1. 求gcd (24140,16762)

解:

$$a_0 = 24140$$
$$a_1 = 16762$$
$$a_2 = a_0 \ mod \ a_1 = 7378$$
$$a_3 = a_1 \ mod \ a_2 = 2006$$
$$a_4 = a_2 \ mod \ a_3 = 1360$$
$$a_5 = a_3 \ mod \ a_4 = 646$$
$$a_6 = a_4 \ mod \ a_5 = 68$$
$$a_7 = a_5 \ mod \ a_6 = 34$$
$$a_8 = a_6 \ mod \ a_7 = 0$$
$$\gcd(24140,16762) = a_7 = 34$$

2. 用扩展欧几里得算法求下列乘法逆元：$1234 \ mod \ 4321$

解:

$$a = 1234$$
$$b = 4321$$
$$x_0 = 1, y_0 = 0$$
$$x_1 = 0, y_1 = 1$$
$$s_0 = ax_0 + by_0 = 1234$$
$$s_1 = ax_1 + by_1 = 4321$$
$$k_1 = \lfloor \frac{s_0}{s_1} \rfloor = 0$$
$$x_2 = x_0 - k_1 x_1 = 1$$
$$y_2 = y_0 - k_1 y_1 = 0$$
$$s_2 = s_0 - k_1 s_1 = 1234$$
$$k_2 = \lfloor \frac{s_1}{s_2} \rfloor = 3$$
$$x_3 = x_1 - k_2 x_2 = -3$$
$$y_3 = y_1 - k_2 y_2 = 1$$
$$s_3 = s_1 - k_2 s_2 = 619$$
$$k_3 = \lfloor \frac{s_2}{s_3} \rfloor = 1$$

$$x_4 = x_2 - k_3x_3 = 4$$
$$y_4 = y_2 - k_3y_3 = -1$$
$$s_4 = s_2 - k_3s_3 = 615$$
$$k_4 = \lfloor \frac{s_3}{s_4} \rfloor = 1$$
$$x_5 = x_3 - k_4x_4 = -7$$
$$y_5 = y_3 - k_4y_4 = 2$$
$$s_5 = s_3 - k_4s_4 = 4$$
$$k_5 = \lfloor \frac{s_4}{s_5} \rfloor = 153$$
$$x_6 = x_4 - k_5x_5 = 1075$$
$$y_6 = y_4 - k_5y_5 = -307$$
$$s_6 = s_4 - k_5s_5 = 3$$
$$k_6 = \lfloor \frac{s_5}{s_6} \rfloor = 1$$
$$x_7 = x_5 - k_6x_6 = -1082$$
$$y_7 = y_5 - k_6y_6 = 309$$
$$s_7 = s_5 - k_6s_6 = 1$$

此时有：

$$ax_7 + by_7 = s_7$$
$$1234 \times (-1082) + 4321 \times 307 = 1$$
$$1234^{-1} = -1082 \equiv 3239 \ (mod\ 4321)$$

3. 用费马小定理计算$3^{201}\ mod\ 11$。

解:

$3^{10}\ mod\ 11 = 1$

$3^{201}\ mod\ 11 = \ (3^{10})^{20} * 3\ mod\ 11 = 3\ mod\ 11 = 3$

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(不使用穷举发)

解:

答案: 6

$$6^{28} \equiv 1\ (mod\ 29)$$
$$6^{84} \equiv 1\ (mod\ 29)$$
$$6^{85} \equiv 6\ (mod\ 29)$$

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（注意这等于$7^{1000}$的十进制数展开的最后一位)。

解:

答案: 1

$$\varphi(10) = 4$$

因为 7 与 10 互质, 由欧拉定理: $7^{\varphi(10)} \equiv 1\ (mod\ 10)$

$$7^{1000}\ mod\ 10 \equiv (7^4)^{250}\ mod\ 10 \equiv 1\ (mod\ 10)$$

6. 下面是孙子用来说明 CRT 的一个例子，请求解$x$。

解：

$$x \equiv 2(\mathrm{mod}\ 3); \quad x \equiv 3(\mathrm{mod}\ 5); \quad x \equiv 2(\mathrm{mod}\ 7)$$

We have $M = 3 \times 5 \times 7 = 105$; $M/3 = 35$; $M/5 = 21$; $M/7 = 15$.
The set of linear congruences

$35b_1 \equiv 1 \pmod 3$; $21b_2 \equiv 1 \pmod 5$; $15b_3 \equiv 1 \pmod 7$

has the solutions $b_1 = 2$; $b_2 = 1$; $b_3 = 1$. Then,

$$x \equiv 2 \times 2 \times 35 + 3 \times 1 \times 21 + 2 \times 1 \times 15 \equiv 233 \pmod{105} = 23$$

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. $17x^2 \equiv 10(mod\ 29)$
   b. $x^2 - 4x - 16 \equiv 0(mod\ 29)$
   c. $x^7 \equiv 17(mod\ 29)$

解：

**a.** $x = 2, 27 \pmod{29}$
**b.** $x = 9, 24 \pmod{29}$
**c.** $x = 8, 10, 12, 15, 18, 26, 27 \pmod{29}$

8. 用下图所示的 RSA 算法对以下数据实现加密和解密：

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

| **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 $d$ | $d \equiv e^{-1} (\mathrm{mod}\ \phi(n))$ |
| 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: | $M = C^d \bmod n$ |

解：

$$n = 55; \emptyset(n) = 40; d = 27; C = 14.$$

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？

解：

不，这不安全。一旦 Bob 泄露了他的私钥，Alice 就可以用它来分解他的模数 N。然后 Alice 可以破解 Bob 发送的任何消息。

以下是分解模量的一种方法：

设 $k = ed - 1$。则 $k$ 与 $0 \: mod$ 全等。在乘法组$Z(N)$中选择一个随机的 $x$。然后 $x^k \equiv 1 \: mod \: N$，这意味着$x^{k/2}$ 是 $1 \: mod \: N$ 的平方根。在 50% 的概率下，这是 N 的非平凡平方根，因此

$\gcd(x^{\frac{k}{2}} - 1, N)$将产生$N$的质因数。

如果$x^{k/2} = 1 \: mod \: N$，就尝试$x^{k/4}$，$x^{k/8}$，……

当且仅当某些 $i$ ， $x^{k/2^i} \equiv -1$ 时，此操作才会失败。如果失败，选择新的 $x$。

这将在预期的多项式时间内因子 $N$。

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$C$，改密文是用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$M$。

解：

请注意，因为$Z = r^e \: mod \: n$，所以$r = Z^d \: mod \: n$，Bob 计算：$tY \: mod \: n = r^{-1} X^d \: mod \: n = r^{-1} Z^d C^d \: mod \: n = C^d \: mod \: n = M$