题目**

安全的即时通讯软件(即时通讯部分)

课程设计要求

采用加密、数字签名技术对即时通讯软件的通信进行保护。

功能要求：

1）登录界面实现；

2）聊天界面及基本通讯功能；

3）采用DES加密算法对消息进行加解密；

个人负责部分

实现安全即时通讯软件界面及相关聊天功能。

## 21 题目

**SHA加密算法**

1 课程设计要求

任务描述

使用编程语言（如：Java）实现SHA-1算法的软件系统设计。

具体要求：

　　1）理解SHA加密的基本思想

　　2）理解SHA摘要生成的原理

3）掌握上述SHA加密及摘要的生成实现方法

1.3 本人任务

1）在深入理解算法的基础上，设计一个完成对所输入信息加密的算法；

　　2）要求输入信息是ASCII码等，对所输入信息完成加密。

**22 SHA摘要算法**

任务描述

使用编程语言（如：c）实现SHA-1算法的软件系统设计。

具体要求：

　　 1）理解SHA加密的基本思想

　　 2）理解SHA摘要生成的原理

3）掌握上述SHA加密及摘要的生成实现方法

**23. 课程设计题目**

**网络攻击软件**（ARP实现）

**24. 课程设计题目**

**端口扫描日志文件的生成**

课程设计要求

能够对本机或者网络安全进行设置和管理，比如可以扫描机器的漏洞，

可以存储端口扫描日志记录。

**25课程设计题目**

RSA数字签名算法的实现(数字签名)

课程设计要求

1.掌握RSA算法的基本思路

2.理解数字签名的基本思想

3.掌握RSA数字签名算法的使用过程和实现方法

**题目26入侵检测系统（或嗅探器）**

**设计内容：**

实现一个入侵检测系统或者嗅探器

**功能要求**

1.具有嗅探功能。2. 能够对数据包进行过滤3. 能够分析数据包，甚至能够对系统日志进行检测和分析。4. 设定检测的规则，可以参考 snort 的规则。5. 可以根据用户自己设置的规则进行报警、记录、甚至响应。6. 能够生成入侵检测系统的日志，记录各种检测到的事件。

**题目27密钥管理系统**

**设计内容：**

设计一个密钥管理系统，可以完成密钥生成和管理，也可以存放自己平时用的各个网站的用户名密码。

**基本要求：**

密钥管理功能（1）可以生成随机数，用作对称算法的密钥（乃至生成大素数）；（2）可以生成公钥对，作为非对称算法的密钥；（3）密钥的加密保存和管理，并且添加必要的信息，比如这个密钥是加密哪个文件等，加密这些密钥一般采用口令，产生的 hash 值，截取相应长度的值作为密钥；（4）可以对密钥进行签名。（5）系统日志记录功能B 账户密码管理功能：可以存放用户名和密码，检测密码的安全性能，比如其长度是否短了，是否与用户名系统；

**题目28文件加解密实验**

**(1)设计内容：**

利用DES算法对文本、图片、音频、视频等文件进行加解密运算

**基本要求：**

（1）理解体会加密算法在文件系统中的应用

（2）加深对加密算法机器应用的理解

（3）分别采用不同工具实现DES加密算法对文件进行加解密的基本概念与基本原理

**题目29网络攻击防护软件**

**设计内容：**

选择一种或者几种病毒、木马以及各种攻击工具的攻击，设计相应的防护软件。

**功能要求**

自己针对相应的攻击和威胁进行设计，保证工作量和代码量，如果工作量不足，应当增加其他的攻击和威胁的防范，包括木马和反木马。

**题目30、安全数据库系统**

**设计内容：**

该系统实现一个安全的数据库系统，对数据库进行数字签名保证完整性，数据加密保证隐秘性。

**功能要求：**1．数据库的数据要进行加密；2. 对数据库的完整性进行保护；3．防止用户根据部分密文明文对，恢复数据库总密钥；4．数据采用一个密钥以某种形式衍生子密钥进行加密；5．保证密钥的安全性。说明：可以采用总密钥，根据 hash 函数，以及每一个数据的各种属性来产生子密钥，由于 hash函数的不可逆性，可以否则攻击者根据已知的部分密钥、明文密文对等来反推数据库的总密钥

**题目31、网络内容安全过滤系统**

**设计内容：**

设计针对邮件、网页以及文件进行过滤的软件。

**功能要求：**

对文本内容、url、网址、ip 进行过滤；2.可以自动去一些网址下载黑名单；3.软件本身设置一定的安全保护措施，防止被篡改、非法访问等；4.可以根据需要增加其他的过滤和功能设置，比如限时上网、超时下线、黑屏警告一些非法行为等。5.增加一定的自学习功能，通过非法信息的特征来升级特征库。

**题目32防伪认证码设计与实现(2人)**

**设计内容：**

设计一个防伪认证码生成器，可以在此基础上建立一个防伪认证网站。

**功能要求**

1. 具有不可逆性。2. 具有不可预测性。即不容易有意构造一个码属于防伪认证码系列。3. 抵抗生日攻击，具有稀疏的特征。4. 防止碰撞发生，即同样的防伪认证码出现。5. 在保证安全性的同时具有实用性，包括码长合理，不能太长。6. 防止根据已有的防伪认证码来预测，或者推测新的有效防伪认证码。