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$C=E(m)$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$k=k_1k_2\cdots k_n$，加密算法

  $E(m_1m_2\cdots m_n)=c_1c_2\cdots c_n$ 其中 $c_i=(m_i+k_i) \bmod 26$.

- 私钥：只要知道加密密钥 就可算出解密密钥.

  传送渠道私密不方便；仅供一对通信双方用太多.

- 公钥：不可由加密密钥算出解密密码.

  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

  只有甲知道解密密钥，将密文还原为明文

RSA公钥密码：

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

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

明文m，密文c，有 加密算法 $c=E(m)\equiv m^w \pmod n$ （无论m与n是否互质都对）

解密算法 $m\equiv c^d \pmod n$

其中w,n公开；$p,q,\varphi(n),d$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$(b_{r-1}b_{r-2}\cdots b_1b_0)_2$

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

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