密码学基础-作业 3

提交方式：通过HITsz Grade平台提交　　提交截止时间：以系统上公布时间为准
提交格式：pdf文件　　文件命名规则：学号_姓名_作业3.pdf
注：若包含照片或插图，请旋转至适合阅读的方向

1. 求：$\gcd(24140,16762)$

2. 用扩展欧几里得算法求下列乘法逆元：$1234 \bmod 4321$

3. 用费马小定理计算：$3^{201} \bmod 11$

4. 用费马小定理找到一个位于0到28之间的数x，使得x^{85}模29与6同余（不使用穷举法）。

5. 用欧拉定理找到一个位于0到9之间的数a，使得7^{1000}模10与a同余（注意这等同于7^{1000}的十进制数展开的最后一位）。

6. 下面是孙子用来说明CRT的一个例子，请求解x。

$$x \equiv 2(\bmod 3);\quad x \equiv 3(\bmod 5);\quad x \equiv 2(\bmod 7)$$

7. 给定29的本原根2，构造离散对数表，并利用该表解下列同余方程：
   a. $17x^2 \equiv 10(\bmod 29)$
   b. $x^2 - 4x - 16 \equiv 0(\bmod 29)$
   c. $x^7 \equiv 17(\bmod 29)$

8. 用下图所示的RSA算法对以下数据实现加密和解密：

$$p = 5,\ q = 11,\ e = 3,\ M = 9$$

Key Generation by Alice	
Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calcuate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption by Bob with Alice's Public Key	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption by Alice with Alice's Public Key	
Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

9. 在RSA公钥密码体制中，每个用户都有一个公钥e和一个私钥d。假定Bob的私钥已泄密。Bob决定生成新的公钥和私钥，而不生成新的模数，请问这样做安全吗？

10. 本题说明选择密文攻击的简单应用。Bob截获了一份发给Alice的密文C，该密文是用Alice的公钥e加密的。Bob想获得原始消息$M = C^d \bmod n$。Bob选择一个小于n的随机数r，并计算$Z = r^e \bmod n$，$X = ZC \bmod n$，$t = r^{-1} \bmod n$。接着，Bob让Alice用她的私钥对X进行认证（见图9.3），从而解密X。Alice返回$Y = X^d \bmod n$。说明Bob如何利用获得的信息求M。

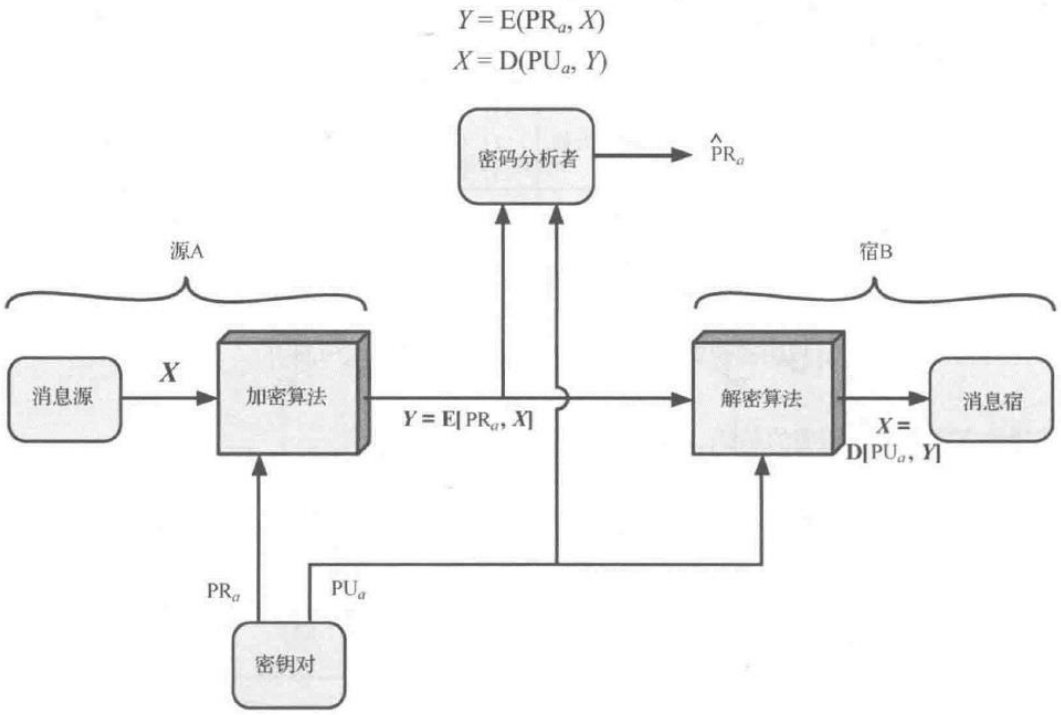

图 9.3　公钥密码体制：认证