密码学数字签字算法DSA实验报告

1. **实验目的**

通过对数字签字算法DSA的实际操作，了解SHA和DSA的工作原理

1. **实验原理**

**SHA**

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，计算Hash值y，即是非常容易的。
    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，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，在计算上是不可能的。

SHA的对消息填充的步骤与MD5算法一致，使其字节长度与448模512同余，即信息的字节长度扩展至，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。值得注意的是，SHA是以大端序存储这个长度数据的。

经过这两步的处理，现在的信息字节长度为，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。

接着对MD缓冲区初始化，缓冲区有5个32比特的寄存器

A=67452301 B=EFCDAB89 C=98BADCFB D=10325476 E=C3DD2E1F0

初始化后以分组为单位对消息进行处理，每一分组Y都用压缩函数处理，共进行四轮，每轮中由20步迭代构成。其中四轮分别使用不同的逻辑函数。每轮的输入为对当前处理的消息分组Y和缓冲区当前的A、B、C、D、E,输出仍放在缓冲区以代替A、B、C、D、E的旧值，每轮处理还需要加上一个加法常量K。

|  |  |
| --- | --- |
| 迭代步数 t | 常量K |
| 0~19 | 5A827999 |
| 20~39 | 6ED9EBA1 |
| 40~59 | 8F1BBCDC |
| 60~79 | CA62C1D6 |

第四轮的输出再与第一轮的输入相加，产生结果

第一轮

第二轮

第四轮

第三轮

明文

512位

A

B

C

D

+

+

+

+

32位

160位

“＋”代表mod232

160位

+

E

最后程序将最后一个分组的160比特作为消息摘要输出。

四轮函数分别为

轮主要操作为：A,B,C,D,E E+f(B,C,D)+A<<<5+W+K , A,B<<<30,C,D

其中Wt是当前512比特长的分组导出的一个32比特长的字

其中W0~W15直接取为输入分组响应的16个字，其余值进行如下计算

Wt=（Wt-16Wt-14Wt-8Wt-3）<<<1。

**DSA**

以往的文件或书信可以通过手写亲笔签名来证明其真实性，而通过计算机网络传输的信息则通过数字签字技术实现其真实性的验证。

数字签字目前采用较多的是非对称加密技术，其实现原理简单的说，就是由发送方利用杂凑函数对要传送的信息进行计算得到一个固定位数的消息摘要值，用发送者的私钥加密此消息的杂凑值所产生的密文即数字签字。然后将数字签字和消息一同发送给接收方。接收方收到消息和数字签字后，用同样的杂凑函数对消息进行计算得到新的杂凑值，然后用发送者的公开密钥对数字签字解密，将解密后的结果与自己计算得到的杂凑值相比较，如相等则说明消息确实来自发送方。

下面我们以DSA（Digital Signature Algorithm）为例，介绍数字签字算法。DSA源于Elgamal签名算法，被美国NIST采纳为DSS（Digital Signature Standard）数字签名标准。下面介绍DSA的算法描述：

1. 全局变量的设置
2. 素数p，2511<p<2512;
3. q是p的一个素因子，2159<q<2160;
4. ,其中h是整数，1<h<(p-1).
5. 私钥：

私钥x是随机数或伪随机数，其中0<x<q.

3. 公钥：

，（p，q，g，y）为公钥。

4．用户的随机数选择：

k为随机数或伪随机数，其中0<k<q。

基于以上选择的参数，DSA的签字过程如下：





则为对消息m的签字，显然，签字长度为320比特。

其中，H是一个安全杂凑函数，在DSS标准中，采用SHA-1算法作为安全的杂凑函数。

签字完成后，把对消息m的数字签字和消息m一同发送给接收方。接收方接收到消息m和数字签字后，对数字签字的验证过程如下：

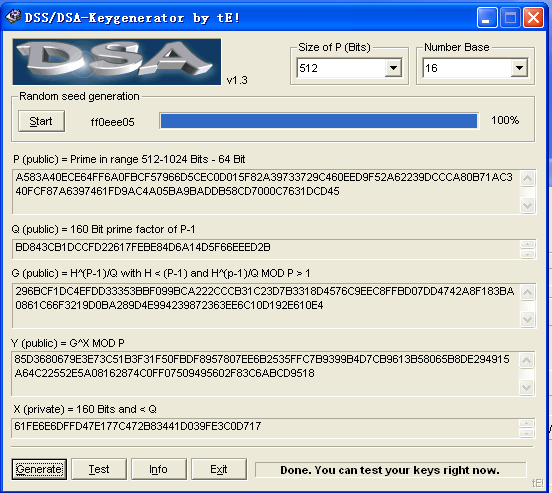
计算： 





如果有：，则说明信息确实来自发送方。否则，签字是无效的。

首先我们使用DSA工具随机生成 全局公开秘钥P、Q、G，用户公钥Y，用户私钥X



然后我们进行签名



最后进行验证

