

## 4.7 RSA 公钥密码

• 密码: 明文  $m$  原始信息经过含有参数  $k$  的函数  $E$  得  $C = E(m)$  密文.

$E$  为加密算法,  $k$  密钥.

• 维吉尼亚密码: 明文分为若干段, 每段  $n$  个数字. 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: 且要知道加密密钥 就可算出解密密钥.

传递渠道私密不方便; 仅能一对一通信应用太窄.

• 公钥: 不可由加密密钥算出解密密钥.

甲将加密密钥公布. 任何与甲通信的人, 将明文用其加密发送.

且有甲知道解密密钥, 将密文还原为明文.

RSA 公钥密码:

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

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  $m$  与  $n$  是否互质都好)

解密算法:  $m = C^d \pmod{n}$

其中  $w, n$  公开;  $p, q, \phi(n), d$  保密

利用了大数分解的困难.

模幂乘运算计算方法:  $a^b \pmod{n}$  将  $b$  用二进制表示为  $(b_{r-1} b_{r-2} \dots b_1 b_0)_2$

$$a^b \equiv a^{b_0} \cdot (a^2)^{b_1} \cdot \dots \cdot (a^{2^{r-1}})^{b_{r-1}} \equiv A_0 \cdot A_1 \cdot \dots \cdot A_{r-1} \pmod{n}$$

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