第三次作业参考答案

作业3-习题1

① 用Fermat定理计算3^{201} mod 11

- Fermat定理说如果 p是素数， gcd（a，p)=1, $a^{p-1} \equiv 1 \bmod p$.
- 因此 $3^{10} \equiv 1 \bmod 11$.
- $3^{201} \bmod 11$

  $= (3^{10})^{20} \times 3 \bmod 11$

  $= (3^{10})^{20} \bmod 11 \times 3 \bmod 11$

  $= 3 \bmod 11$

作业3-习题2

② 用**Fermat**定理找到一个位于**0**到**72**之间的数，使得**a**模**73**与 $\mathbf{9^{794}}$同余

$9^{794} \bmod 73$

$=(9^{72})^{11} \times 9^{2} \bmod 73$

$=(9^{72})^{11} \bmod 73 \times 9^{2} \bmod 73$

$=9^{2} \bmod 73$

$=8$

作业3-习题3

③ 用RSA算法对下列数据实现加密和解密

a. p=3；q=11，e=7；M=5

$n=pq=3\times 11=33$

$\phi(n)=(p-1)(q-1)=2\times 10=20$

$d=e^{-1} \bmod 20=3$

$C=M^e \bmod n =5^7 \bmod 33$

$=5^4\times 5^2\times 5^1 \bmod 33$

$=3875 \bmod 33$

$=14$

$M=C^d \bmod n =14^3 \bmod 33$

$=14^2\times 14^1 \bmod 33$

$=31\times 14 \bmod 33$

$=434 \bmod 33$

$=5$

作业3-习题3

③ 用**RSA**算法对下列数据实现加密和解密

b. p=3；q=11，e=7；M=9

$n=pq=3 \times 11=33$

$\phi(n)=(p-1)(q-1)=2 \times 10=20$

$d=e^{-1} \bmod 20=3$

$C=M^e \bmod n = 9^7 \bmod 33$

$=9^4 \times 9^2 \times 9^1 \bmod 33 = 9^4 \bmod 33 \times 9^2 \bmod 33 \times 9^1 \bmod 33$

$= 9^4 \bmod 33 \times 15 \bmod 33 \times 9 \bmod 33 = 15^2 \bmod 33 \times 135 \bmod 33$

$=27 \bmod 33 \times 3 \bmod 33 = 81 \bmod 33 = 15$

$M=C^d \bmod n = 15^3 \bmod 33$

$=15^2 \times 15^1 \bmod 33$

$=27 \times 15 \bmod 33$

$=405 \bmod 33$

$=9$

作业3-习题3

③ 用**RSA**算法对下列数据实现加密和解密

c. $p=7$； $q=11$， $e=17$； $M=8$

$n=pq=7\times 11=77$

$\phi(n)=(p-1)(q-1)=6\times 10=60$

$d=17^{-1} \bmod 60=53$

$C=M^{e} \bmod n =8^{17} \bmod 77$

$=8^{16}\times 8^{1} \bmod 77= 8^{4} \bmod 77\times 8^{4} \bmod 77 \times 8^{4} \bmod 77 \times 8^{4} \bmod 77 \times 8 \bmod 77$

$= 15^{4} \bmod 77 \times 8 \bmod 77 =71^{2} \bmod 77 \times 8 \bmod 77=36 \bmod 77 \times 8 \bmod 77$

$=288 \bmod 77 =57$

$M=C^{d} \bmod n =57^{53} \bmod 77$

$=8$

作业3-习题4

④ 请通过中国剩余定理（CRT）回答下面的问题：

六位教授分别在周一至周六开始授课，并且分别每隔2，3，4，1，6，5天授课一次，该大学禁止周日上课。什么时候所有六位教授首次发现必须同时停一次课？

$x = 1 + 2K1 = 2 + 3K2 = 3 + 4K3 = 4 + K4 = 5 + 6K5 = 6 + 5K6 = 0+7K7$

(1) $x \equiv 1 \bmod 2$; (2) $x \equiv 2 \bmod 3$; (3) $x \equiv 3 \bmod 4$; (4) $x \equiv 4 \bmod 1$;

(5) $x \equiv 5 \bmod 6$; (6) $x \equiv 6 \bmod 5$; (7) $x \equiv 0 \bmod 7$

- **(4)** 表示没有限制，天天上课， **(1)** 和 **(2)** 包含在 **(3)** 和 **(5)**中，
  (3)式表明 **x** 与 **3, 7,or 11 (mod 12)**同余， **(5)**式表明**x** 与**5 or 11 (mod 12)**同余，
- 同时满足（3）和（5）等价于 **$x \equiv 11 \pmod{12}$**，因此，问题求解等价于
- $x \equiv 11 \pmod{12}$; $x \equiv 6 \bmod 5$; $x \equiv 0 \bmod 7$
- $x \equiv -1 \pmod{12}$; $x \equiv 1 \bmod 5$; $x \equiv 0 \bmod 7$

- $x \equiv 11 \pmod{12}$; $x \equiv 6 \bmod 5$; $x \equiv 0 \bmod 7$
- $x \equiv -1 \pmod{12}$; $x \equiv 1 \bmod 5$; $x \equiv 0 \bmod 7$
- 这里 $m1 = 12$; $m2 = 5$; $m3 = 7$; $M = 420$
- $M1 = 35$; $M2 = 84$; $M3 = 60$
- $M1' M1 \equiv 1 \bmod 12$, $M1'=11$
- $M2' M2 \equiv 1 \bmod 5$, $M2'=4$
- $M3' M3 \equiv 1 \bmod 7$, $M3'=2$
- $x \equiv 11 \times 11 \times 35 + 6 \times 4 \times 84 + 0 \times 2 \times 60$
- $= 6251 \equiv 371 \pmod{420}$

作业3-习题5

⑤ 设ElGamal体制的公用素数p = 71，其本原根g = 7

a.若B的公钥$Y_b = 3$，A选择的随机整数k = 2，则M = 30的密文是什么？

- $C_1=g^k \bmod p= 7^2 \bmod 71=49$
- $C_2=(Y_b)^k M \bmod P=3^2 \times 30 \bmod 71=270 \bmod 71=57$
- 所以 M = 30 的加密后密文为（49，57）

作业3-习题5

⑤ 设ElGamal体制的公用素数p = 71，其本原根g = 7

a.若B的公钥$Y_b = 3$，A选择的随机整数k = 2，则M = 30的密文是什么？

b.若A选择的k值使得M=30的密文C = (59，C_2)，则整数C_2是多少？

- $C_1 = g^k \bmod p = 7^k \bmod 71 = 59$
- 则 k = 3
- $C_2 = (Y_b)^k M \bmod P = 3^3 \times 30 \bmod 71 = 810 \bmod 71 = 29$

作业3-习题6

⑥ 在**ElGamal**算法中，为什么要使用不同的随机数**k**来加密不同的消息？

攻击**ElGamal**加密算法等价于解离散对数问题，要使用不同的随机数**k**来加密不同的信息。假设用同一个**k**来加密两个消息**m1**，**m2**，所得到的密文分别为**(a1，b1)(a2，b2)**，

- $a1=g^k \bmod p$
- $b1=y^k m1 \bmod p = g^{xk} m1 \bmod p$
- $a2=g^k \bmod p$
- $b2=y^k m2 \bmod p = g^{xk} m2 \bmod p$

则**b1/b2=m1/m2**，故当**m1**已知，**m2**可以很容易地计算出来。