解答内容不得超过装订线

四、分析思考题（10 分）

1）上述程序运行后，屏幕上显示的是什么？（2 分）

答案：　1234

评分标准：　1234，　2 分

123400000，　1 分

4321，　0.5 分

2）子程序 f2to10 的功能是什么？它的入口参数和出口参数分别是什么？(3 分)

答案：　将一个无符号的双字类型数转换成十进制字符串，并保存到缓冲区中。

入口参数：存放转换结果的首地址；

待转换的双字类型的数

出口参数：无

评分标准：　将整数转换为字符串，输入和输出参数写错或没有写，2 分

将整数转换为字符串，输入输出参数为 d1、buf1，2.5 分

将长（双字）整数转换为 10 进制字符串，输入为长整数和缓冲区偏移地址，　3 分

3）若语句②写在标号①之前，程序会出现异常，请说明原因？（3 分）

答案：32 位数除 10，被除数必须为 64 位 (EDX, EAX)。除 10 以后，商保存在 EAX，余数保存在 EDX，第一次除 10 的余数不为 0。若将语句②写在标号①之前，导致每次进行除法时，EDX 是上一次除法的余数，一般不为 0。导致被除数从 32 位变成 64 位，每次除 10 的余数不为 0，商也不为 0，不断循环，会导致 PUSH DX 出现访问异常。

评分标准：　仅指明被除数为 (EDX, EAX) 或 仅指明余数为 (EDX)，　0.5 分

同时指明被除数为(EDX, EAX)、余数为 (EDX)，2 分

指明被除数为(EDX, EAX)、余数为 (EDX)、分析余数都不为 0 导致内存越界，3 分

4）若漏写了语句③，程序也会出现异常，请说明原因？（2 分）

漏写了语句③, ecx 会保持为 0. 在执行” next2：… loop next”之间的循环时，表面上会执行 2^32 次，但 POP　ax 或者 mov [esi], al 会出现异常，即访问单元的地址超出程序的地址空间。

评分标准：　仅说明 ecx 一直为 0，0.5 分

(ecx)=0、loop next 执行 1 次或 0 次，1 分

(ecx)=0、loop next 执行 2^32（2^16 也不扣分）导致内存越界，2 分

五、分析优化题（共 10 分）。

(1) 指出该段程序执行效率不高的原因 （2 分）。

程序中出现很多冗余语句：i++、count++、str[i]

评分标准： 写出“程序中出现很多冗余语句”或指出上面列出的 3 处冗余，2 分

指出上面 3 处冗余中的 2 个， 1.5 分

指出程序没有优化（有冗余）， 0.5 分

(2) 改编相应的汇编语言程序，以提高程序的执行效率。要求写出变量与寄存器对应关系。(6 分)

00E917A3 ~ 00E917A9: i++ => inc dword ptr [ebp-28h]

00E917D2 ~ 00E917D8: count++ => inc dword ptr [ebp-1Ch]

访问 str[i]: 00E917B8 ~ 00E917D0

```
cmp     ecx,41h
jl      00E917DB
cmp     ecx,5Ah
jg      00E917DB
```

评分标准： 重写整个程序段并优化， 6 分

优化上面 3 处冗余中的 2 个， 5 分

优化上面 3 处冗余中的 1 个， 3 分

(3) “00E917C3 jl 00E917DB”处指令的机器码为 7CH 16H，解释 16H 代表的含义（2 分）

该指令的下一条指令地址为 00E917C5， 转移的目的地为 00E917DB，

00E917DB – 00E917C5 = 16H， 即代表了目标地址 与 当前 EIP 之间的偏移量。

评分标准： 目标地址与 EIP（或当前指令的下一条指令的偏移地址）之间的偏移量，2 分

目标地址与当前指令的偏移地址之间的偏移量，1.5 分