**作业题目：**

1. 编程实现SHA-1、SHA-2(SHA-256)、SHA-3(SHA-3-256)、MD5、RIPMD-160（每组实现一个算法，具体参照分组名单）算法并寻找碰撞：

1.每位同学姓名的全拼加学号。如 姓名：刘新光 学号: 2014210846, 则输入消息为’liuxinguang2014210846’ 。对对应算法给出字符串的杂凑值，并提交每个算法的C语言程序 （列出每步的中间结果，如MD5有64步，实例需将每步的输出值列出。）

2.编程实现对应算法杂凑值高50比特碰撞，并提交实现碰撞寻找的C语言程序。（如SHA-256杂凑值为256比特，只需要寻找两个不同的消息，其产生的杂凑值的最左边50个比特是相同的。）

1. 假设有128比特的AES密钥， 用16进制表示为

3AE11562A8F3C71A2BF6DFA1509BCAF1

使用该密钥，在10轮AES下计算下列明文（以16进展表示）的加密结果：

3243F6A8885A308D313198A2E0370734

要求：1 给出C代码。2 给出11\*128个子密钥。 3 给出密文。

三、编程实现GCM认证加密算法。其中加密算法选用AES，密钥选取与第二题相同。认证加密消息为每位同学姓名全拼加学号。要求输出最终的MAC值，并提交算法的c语言程序。