现代密码学

第四十五讲 RSA签名算法

信息与软件工程学院

RSA签名算法---密钥生成

1、选两个保密的大素数p和q，计算$n=p\times q$，$\phi(n)=(p-1)(q-1)$；

2、选一整数e，满足$1<e<\phi(n)$，且$gcd(\phi(n),e)=1$；

3、计算d，满足$d\cdot e\equiv 1 \mod \phi(n)$；

4、以$\{e,n\}$为公钥，$\{d,n\}$为私钥。

RSA签名算法---签名算法

设消息为$m \in Z_n$，对其签名为

$$s \equiv m^d \bmod n$$

消息m的签名为s

RSA签名算法---验证算法

接收方在收到消息m和签名s后，验证

$$m \overset{?}{\equiv} s^e \bmod n$$

- 如果等式成立，则s是消息m的有效签名；反之，则是无效签名。

RSA签名的正确性

- 因为 $d \cdot e \equiv 1 \mod \phi(n)$
- 所以 $s^e \equiv m^{de} \equiv m^{1+k\phi(n)} \equiv m^1 m^{k\phi(n)} \equiv m \mod n$
- 其中 k 为某个整数

RSA签名算法---缺点

- 对任意$y \in Z_n$，任何人可计算$x \equiv y^e \bmod n$，因此任何人可伪造对随机消息x的签名。
- 如果消息x_1和x_2的签名分别为y_1和y_2，则知道x_1，y_1，x_2，y_2的人可伪造消息$x_1 \ x_2$的签名$y_1 \ y_2$。
- 在RSA签名方案中，需签名的消息$x \in Z_n$，所以每次只能对$\lfloor \log_2 n \rfloor$位长的消息进行签名。签名速度慢。
- 解决方法：引入hash函数

RSA的安全基础

- RSA签名方案的安全性归约于大数分解问题