现代密码学

第四十六讲 ElGamal签名算法

信息与软件工程学院

- 1985年，EIGamal提出了一个基于离散对数问题的签名方案，后来称为EIGamal数字签名方案。

- 1991年该数字签名方案的变形被美国国家标准局(NIST)确定为数字签名标准(DSS)。

ElGamal签名算法---密钥生成

1、选取大素数p，$g \in Z_p^*$ 是一个本原元。p和g公开；

2、随机选取整数x,$1 \leqslant x \leqslant p-2$，计算$y = g^x \bmod p$。

3、公钥为y，私钥为x

ElGamal签名算法---签名算法

对于消息m，首先随机选取整数k，$1 \leqslant k \leqslant p-2$，然后计算：

$$r = g^k \bmod p, \quad s = (h(m)-xr)k^{-1} \bmod (p-1),$$

则m的签名为(r, s)，其中h为Hash函数。

ElGamal签名算法---验证算法

接收方在收到消息m和签名(r, s)后，验证

$$y^r r^s = g^{h(m)} \bmod p$$

- 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。

ElGamal签名的正确性

因为

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

所以有

$$sk + xr = h(m) \bmod (p-1)$$

所以

$$g^{h(m)} = g^{(sk+xr)} = g^{sk} g^{xr} = y^r r^s \bmod p$$

与ELGamal签名方案有关的两个问题

- 用ElGamal方案计算一个签名时，使用的随机数k能不能泄露？
- 若Bob用相同的k值来签名不同的两份消息，Oscar能否攻破这个体制？