

4.7 RSA 公钥密码

○ 密码：明文 m 原始信息经过含有参数 k 的变换 E 得 $C = E(m)$ 。

E 为加密算法， k 密钥

，维吉尼亚密码：明文分为若干段，每段 n 个字符。密钥 $k = k_1, k_2, \dots, k_n$ 加密算法

$$E(m_1, m_2, \dots, m_n) = c_1 c_2 \dots c_n \quad \text{其中 } c_i = (m_i + k_i) \bmod 26.$$

○ 私钥：只要知道加密密钥即可算出解密密钥。

传递渠道和密不安全；仅凭一对密钥从方用太广。

○ 公钥：不可由加密密钥算出解密密码。

只有加密密钥公布，任何人都可以知道，但明文用其加密发送

只有自己知道解密密钥，将密文还原为明文。

RSA 公钥密码：

取两个不等的大质数 p, q ，使得 $n = pq$, $\phi(n) = (p-1)(q-1)$

取 $w, (w, \phi(n)) = 1$, $d = w^{-1} \pmod{\phi(n)}$

明文 m , 密文 c , 有加密算法: $c = E(m) = m^w \pmod{n}$ (无论 m 及 n 是不是质数)
解密算法: $m = c^d \pmod{n}$

其中 w, n 公开; $p, q, \phi(n), d$ 保密

利用大数分解的困难。

模幂乘法计算方法: $a^b \pmod{n}$ 等于 b 用二进制表示为 $(b_r, b_{r-1}, \dots, b_1, b_0)_2$

$$a^b \equiv a^{b_r} \cdot (a^2)^{b_{r-1}} \cdots (a^{2^{r-1}})^{b_1} \equiv A_0^{b_r} \cdot A_1^{b_{r-1}} \cdots A_{r-1}^{b_1} \pmod{n}$$

$$\text{其中 } A_0 = a, A_i = (A_{i-1})^2 \pmod{n}$$