**密码学实验四实验报告**

姓名：孟衍璋 学号：16337183

1. **实验目的**

实现安全hash算法。

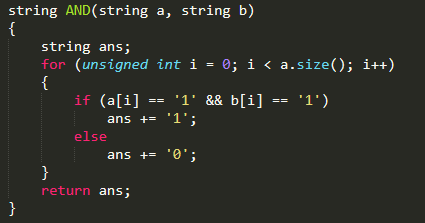
1. **实验内容**

将自己的学号进行hash并给出结果。

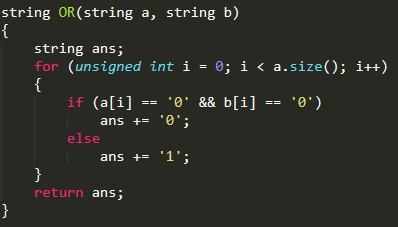
1. **实验及算法原理**

本次实验需要实现SHA-1算法，这是一个具有160比特消息摘要的迭代hash函数。SHA-1建立在对比特串的面向字的操作，每一个字由32比特（或者8个16进制数）组成。SHA-1用到了6个面向字的操作，分别如下：

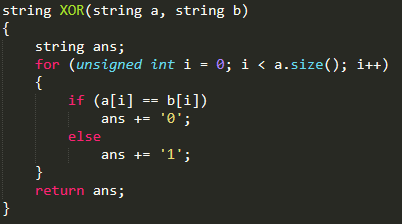
**X和Y的逻辑“和”：**



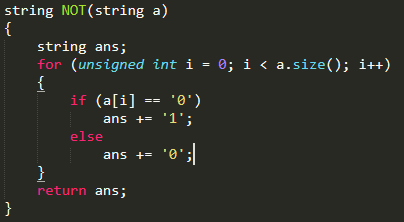
**X和Y的逻辑“或”：**



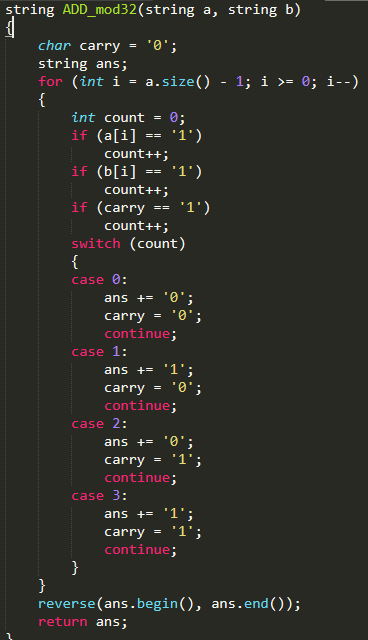
**X和Y的逻辑“异或”：**



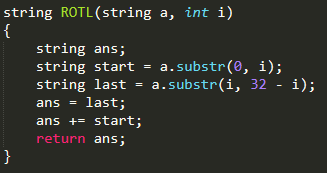
**X的逻辑“补”：**



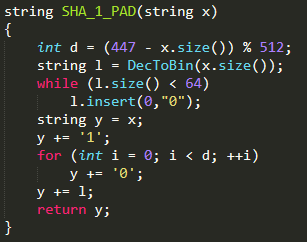
**模232整数加：**



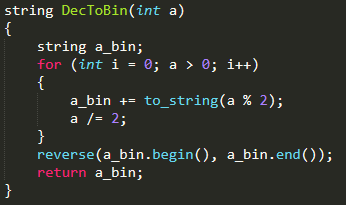
**X循环左移s个位置（0<=s<=31）：**



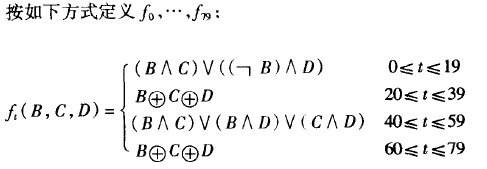
实现了这些面向字的操作之后，接下来要考虑的就是SHA-1所用的填充算法，代码实现如下：



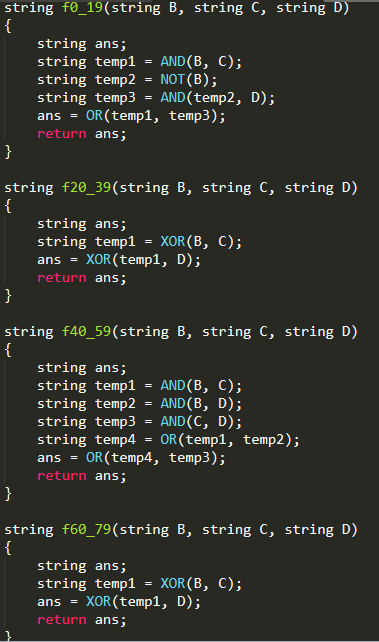
其中用到的将十进制数转换为二进制数的函数如下：



接下来还要实现如下函数：

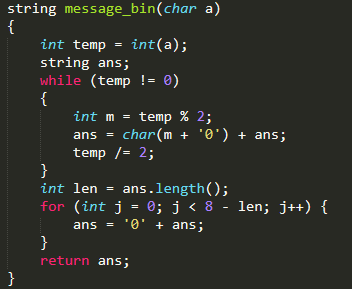


代码实现如下：

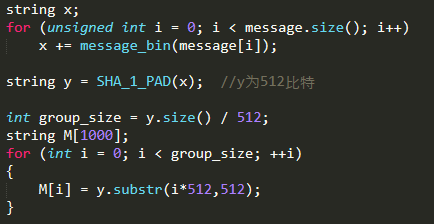


实现了上述函数之后，便可以开始依次按照SHA-1算法的步骤实现加密。

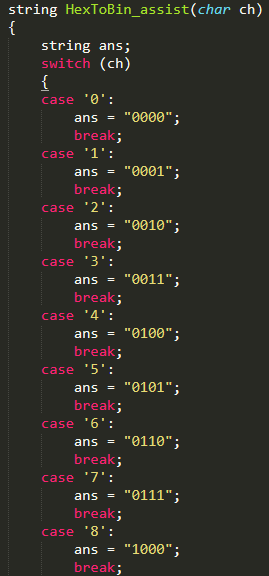
首先，将明文转换为二进制形式，其函数实现代码如下：

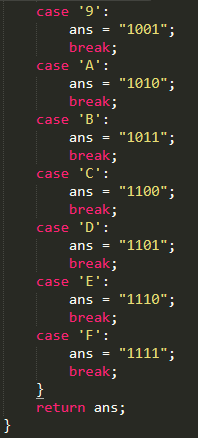


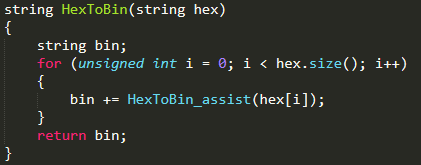
将转换为二进制后的明文串进行填充，将所得到的y分为512比特一组：



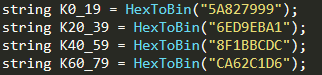
定义常数字符串，因为函数的接口都是字符串的二进制表示，所以这里需要将十六进制表示转化为二进制表示的函数，实现代码如下：

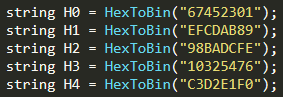




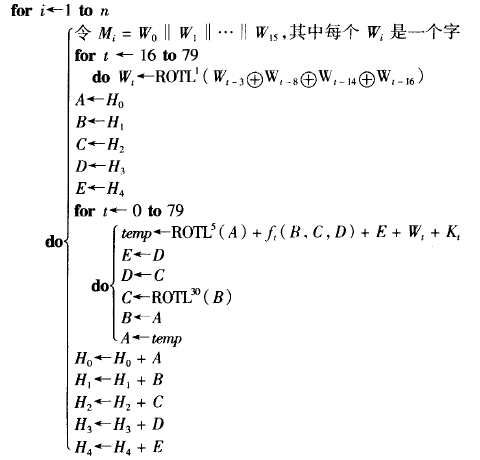


定义常数字符串：





之后按照下列步骤使用之前定义的操作函数进行实现：



1. **实验代码**



1. **运行截图**



1. **结果分析**



在线解密工具运行之后所得的结果与我的结果相符。

1. **总结**

这次实验是实现SHA-1，只需要参考书上的步骤，按照步骤来便可以依次实现。相比较之下比上一次实验AES的实现要简单许多，步骤没有这么繁杂，而且有了上一次实验的经验，很多之前踩过的坑也都避开了，不过还是有很多地方需要注意。

在做这个实验的过程中，首先将需要实现的函数列出来，对于SHA-1，主要是那6个面向字的操作的函数，填充算法，还有在压缩过程中的函数f。只要理清了思路，便可以以较快的速度实现出来。

本次实验最开始刚写完可以运行的代码之后，运行的结果与网站上验证的结果并不相符，一定是在之前的函数有哪一步有些小问题，经过检查之后发现是在实现模232整数加的函数中，将进位置为0的情况没有考虑进去，只写了进位置为1的情况，所以出现了错误。修改之后所得结果便是正确的。

总而言之，这次实验让我清楚了SHA-1的实现过程，对hash函数有了更深的理解。收获还是蛮丰富的。