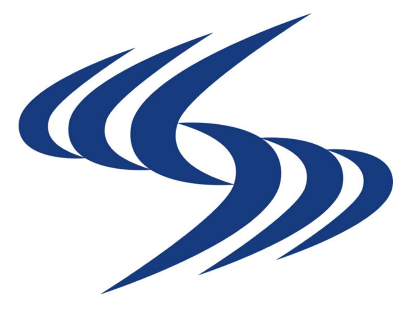
**信息安全工程实践2**

**任 务 书**

**A0802260030**

****

**东北大学软件学院**

**2024年11月**

# 一．概述

## 1．课程基本信息

**中文名称：**信息安全工程实践3

**英文名称：**Design and programming for Information Encryption/Decryption

**适用专业：**信息安全

**实践学时：**32学时

**学 分：**2.0 学分

**先修课程:** 信息安全数学基础、计算机引论（C语言）、计算机组成原理与体系结构、现代密码学与加解密技术

**课程进行方式：**校内实验室，学生上机为主，老师讲解为辅

## 2．课程目的

1. 通过实践使信息安全专业学生加深对密码学基本原理和加解密理论知识的理解。
2. 培养学生在计算机上实现不同类型加密、解密操作运算功能的能力。利用实现的典型加解密方法对输入明文或文件实施加密，并对密文或文件进行解密。能够实现基本的密钥分配方法。
3. 培养学生具备简单网络程序开发能力，能够在两个联网终端间进行消息加解密操作。
4. 通过参与信息加解密实践，提高学生的分析设计能力、开发过程的团队合作能力、组织管理能力和语言表达能力。

信息安全工程实践（三）能够使信息安全专业学生加深对密码学基本原理和加解密理论知识的理解。培养学生在计算机上实现不同类型加密、解密操作运算功能的能力。利用实现的典型加解密方法对输入明文或文件实施加密，并对密文或文件进行解密。能够实现基本的密钥分配方法。培养学生具备简单网络程序开发能力，能够在两个联网终端间进行消息加解密操作。通过参与信息加解密实践，提高学生的分析设计能力、开发过程的团队合作能力、组织管理能力和语言表达能力。

## 3．课程策略

1. 每个学生**必须**加入一个团队，完成一个系统的实现， 每个团队不得超过4人；
2. 每30人左右为一个班，指定一个指导教师；
3. 课程进行过程中遵照一个标准的软件开发过程进行分析、设计、开发和测试；
4. 指导老师指导学生完成系统开发过程中的各个关键活动，并且帮助学生解决在开发过程中出现的各种问题；
5. 指导老师根据学生的问题，对一些知识点或问题做重点讲解。

# 二．实践内容及要求

本实践对系统及开发工具不作任何限制，同学可以选择各自熟悉的系统和开发工具完成以下实践内容。

## 1．单机加解密实践

1）单表替代密码实现

从下面的四个单表替代密码中至少选择两个密码予以实现。

* Caesar cipher
* Keyword cipher
* Affine cipher
* Multiliteral cipher

2）多表替代密码实现

从下面的三个多表替代密码中至少选择两个密码予以实现。

* Vigenere cipher
* Autokey ciphertext
* Autokey plaintext

3）多图替代密码实现

* Playfair cipher

4）置换密码实现

从下面的三个置换密码中至少选择两个密码予以实现。

* Permutation cipher
* Column permutation cipher
* Double-Transposition cipher

5）流密码实现

从下面的两个流密码中至少选择一个密码予以实现。

* RC4
* CA

6）分块密码实现

从下面的两个分块密码中至少选择一个密码予以实现。

* DES
* AES

7）公钥密码实现

从下面的两个分块密码中至少选择一个密码予以实现。

* RSA

编写程序构造一RSA密钥；

编写程序实现快速指数算法；

编写程序生成大素数；

实现RSA密码体制。

* ECC（选做）

8）单向散列函数

* MD5（选做）

9) DH密钥交换过程实现

实现DH密钥交换过程，并通过实例演示此过程。

单机加解密实践最终应以统一界面展示，图1为参考界面，可根据此图自行设计功能更为丰富的展示界面。

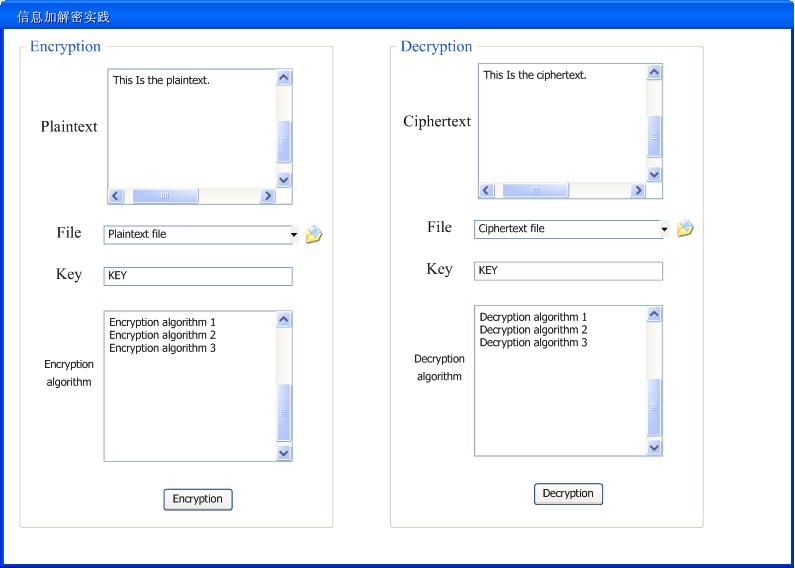


图1 单机加解密展示界面

## 2．双机加解密实践

1）双机通信实现

通过Socket编程实现双机通信功能，能够在两个终端间交换消息并传输文件。

2）双机加解密实现

将单机加解密实践的全部内容移植到双机环境中，其中一端为加密端，另一端为解密端。加密端界面设计可参考图2。

3）针对单机加解密1）-7）实现的密码，至少选择一个密码，使用DH在加密段和解密端间交换密钥。

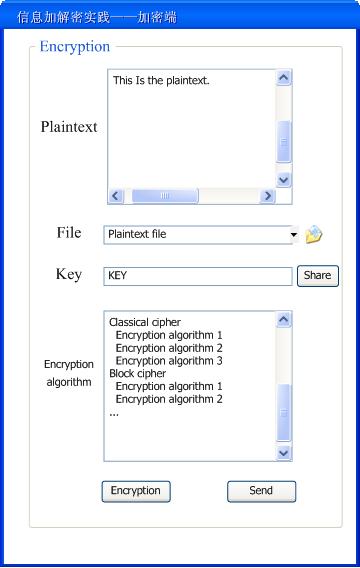


图2 加密端操作界面

解密端界面设计可参考图3。

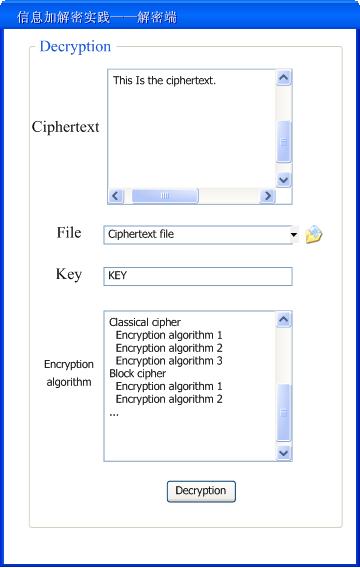


图3 解密端操作界面

# 三．实践计划

### 1 项目实践阶段说明

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 编号 | 任务名称 | 开始时间 | 结束时间 | 相关人员 | 提交成果 |
| 一．实践准备阶段（4学时） | | | | | |
| 1 | 实践内容和要求 | 2024-11-25 | 2024-11-25 | 所有指导老师和学生 |  |
| 2 | 学生分组 | 2024-11-25 | 2024-11-25 | 所有指导老师和学生 | 分组名单 |
| 二．项目实践阶段(24学时) | | | | | |
| 1 | 主体实践 | 2024-11-26 | 2024-12-4 | 项目组成员 |  |
| 三.验收阶段（4学时） | | | | | |
| 1 | 项目总结 | 2024-12-5 | 2024-12-5 | 指导教师  项目组成员 | 项目总结报告  可执行程序及源代码 |
| 2 | 答辩 | 2024-12-5 | 2024-12-5 | 指导教师  项目组成员 |  |

# 四．考核的方法和成绩的评定

### 1．最终成绩根据以下三个方面进行评定

出席情况：占20%

总结报告：占50％

答辩：占30％

### 2．验收结果的评定

在实践课结束的前两天，教师应组织学生验收设计的软件系统。验收采用答辩的方式进行。首先由组长对设计的内容进行讲解，讲解应主要介绍系统的功能、结构和小组成员承担的任务。然后教师可以提问的方式考核每一个小组成员相关问题，根据小组成员承担的任务量、完成任务的情况和回答问题的结果评定学生的验收结果。

### 3．实践总结报告

教师在课程结束后，可根据每个小组的分工情况具体查看学生实践总结报告的内容，根据设计文档的结构是否合理、文字组织是否通顺、图表是否规范和文档内容是否完整评定每个学生的这部分成绩。

### 4．特殊情况说明

小组组长成绩评定：可根据小组组长对整个项目组织的情况、承担的任务情况和小组开发的结果参考，对以上情况较好的小组，可考虑适当提高小组组长的成绩。

# 五．课程设计结果的提交

1. 项目组总结报告（一份、A4纸打印，同时包括一份电子文档）；
2. 答辩报告（制作PPT报告，电子方式提交），要求重点突出，思路清晰，同时就此报告准备答辩；
3. 可执行程序及源代码。

所有电子方式提交的文件全部存放在一个目录。

# 六．课程设计总结报告的格式

总结报告不得少于20页。

**课程编号：A0802260030**

信息安全工程实践2

总结报告



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **姓名** |  | **学号** | |  |
| **班级** |  | **指导教师** | |  |
| **实验名称** | **信息安全工程实践2** | | | |
| **开设学期** | **2024-2025秋季学期** | | | |
| **开设时间** | **第13周——第14周** | | | |
| **报告日期** | **2024年12 月14日** | | | |
| **评定成绩** |  | | **评定人** |  |
| **评定日期** |  |

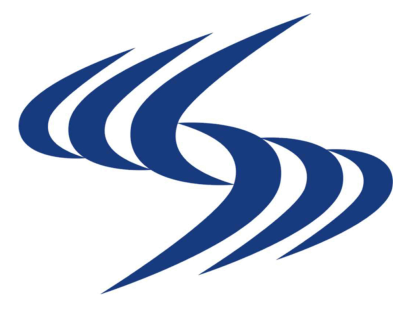
**东北大学软件学院**

1. 实践目的与意义
2. 实践环境
3. 项目组分工
4. 系统设计
5. 系统实现

六、 结束语

**附录：**

**《信息安全程序实践2》成绩评定表**



|  |  |  |  |
| --- | --- | --- | --- |
| **评价内容** | **具 体 要 求** | **分值** | **得分** |
|
| **报告质量** | **实验报告格式规范，符合要求；报告内容充实、正确，实验目的归纳合理到位。** | **20** |  |
| **平时表现** | **课程设计过程中，无缺勤现象，态度积极，具有严谨的学习态度和认真、踏实、一丝不苟的科学作风。** | **10** |  |
| **提交材料及实践验收成绩** | **能够按照规范提交课程设计要求的所有材料（要求在以“学号-姓名”命名的文件夹中，包含实验报告电子版和实验源代码等），材料完备，格式内容等符合要求。能够按实验要求合理设计并开发出程序，功能完整性强，原理及实验结果分析准确，归纳总结充分。答辩认真，清晰，分工明确。** | **60** |  |
| **创新性** | **对完成选做实践项目过程中有创新性。** | **10** |  |
| **总 分** | | |  |