



现代密码学

第四十五讲 RSA签名算法

信息与软件工程学院

A decorative graphic consisting of several horizontal blue bars of varying lengths, stacked vertically, is positioned to the left of the title.

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 $d \cdot e \equiv 1 \pmod{\phi(n)}$;
- 4、以 $\{e, n\}$ 为公钥, $\{d, n\}$ 为私钥。

A decorative blue horizontal bar with a series of parallel lines is located on the left side of the slide.

RSA 签名算法——签名算法

设消息为 $m \in Z_n$, 对其签名为

$$s \equiv m^d \pmod{n}$$

消息 m 的签名为 s

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

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

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

- 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。

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

RSA签名的正确性

- 因为 $d \cdot e \equiv 1 \pmod{\phi(n)}$
- 所以 $s^e \equiv m^{de} \equiv m^{1+k\phi(n)} \equiv m^1 m^{k\phi(n)} \equiv m \pmod{n}$
- 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 $x \equiv y^e \pmod n$ ，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