**基于米勒拉宾算法的RSA密码系统**

**问题记录**

第八组

1. 开发平台是否采用最新版本，为什么？

Keil-MDK5与Proteus均未采用最新版本，Keil-MDK采用5.25版本，最新版本为5.32。Proteus采用8.6版本，最新版本为8.11，原因如下：

Keil-MDK5.32与5.25没有明显差别，且5.25版本是目前比较常用的版本，网上找到大量资源，包括一些器件包，工程样例等等。因此5.25版本是一个较好的选择。

目前使用的Proteus8.6，最新版本为8.11。Proteus 7.X的版本并未采用，因为Proteus 8对软件的架构有重大革新，增加对编译器环境的支持，同时糅合原理图设计、编程调试和PCB设计页面，仿真调试更直观，操作便利性大大提高。而STM32系列8.6本身已经支持，且根据官网描述，8.11的新的东西与我们做的项目无关。

2. RSA算法是否工作量太大，实现起来比较困难？

课后我们重新查找了资料，认为如果实现一个比较简单的RSA算法，再加上显示的控制模块等等，是可以在700行左右完成的。我们现在的想法是实现RSA算法的加密部分，即输入一串字符，并生成秘钥对其进行加密，但不进行解密部分。经过重新的思考与讨论，我们认为实现的难度比较合理。

3. C语言与汇编的混编。

通过答辩我们得知，在代码核心部分即一些运算量较大的部分使用汇编语言可以提高性能。我们在编程实践环节会尝试这种C语言与汇编混编的方式来实现相应功能。

4. 样例程序测试。

在使用样例程序测试方面我们前期做的不够到位，接下准备抓紧时间找到合适的样例程序来测试，为之后的编程实践铺路。

5. 提交要求。

①实现RSA加密过程，最后希望展示的结果是在Proteus仿真中输入一串字符，之后进行RSA加密，并在仿真中通过显示屏显示输入的字符串，生成的随机数，由随机数得到的秘钥，以及加密后的密文。以此验证功能的实现是否完备。

②提交相应的代码，实验报告以及过程记录与交流记录。

③如果时间充足，会尝试在自己的开发板（STM32F107VCT6）上验证我们的程序。