
— 计算机程序设计基础 (1) —

第2次作业

本学期作业提交说明

- 每次作业建议提交实验报告（如果当次作业要求提交则必须提交）。报告可包含但不限于：对作业的简单思路分析、实验结果的截图、代码、分析总结等。**如果提交的作业不包含足够说明信息，造成作业评判困难的，不给予相应题目分数，且不接受复议补交！**
- 对于需要写代码的题目，要求同时提交源代码；源代码可以直接拷贝到实验报告里，代码较长的话可以另附源代码文件提交。
- 实验报告可以提交word或pdf格式，建议提交pdf版。如果提交代码文件，注意仅提交*.h/c/cpp/hpp等源代码文件和代码运行所必须的依赖项即可，Visual Studio或Xcode等IDE产生的项目解决方案（如.sln）等文件不要提交！
- 实验报告、代码文件等都放在一个文件夹内，压缩成*.zip/rar等压缩文件，按时提交到网络学堂。
- **作业严禁抄袭！一旦发现并被判定为抄袭，无论抄与被抄，当次作业直接按照零分处理！**

本次作业提交说明

- 本次作业必做题2道（共10分），选做题1道。
- 选做题附加分0.5分，视完成情况给分，但本次作业分数不超过10分。
- 截止时间：**第5周周日（2017.10.21）23:59，缓交扣除当次作业分数的20%！**

第1题

上机查找程序中语法错误，并纠正，后编译运行。（5分）

要求：

1. 将给出的程序修改正确后，保存在文件exp2-1.cpp（文件名仅示例，后续命名保持规范统一即可）中，并提交，同时提交程序的运行结果界面的截图。
2. 对修改后的源程序做注释（**直接将注释写在.cpp程序文件中**）。

```
include "iostream.h";
use namespace std
int main( )
{ int x1,x2;
  unsigned y;
  char c1;
  x1=65535;x2=x1+5;
  cin>>"enter y:">>y1
  c1=97;c2='A',c2=c2+32;
  cout<<"x1="<<x1;
  cout<<"x2="<<x2
  cout<<"y="<<(y+15);
  cout<<"c1="<<c1;
  cout<<'c2='<<c2
  return(0);
};
```

作业范例：

```
#include <iostream> // 1.如果没有#, 编译时出错: xxxxx
using namespace std;
int main()
{
    ...
}
```

第2题

参考下列程序，读懂后编写一程序，在运行时输入一个数字（0–9），则输出该字符的ASCII值，并打印该字符的前导字符（即字符码减少1）及字符的后续字符（字符码增加1）。注意程序运行界面的清晰，提交源代码和运行结果。（5分）

```
#include <iostream> // 包含I/O头文件
using namespace std; // 使用命名空间，一年后你会知道该语句意思
int main()
{
    char c1='C', c2='h', c3='i', c4='n', c5='a';
    // 定义了c1-c5这5个字符型变量，并初始化
    c1 = c1 + 4; // 对c1的值加4
    c2 = c2 + 4;
    c3 = c3 + 4;
    c4 = c4 + 4;
    c5 += 4; // 注意运算符，以后再讲
    cout << "password is:" << c1 << c2 << c3 << c4 << c5 << endl;
    return 0;
```

```
}
```

运行结果：

```
password is:Glmre
```

选做题第1题

知识背景：密码系统

定义：密码系统是一个五元组 (E, D, M, K, C) ，其中，

- M : 明文空间
- K : 密钥空间
- C : 密文空间
- $E: M \times K \rightarrow C$ (加密算法)
- $D: C \times K \rightarrow M$ (解密算法)

例：凯撒密码：

- 表达为一个密码系统
 - $M = C = \{\text{所有罗马字母序列}\}$
 - $K = \{i | i \in \mathbb{Z}, 0 \leq i \leq 25\}$
 - $E = \{E_k | k \in K, m \in M, E_k(m) = (m + k) \bmod 26\}$
- m 表示相应字母在字母表中的位置（如下表所示）
 - HELLO 写成 7, 4, 11, 11, 14
 - 如果 $k = 3$, 密文为 KHOOR (10, 7, 14, 14, 17)

字母	A	B	...	Y	Z
数字	0	1	...	24	25

试根据上述凯撒密码原理来设计一套加密/解密软件。甲方采样密钥 k 来对输入一段文字加密，乙方使用 k 能对加密文字进行解密。 k 由甲乙双方协商设定。

提示：本题可以在一个程序中实现加密、解密的操作，也可以用两个程序分别实现加密与解密。如果在一个程序中实现，需要在代码中明确地体现出加密、解密的操作，禁止将未加密明文直接当做解密结果输出。