实验六 密码学Hash函数的相关实践

一、 实验目的：

1、理解密码学Hash函数的设计思想，掌握常用的密码学Hash函数的实现流程。

2、深刻理解验证消息完整性的机制——消息认证的设计思想，掌握基于Hash函数的消息认证码HMAC的有效实现方案。

3、通过设计程序结构，增强程序的实用性和可扩展性，提高编程能力。

二、 实验说明：

本次实验内容按照难度不同分为初级、中级与高级三个等级，得分会以选定的实验等级为基准。

三、 实验内容：

**1、初级：**

**实现SHA-1算法。**

**2、中级：**

**实现HMAC算法。**

**3、高级：**

**实现课件上的“网站卫士”。**

“网站卫士”是一个网络安全软件产品。它的主要功能是通过网络扫描网站的网页，监测网页是否被修改，当发现网页被修改后，系统能够自动报警和恢复。

* 初始化过程

（1）对监视网站的文件备份到监控主机上。

（2）对每个备份的文件生成一个结构：文件位置、文件的哈希值。

* 监控过程

监控主机对监控网站进行轮回扫描，对扫描的文件进行如下操作：

（1）计算文件的哈希值，并与备份的文件哈希值进行比较，如果相同，转（4）步。

（2）如果不同，上载备份文件替换网站现有文件，转（4）步。

（3）如果备份文件不存在，则删除网站上这个文件，转（4）步。

（4）监控程序扫描下一文件。

注意：

1. 算法的输入是任意比特长的字符串。

2、通过设计不同的测试样例，体会密码学Hash函数在保证数据完整性方面起到的作用，并结合课上所讲体会其安全性。

四、 实验要求：

1、请合理划分程序结构，每一部分独立为一个.sage或.sagews文件，同实验报告一起打包提交，压缩文件命名格式为：**学号\_姓名\_实验六.zip/rar…**

2、代码鼓励写注释。**实验报告**应至少含有算法原理、算法流程、测试样例及运行结果，鼓励写心得体会或感想建议。

3、本次实验进行时间为**两周**。希望大家能及时上交sage文件以及实验报告。打包后的文件请发送到课程邮箱：buaa2015\_xinan@163.com。截止至第五次实验课前(6月3日)。