姓名：佘崧林

学号：1613574

MD5

实验目的

通过实际编程了解 MD5 算法的过程，加深对 Hash 函数的认识。

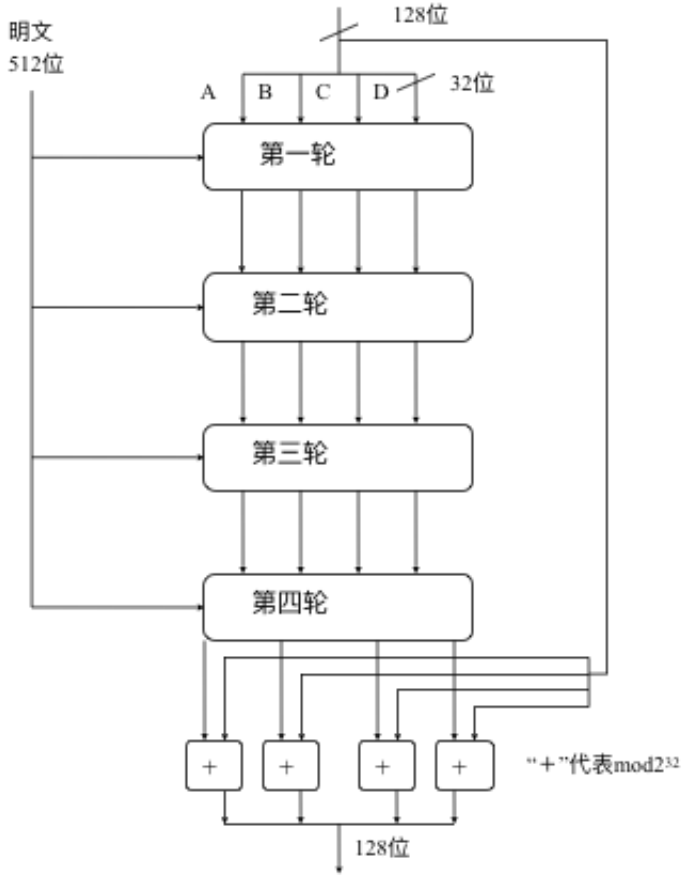
实验原理

Hash函数是将任意长的数字串转换成一个较短的定长输出数字串的函数，输出的结果称为Hash值。Hash函数具有如 下特点:

1. 快速性:对于任意一个输入值x，由Hash函数H(x)，计算Hash值y，即y=H(x)是非常容易的。
2. 单向性:对于任意一个输出值y，希望反向推出输入值x，使得y=H(x)，是非常困难的。
3. 无碰撞性:包括强无碰撞性和弱无碰撞性，一个好的Hash函数应该满足强无碰撞性，即找到两个不同的数字 串x和y，满足H(x)=H(y)，在计算上是不可能的。

Hash函数可用于数字签名、消息的完整性检验。消息的来源认证检测等。 现在常用的Hash算法有MD5、SHA-1等。下面从MD5入手来介绍Hash算法的实现机制。

MD系列单向散列函数是由Ron Rivest设计的，MD5算法对任意长度的输入值处理后产生128位的Hash值。MD5算法的实现步骤如下:



在MD5算法中，首先需要对信息进行填充，使其字节长度与448模512同余，即信息的字节长度扩展至n*512+448， n为一个正整数。填充的方法如下:在信息的后面填充第一位为1，其余各位均为0，直到满足上面的条件时才停止用 0对信息的填充。然后，再在这个结果后面附加一个以64位二进制表示的填充前信息长度。经过这两步的处理，现在 的信息字节长度为*n*512+448+64=(n+1)*512，即长度恰好是512的整数倍，这样做的目的是为了满足后面处理中对 信息长度的要求。

MD5中有A、B、C、D，4个32位被称为链接变量的整数参数，它们的初始值分别为: A0=0x01234567， B0=0x89abcdef， C0=0xfedcba98， D0=0x76543210

当设置好这4个链接变量后，就开始进入算法的4轮循环运算。循环的次数是信息中512位信息分组数目。

首先将上面4个链接变量复制到变量A、B、C、D中，以备后面进行处理。

然后进入主循环，主循环有4轮，每轮循环都很相似。第一轮进行16次操作，每次操作对A、B、C、D中的3个做一次 非线性函数运算，然后将所得结果加上第四个变量，文本的一个子分组(32位)和一个常数。再将所得结果向左循环 移S位，并加上A、B、C、D其中之一。最后用该结果取代A、B、C、D其中之一。

以下是每次操作中用到的4个非线性函数(每轮一个)。

$$F(B,C,D) = (B \wedge C) \vee (\overline{B} \wedge D)$$

$$G(B,C,D) = (B \wedge D) \vee (C \wedge \overline{D})$$

$$H(B,C,D) = B \oplus C \oplus D$$

$$I(B,C,D) = C \oplus (B \vee \overline{D})$$

MD5轮主要操作为:

a=b+((a+f(b,c,d)+M+t)<<<s)

对应于四轮操作，f分别取F，G，H，I;对每一轮的16次运算，M分别取M1，M2，...，M16。对于4轮共64次运算， t为给定的一些常数，另外一个常数s(i)是232*abs(sin(i)),其中i=1，2，...，64。在sin(i)中，i的单位是弧度，由此构

成了32位的随机数源是s(i)，它消除了输入数据中任何规律性的特征。

实验要求

1. 算法分析：请参照教材内容，分析MD5算法实现的每一步原理。
2. 算法实现：利用 Visual C++ 语言，自己编写MD5的实现代码，并检验代码实现的正确性。
3. 雪崩效应检验：尝试对一个长字符串进行Hash运算，并获得其运算结果。对该字符串进 行轻微的改动，比如增加一个空格或标点，比较Hash结果值的改变位数。进行8次这样的测试。

实验内容

详细的代码此处就不列举了，可以见 `.cpp` 文件。

运行结果：

```
$ ./bin/lab5
Raw Text: Hello World
Desired Md5: e59ff97941044f85df5297e1c302d260
Calc Md5: e59ff97941044f85df5297e1c302d260
Raw Text: Hello Worl
Desired Md5: 7df9c6e537b0683ddbcf3a443e053142
Calc Md5: 7df9c6e537b0683ddbcf3a443e053142
Raw Text: Hello Word
Desired Md5: ab37c47478377042b699f03b8769cd64
Calc Md5: ab37c47478377042b699f03b8769cd64
Raw Text: Hello Wold
Desired Md5: 7748957eae5acebdb32645eff8837131
```

```
Calc Md5: 7748957eae5acebdb32645eff8837131
Raw Text: Hello orld
Desired Md5: 41032fa65a13d1c9ad73823bd87d6902
Calc Md5: 41032fa65a13d1c9ad73823bd87d6902
Raw Text: Hell World
Desired Md5: 074028af8a35509ca6543808137ae050
Calc Md5: 074028af8a35509ca6543808137ae050
Raw Text: Helo World
Desired Md5: 4156f0a5ccf0b61e98150c7cd7da2e16
Calc Md5: 4156f0a5ccf0b61e98150c7cd7da2e16
Raw Text: Hllo World
Desired Md5: 042a1cb6170cc5af186de0faf909390c
Calc Md5: 042a1cb6170cc5af186de0faf909390c
Raw Text: ello World
Desired Md5: 7a36a259583db8df4122b9ff6c5237b1
Calc Md5: 7a36a259583db8df4122b9ff6c5237b1
```