实验九-哈希函数

【实验目的及要求】

1、理解密码学Hash函数的安全性质、攻击方法、设计思想，掌握常用的密码学Hash函数的实现流程。

2、理解消息认证码的设计思想，掌握基于Hash函数的消息认证码HMAC的实现方法。

【实验步骤】

（一）必做

（1）实现SHA-1哈希算法。

（2）实现HMAC-SHA1。

（3）实现国密算法SM3，并且在实验报告中给出流程图和伪代码，具体实现可参照上课PPT或附件。

（二）选做

1、难度：简易

实现对SHA-1的第一类生日攻击。

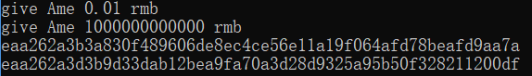
即对于给定的输出H（*x*），随机生成输入串，以得到某个输出H（*y*），使得它的前*n*比特与H（*x*）相同。

2、难度：中等

实现对SHA-1的第二类生日攻击。

即对给定的消息产生它的变形，以及构造假冒的消息并产生它的变形（变形后的消息与元消息意思相同，但格式稍有变化，比如多加几个空格）；在两个消息集合中找到一对消息使得他们作为SHA-1的输入时得到的输出前n比特是相同的。

参考输出格式：



【实验报告】

1、 实验布置两周内，请同学们将实验报告提交至OJ平台对应位置，逾期者酌情扣分。

2、 对于每个算法，报告中应含有函数调用关系图、测试样例及运行结果截图，并且记录自己本次实验的收获感想，和对实验不足之处的建议，部分算法需要流程图**和**伪代码。

3、 报告格式见附件二；且该格式仅供参考，同学们可酌情更改。

**4、 请注意：所有实验中，**并不是做困难难度的实验的难度系数一定高于难度为中等；**难度系数由实验自身难度和具体实现情况以及程度决定；**如果只能敷衍完成，同学们不如选择在更简单的选做题上创新。