



现代密码学

第四十七讲 DSS签名算法

信息与软件工程学院



- 1991年，数字签名标准(DSS)在ElGamal数字签名和Schnorr数字签名的基础上发展而来，被美国国家标准局(NIST)确定为数字签名标准。

DSS签名算法---密钥生成

- 1、设 $512 \leq L \leq 1024$ 且 L 是64的倍数，选取 $2^{L-1} < p < 2^L$ 大素数，其满足存在160比特的素数 $q \mid p-1$
- 2、随机选取整数 h ， $1 < h < p-1$ 且使 $g = h^{(p-1)/q} \bmod p$ ， p 和 g 公开；
- 3、随机选取整数 x ， $1 \leq x \leq q-1$ ，计算 $y = g^x \bmod p$ 。
- 4、公钥为 y ，私钥为 x

A decorative blue horizontal bar with a series of horizontal lines is positioned to the left of the title.

DSS 签名算法——签名算法

对于消息 m ，首先随机选取一个整数 k ， $1 \leq k \leq p-2$ ，然后计算：

$$r = g^k \bmod p \bmod q ,$$

$$s = (h(m) + xr) k^{-1} \bmod q,$$

则 m 的签名为 (r, s) ，其中 h 为Hash函数SHA。

DSS 签名算法——验证算法

接收方在收到消息 m 和签名 (r, s) 后，计算

$$u_1 = h(m) s^{-1} \bmod q$$

$$u_2 = r s^{-1} \bmod q$$

验证等式

$$g^{u_1} y^{u_2} \bmod p \bmod q = r$$

- 如果等式成立，则 (r, s) 是消息 m 的有效签名；反之，则是无效签名。



DSS签名的正确性

因为

$$u_1 + xu_2 \bmod q = (h(m) + xr) s^{-1} \bmod q = k$$

所以

$$\begin{aligned} g^{u_1} y^{u_2} \bmod p \bmod q &= g^{u_1 + xu_2} \bmod p \bmod q \\ &= g^k \bmod p \bmod q = r \end{aligned}$$