



南开大学  
Nankai University

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

——数字签名算法 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

### 一、 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。

### 二、 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。

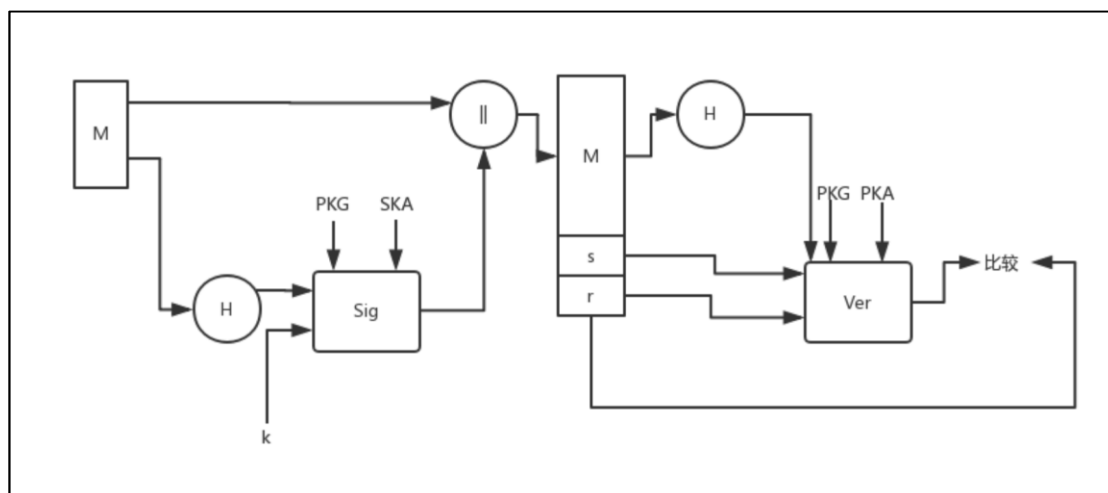
接收方收到消息和数字签字后，用同样的杂凑函数对消息进行计算得到新的杂凑值，然后用发送者的公开密钥对数字签字解密，将解密后的结果与自己计算得到的杂凑值相比较，如相等则说明消息确实来自发送方。

### 三、 实验要求

1. 参照教材，熟悉数字签字算法 DSA；
2. 参照教材，熟悉杂凑函数算法 SHA；
3. 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。

### 四、 实验内容

1. DSS 基本签名方式



## 2. 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  $512 \leq L \leq 1024$  且  $L$  是 64 的倍数

$q$ :  $p-1$  的素因子，长为 160 比特

$g$ :  $g \equiv h^{(p-1)/q} \pmod{p}$ , 其中  $h$  是满足  $1 < h < p-1$  且使  $h^{(p-1)/q} \pmod{p} > 1$  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 $y$

$y$ :  $y \equiv g^x \pmod{p}$

### (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：

$$r \equiv (g^k \bmod p) \bmod q,$$

$$s \equiv [k^{-1}(H(M) + xr)] \bmod q,$$

$H(M)$ 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

$$w \equiv (s')^{-1} \bmod q,$$

$$u_1 \equiv [H(M')w] \bmod q$$

$$u_2 \equiv r' w \bmod q,$$

$$v \equiv [(g^{u_1} y^{u_2}) \bmod p] \bmod q$$

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  $y \equiv g^x \bmod p$

则

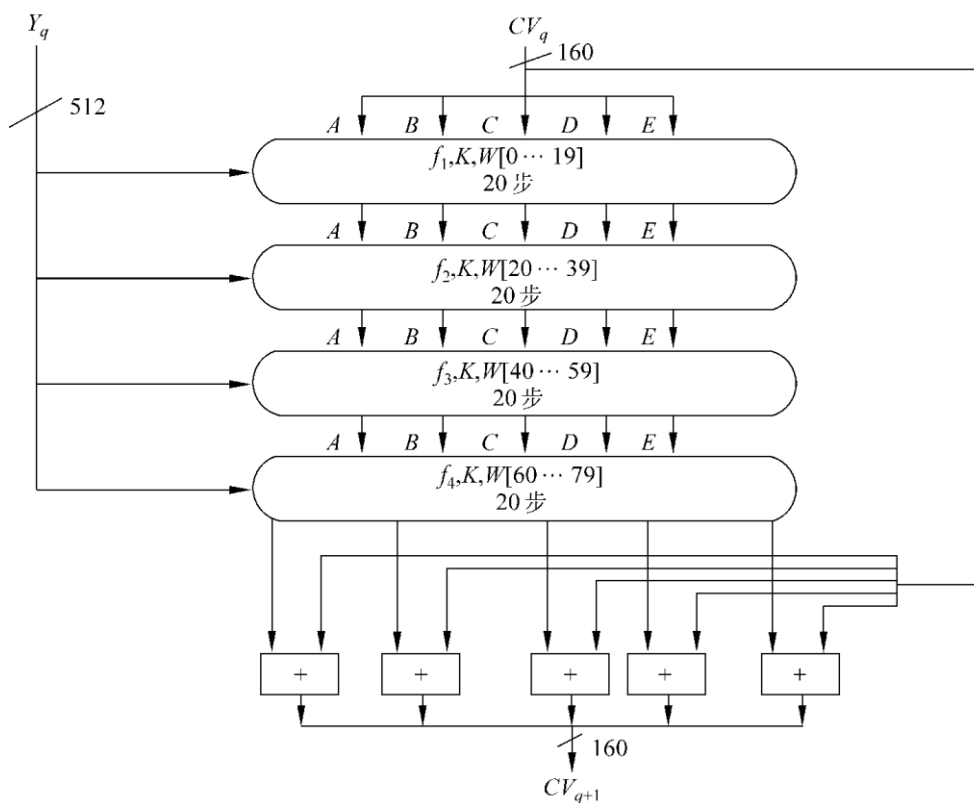
$$\begin{aligned} v &\equiv [(g^{H(M)w} g^{xrw}) \bmod p] \bmod q \equiv [g^{(H(M)+xr)s^{-1}} \bmod p] \bmod q \\ &\equiv (g^k \bmod p) \bmod q \equiv r \end{aligned}$$

## (8) 安全性证明

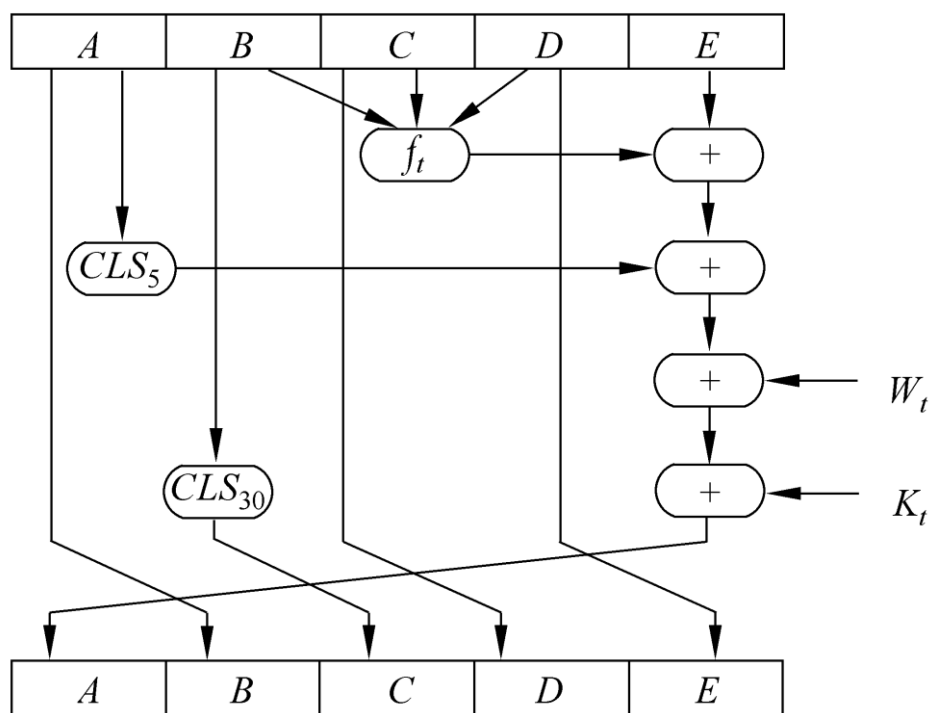
由于离散对数的困难性，敌手从  $r$  恢复  $k$  或从  $s$  恢复  $x$  都是不可行的。

## 3. 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



## 五、 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

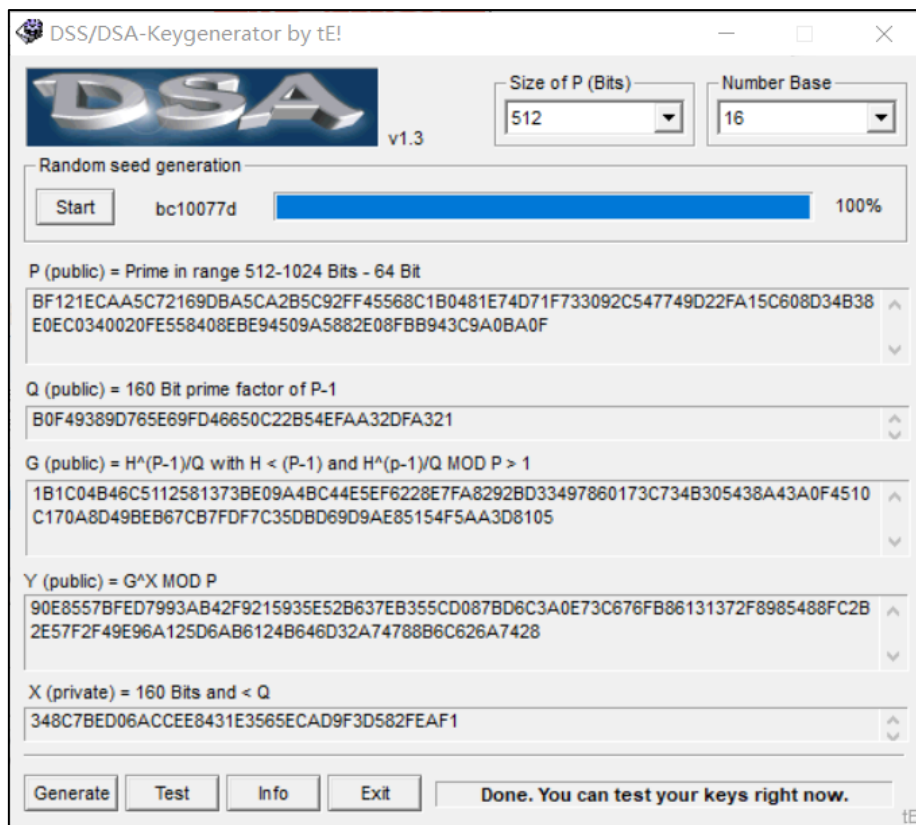
全局公开钥 P：一个大素数，长为 L 比特，其中  $512 \leq L \leq 1024$  且 L 是 64 的倍数

全局公开钥 Q：P-1 的素因子，长为 160 比特

全局公开钥 G：  $G \equiv H^{(P-1)/Q} \pmod{P}$ ，其中  $1 < H < P-1$  且  $H^{(P-1)/Q} \pmod{P} > 1$

用户秘密钥 X：随机数，满足  $0 < X < Q$

用户公开钥 Y：  $Y \equiv G^X \pmod{P}$



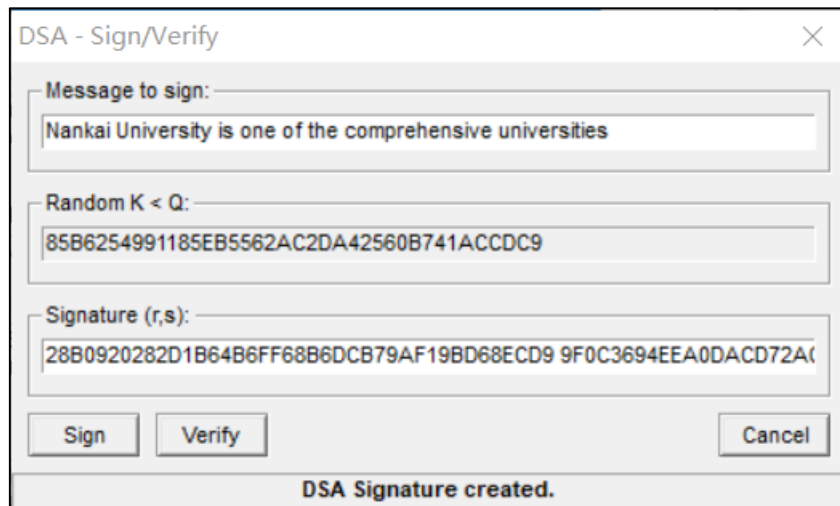
### 2. 对消息完成签名认证

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:

85B6254991185EB5562AC2DA42560B741ACDC9

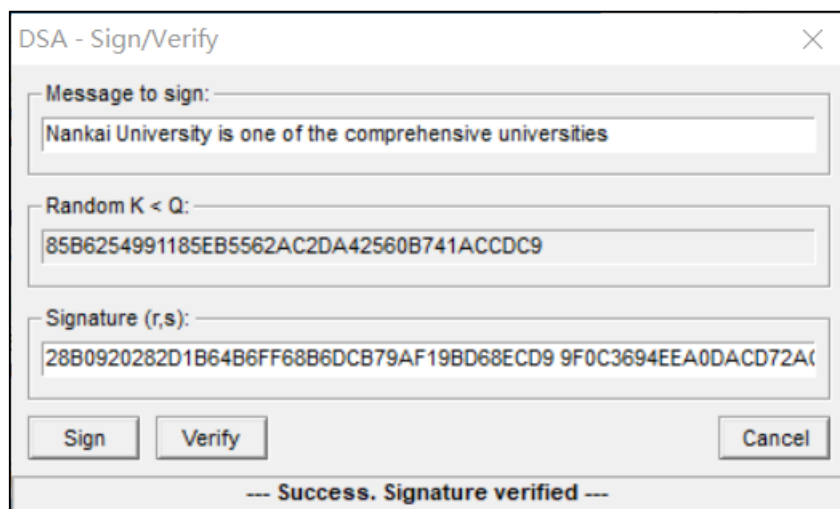


签名 (r,s):

r : 28B0920282D1B64B6FF68B6DCB79AF19BD68ECD9

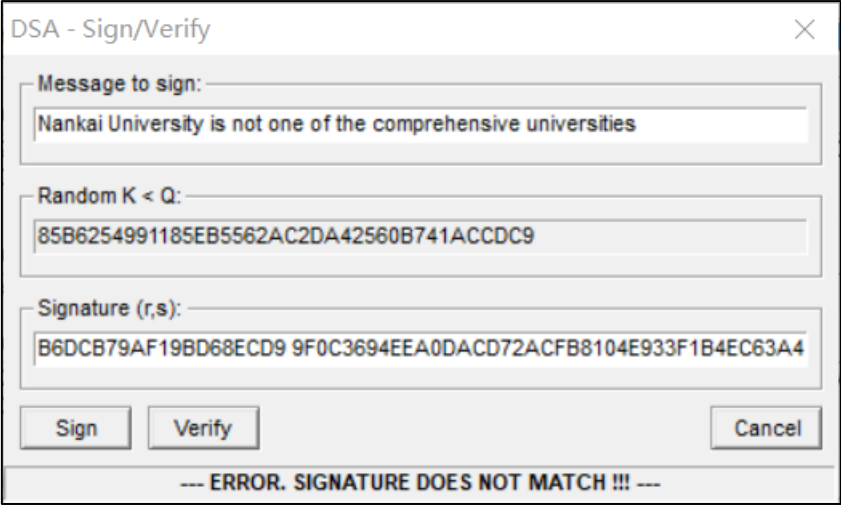
s: 9F0C3694EEA0DACD72ACFB8104E933F1B4EC63A4

### 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



DSA - Sign/Verify

Message to sign:  
Nankai University is not one of the comprehensive universities

Random K < Q:  
85B6254991185EB5562AC2DA42560B741ACDC9

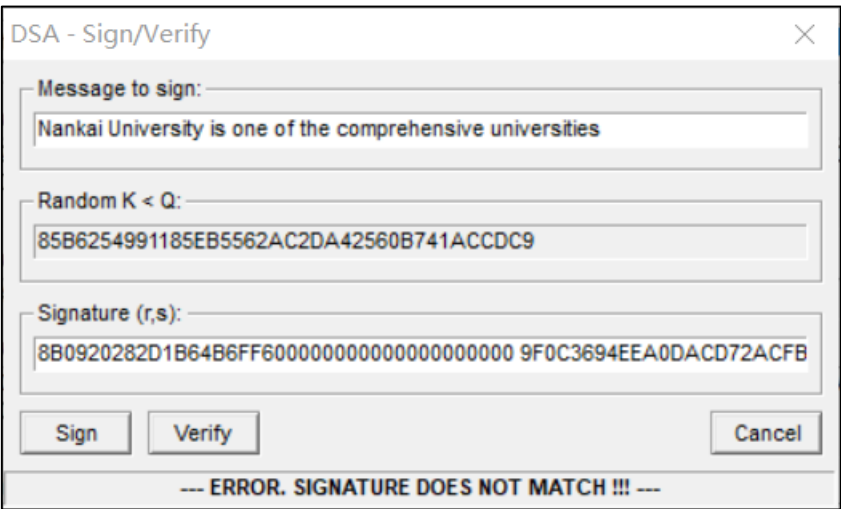
Signature (r,s):  
B6DCB79AF19BD68ECD9 9F0C3694EEA0DACD72ACFB8104E933F1B4EC63A4

Sign Verify Cancel

--- ERROR. SIGNATURE DOES NOT MATCH !!! ---

验证失败

#### 5. 修改消息签名，尝试验证



DSA - Sign/Verify

Message to sign:  
Nankai University is one of the comprehensive universities

Random K < Q:  
85B6254991185EB5562AC2DA42560B741ACDC9

Signature (r,s):  
8B0920282D1B64B6FF60000000000000000000000000 9F0C3694EEA0DACD72ACFB

Sign Verify Cancel

--- ERROR. SIGNATURE DOES NOT MATCH !!! ---

验证失败