

南 开 大 学

网络空间安全学院

密码学课程报告

|  |
| --- |
| 第五次实验报告  ——数字签字算法DSA |

学号： **1611519**

姓名： 周子祎

年级： 2016 级

专业： 信息安全-法学

2018 年 12 月 21 日

**密码学第五次实验报告**

——数字签字算法DSA

1. 实验目的

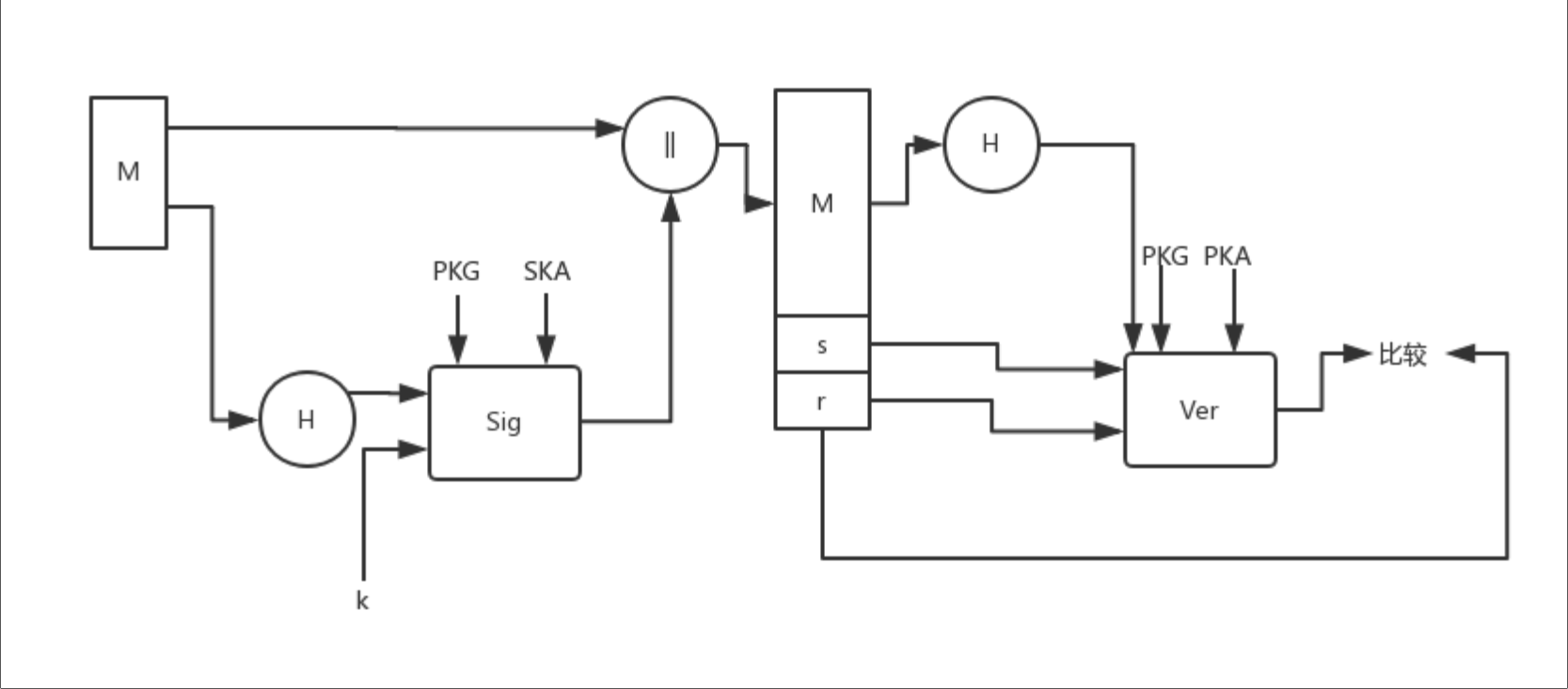
通过对数字签字算法DSA的实际操作，理解DSS的基本工作原理。

1. 实验原理

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。

1. 实验要求
2. 参照教材，熟悉数字签字算法DSA；
3. 参照教材，熟悉杂凑函数算法SHA；
4. 这里给出一个可运行的DSA数字签字演示程序，运行这个程序，对一段文字进行签字和验证，了解DSA算法的签字和验证过程。
5. 实验内容
6. **DSS基本签名方式**



1. **DSA数字签名算法**

DSA算法描述如下：

**(1) 全局公开钥**

p：一个大素数，长为L比特，其中512≤L≤1024且L是64的倍数

q：p-1的素因子，长为160比特

g：g≡h(p-1)/q mod p，其中h是满足1<h<p-1 且 使h(p-1)/q mod p>1的任一整数

**(2) 用户秘密钥x**

x：随机数或伪随机数，满足0<x<q

**(3) 用户公开钥y**

y：y≡gx mod p

**(4) 用户为待签消息选取的秘密数k**

k：随机数或伪随机数，满足0<k<q

**(5) 签字过程**

用户对消息M的**签字为(r, s)**，

其中：

**r≡(gk mod p) mod q,**

**s≡[k-1(H(M)+xr)] mod q，**

H(M)是由SHA求出的杂凑值

**(6) 验收过程**

设接收方收到的消息为M′，签字为(r′,s′)

计算

**w≡(s′)-1 mod q,**

**u1≡[H(M′)w] mod q**

**u2≡r′ w mod q,**

**v≡[(gu1yu2) mod p] mod q**

检查 v 是否等于 r′，若相等，则认为签字有效。

**(7) 验收原理证明**

若接收者收到的(M′,r′,s′) 等于发送者发送的(M,r,s)，

即**M′= M**，**r′ = r**，**s′ = s**

且公开钥y满足**y≡gx mod p**

则

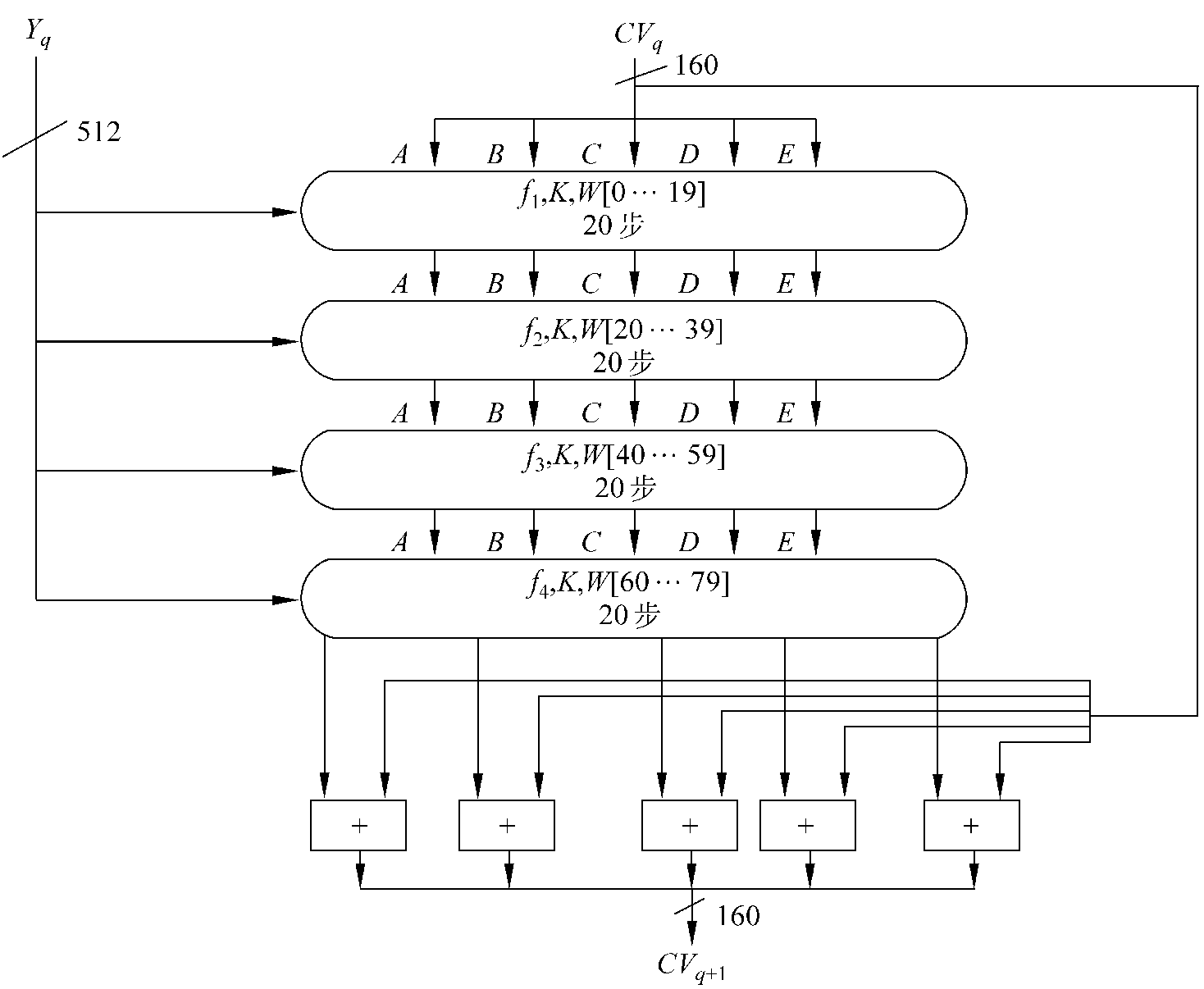


**(8) 安全性证明**

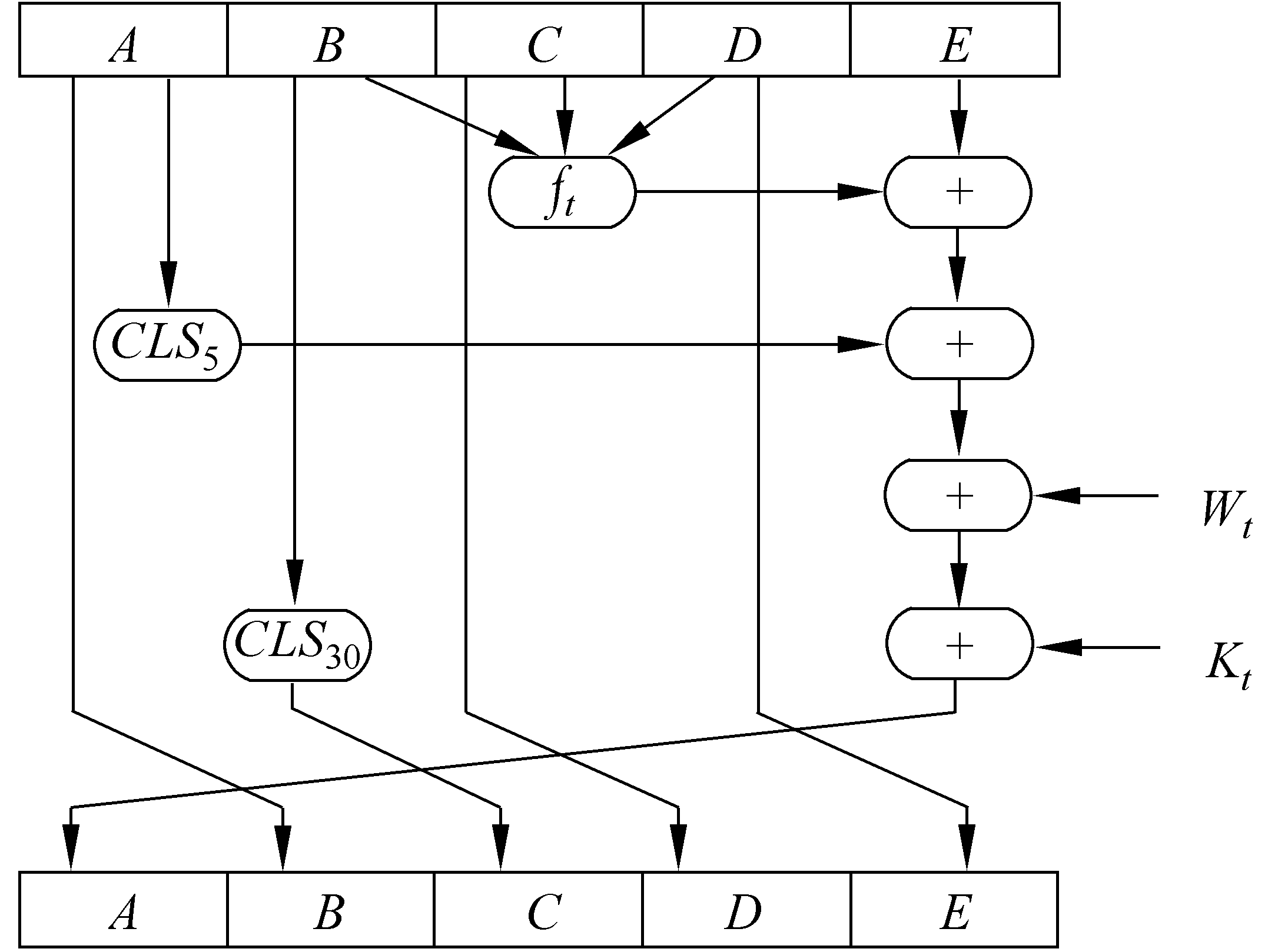
由于离散对数的困难性，敌手从r恢复k或从s恢复x都是不可行的。

1. **SHA杂凑函数算法**

**SHA分组处理框图**



**SHA压缩函数中一次分组处理中一步迭代流程图**



1. 实验过程

**1. 初始化参数**

**获取DSA签名算法全局公开钥P、Q、G，用户公开钥Y，用户秘密钥X**

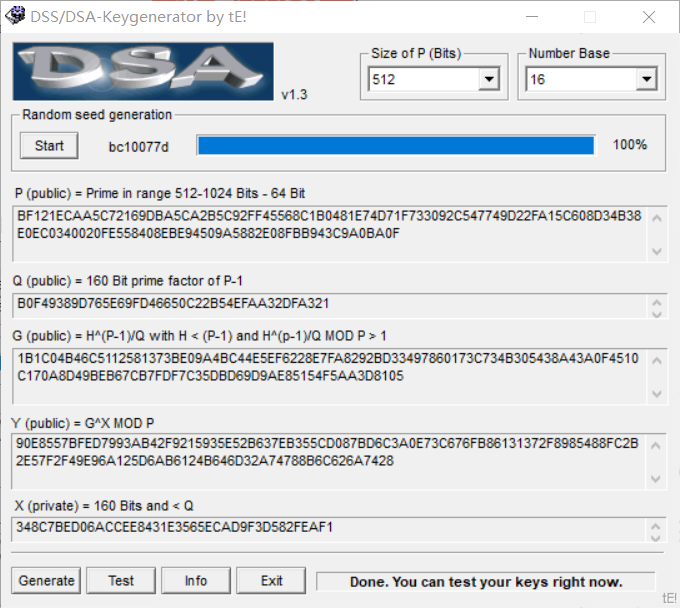
全局公开钥P：一个大素数，长为L比特，其中512≤L≤1024且L是64的倍数

全局公开钥 Q：P-1的素因子，长为160比特

全局公开钥 G：G≡H(P-1)/Q MOD P，其中1<H<P-1 且H(P-1)/Q mod P>1

用户秘密钥X：随机数，满足0<X<Q

用户公开钥Y：Y≡GX mod P



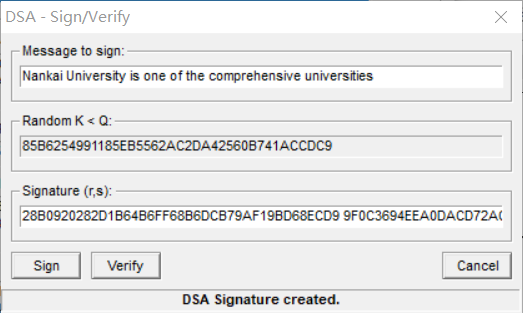
**2. 对消息完成签名认证**

**待签消息：**

**Nankai University is one of the comprehensive universities**

**为待签消息选取的秘密随机数K：**

**85B6254991185EB5562AC2DA42560B741ACCDC9**

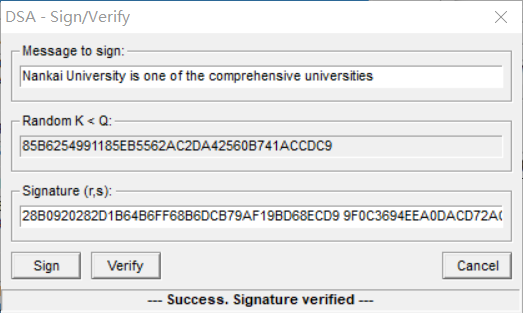


**签名（r,s）：**

**r ：28B0920282D1B64B6FF68B6DCB79AF19BD68ECD9**

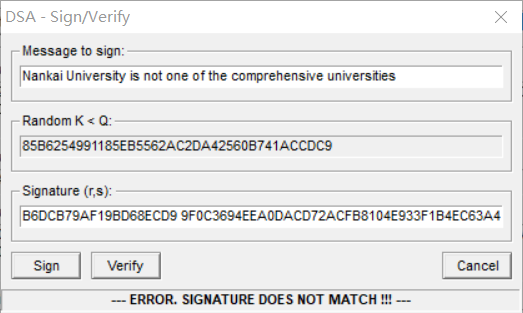
**s：9F0C3694EEA0DACD72ACFB8104E933F1B4EC63A4**

**3. 对消息完成签名认证**



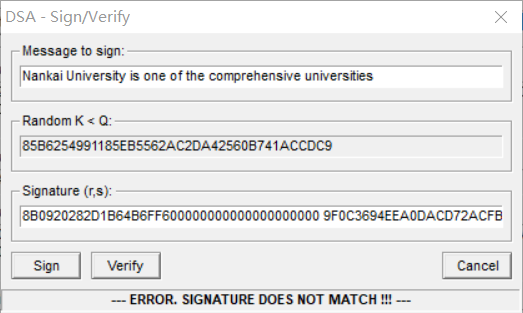
验证成功

**4. 修改消息内容，尝试验证**



验证失败

**5. 修改消息签名，尝试验证**



验证失败