

Chapter 8

开发环境要求

8.1 编译器

课程要求编译链接器使用 gcc，如果是 windows 操作系统，推荐使用 mingw-w64 13.2.0 版本以上。

关于 gcc 的介绍除了官网上的介绍外，推荐两个贴子：

- MinGW-w64 安装教程——著名 C/C++ 编译器 GCC 的 Windows 版本，网址：<https://zhuanlan.zhihu.com/p/76613134>
- 01.MinGW 下载及其安装，网址：https://blog.csdn.net/liujiahao_/article/details/144674808

8.2 编辑器

编辑器按照自己喜好选择，推荐使用 vs code，网址<https://code.visualstudio.com/>

8.3 作业提交

本课程使用 gitee 提交作业¹。

在课程开始首先要有 gitee 账号，通过教师发送的邀请链接加入课程组织，然后就可以 fork 编程练习的初始仓库，clone fork 到自己仓库的编程练习初始仓库到本地，修改相关的文件，如果有需要添加新的文件，依次执行 commit、push，更新自己仓库里的文件，在确定作业完成后，发起 pull request (pr)，老师看到你的 pr 后，会认为你的作业已经完成，会到你的仓库下载你本次作业的仓库，然后关闭你的 pr，根据你提交的内容进行评分。

编写的程序要能对错误的参数进行识别，并输出明确的提示信息，并进行合理的错误处理。

¹gitee 网站是<https://gitee.com/>

`pr` 表示你作业提交的动作，没有 `pr` 等同没有提交作业。

为了让同学们真正知道算法的具体实现，避免抄袭，我们会使用代码重复率检测工具对所有同学的代码进行检查，但是考虑到同学们会不可避免地使用大模型工具，所以我们将同学间的代码允许重复率设定在 35% 以下，此重复率不包含注释，当两个同学的代码重复率 $\geq 35\%$ 时，老师会现场从提交的代码中抽出几个功能模块，让学生现场编写，可以查看你计算机存的任何代码，但是不能上网查询。能够现场编写出来的，说明虽然使用的工具，但是知道如何编写，正常给分，不能现场编写出来的，此次作业为零分。

Chapter 9

实践类练习分值说明

实践类练习分为编程类和 CTF 类两类，这两类占课程总成绩的 30%，也就是 30 分，各部分练习所占比重如下：

| 序号 | 实验名称 | 分值 |
|----|------------|-----|
| 1 | 古典密码-凯撒加密 | 60 |
| 2 | 古典密码-汉字加密 | 50 |
| 3 | 流密码 | 50 |
| 4 | 分组加密 | 60 |
| 5 | 公钥密码 | 50 |
| 6 | 哈希函数 | 60 |
| 7 | 证书生成及应用 | 30 |
| 8 | 密码学 CTF 练习 | 60 |
| 总计 | | 420 |

表 9.1: 实验分值表

这部分的最终实际得分为：各项实际得分之和 $\times \frac{30}{420}$

Chapter 10

编程类练习参考评分标准

10.1 编程类练习评分标准 (有报告)

10.1.1 设计考虑

通过此类练习希望学生能够通过应用掌握一些工程工具，如此课程中的 git 工具使用、流程图的绘制软件及绘制方法。

另外希望学生能够进一步熟练使用 C 语言进行编程，提高使用 C 语言的能力。

学生能够理解已有的密码算法，并能够用 C 语言实现。

学生能够利用 GMP 大数据库编写算法，具备初步利用第三方库的能力，同时可以利用他设计并实现一些底层的数学算法。

通过编写规范的技术文档，基本掌握此类文档的编制方法。

10.1.2 参考评分标准

每次代码评分总分，如果没有按时提交为 0 分，没有按时提交，但是有合理理由 (比如一些不可控制的因素)，并被老师接受，为了体现公平，其评分总分为此次按时交作业中的最低分，最后得分将按其实际总分等比例获得。

每次代码评分总分为 60 分，评分规则为：

- CR(code running): 代码运行情况，共 35 分，细则为：
 - 是否有按要求命名的 exe，无，则 CR=0 分。
 - 有按要求命名的 exe，则按以下细则评分：
 - * 有可执行程序，但无法运行，0 分。
 - * 可以运行，按照测试用例的赋分，通过相应的测试用例获得相应的分值，总分为之和，0——35 分。
- DQ(document qualification): 文档文字描述，共 15 分，细则为：

- DQ-1 文档中有文字描述, 无 0 分, 有 5 分。如果文档有格式要求, 如果文档未给定模板写, 记 0 分。如果要求按照 pdf 格式提交, 未按此格式, 记 0 分。
- DQ-2 文字描述质量. 简练清晰 5 分, 把框架或功能准确描述出来 3, 描述混乱 0.
- DQ-3 有框架或功能流程图. 无 0 分, 不满足规范或者不准确 3 分, 满足规范且准确 5 分。
- EN(explanatory note), 共 5 分, 如果未按要求格式对源代码进行注释, 此项得分为 0。如果按照格式要求进行了注释, 则看注释是否清晰无错误, 得分 0-5 分。
- TC(test cases): 测试用例, 共 5 分, 此项总分为一下各项之和, 细则为:
 - TC-1 测试用例. 无 0 分, 有但是描述不规范 1 分, 有且描述规范 2 分.
 - TC-2 测试用例设计. 覆盖全面功能且考虑全面 3 分, 覆盖全部功能但考虑不全面主要内容 1, 未覆盖全面功能且考虑欠缺 0 分。

10.2 编程类练习评分标准 (无报告)

此类练习只需要提交源代和编译后的代码到 gitee 上即可。

评价依据是, 如果没有按时提交 (无对应仓库的 pr) 为 0 分, 没有按时提交, 但是有合理理由 (比如一些不可控制的因素), 并被老师接受, 为了体现公平, 其评分总分为此次按时交作业中的最低分, 最后得分将按其实际总分等比例获得。

代码评分总分为 50 分, 评分规则为:

- CR(code running): 代码运行情况, 共 35 分, 细则为:
 - 是否有按要求命名的 exe, 无, 则 CR=0 分。
 - 有按要求命名的 exe, 则按以下细则评分:
 - * 有可执行程序, 但无法运行, 0 分。
 - * 可以运行, 按照测试用例的赋分, 通过相应的测试用例获得相应的分值, 总分为之和, 0——35 分。
- EN(explanatory note), 共 15 分, 细则如下, 总分为各项之和:
 - EN-1 无注释. 无 0 分, 有注释给 5 分.
 - EN-2 如果未按要求格式对源代码进行注释, 此项得分为 0。如果按照格式要求进行了注释, 则看注释是否清晰无错误, 得分 0-10 分。