Problem 1

(a)选择$p = 7, q = 13$，那么

$$\begin{gathered} n = pq = 91 \\ (p-1)(q-1) = 72 \end{gathered}$$

所以可以选择

$$e = 5$$

记

$$a = 72, b = 5$$

计算欧几里得除法：

$$\begin{aligned} a &= 14b + 2 \Rightarrow 2 = a - 14b \\ 5 &= 2 \times 2 + 1 \Rightarrow 1 = 5 - 2 \times 2 = b - 2 \times (a - 14b) = 29b - 2a \\ 2 &= 2 \times 1 + 0 \end{aligned}$$

所以

$$29 \times 5 - 2 \times 72 = 1$$

因此可以取

$$d = 29$$

(b)选择$m = 3$，加密后得到

$$\hat{m} = 3^5 \mod 91$$

计算后，我们有

$$\begin{aligned} 3^5 &\equiv 243 \\ &\equiv 61 \mod 91 \end{aligned}$$

所以

$$\hat{m} = 61$$

(c)

$$m = \hat{m}^d \equiv 61^{29} \mod 91$$

计算后，我们有

$$
\begin{aligned}
61^{29} &\equiv (-30)^{29} \\
&\equiv (-30) \times (900)^{14} \\
&\equiv (-30) \times (-10)^{14} \\
&\equiv (-30) \times (100)^{7} \\
&\equiv (-30) \times 9^{7} \\
&\equiv (-270) \times 81^{3} \\
&\equiv (-270) \times (-10)^{3} \\
&\equiv 2700 \times 100 \\
&\equiv 61 \times 9 \\
&\equiv (-30) \times 9 \\
&\equiv -270 \\
&\equiv 3 \mod 91
\end{aligned}
$$

Problem 2

(a)因为

$$\phi(n) = (p-1)(q-1)$$

并且已知e，注意d满足

$$ed \equiv 1 \mod (p-1)(q-1)$$

所以很容易计算出d。

(b)因为

$$
\begin{aligned}
\phi(n) = (p-1)(q-1) \\
n = pq
\end{aligned}
$$

所以

$$
\begin{aligned}
n - \phi(n) = p + q - 1 \\
p + q = n - \phi(n) + 1
\end{aligned}
$$

所以p,q是二次方程

$$x^2 - (n - \phi(n) + 1)x + n = 0$$

的两个根。

Problem 3

(a)如果m,n互质，那么

$$m^{\phi(n)} \equiv m^{(p-1)(q-1)} \equiv 1 \mod n$$

注意到我们有

$$ed \equiv 1 \mod (p-1)(q-1)$$

所以

$$ed = 1 + k(p-1)(q-1), k \in \mathbb{Z}$$

从而

$$m^{ed} \equiv m^{1+k(p-1)(q-1)} \equiv m \times \left(m^{(p-1)(q-1)}\right)^k \equiv m \mod n$$

(b)注意到我们有

$$a = 1 + k(p-1), k \in \mathbb{Z}$$

由欧拉定理，我们可得

$$m^{p-1} \equiv 1 \mod p$$

所以

$$m^a \equiv m^{1+k(p-1)} \equiv m \times \left(m^{(p-1)}\right)^k \equiv m \mod p$$

(c)如果

$$p_i | a - b, i = 1, \ldots, n$$

因为p_i为互不相同的质数，那么

$$\prod_{i=1}^{n} p_i | a - b$$

所以

$$a \equiv b \mod \prod_{i=1}^{n} p_i$$

(d)假设

$$n = \prod_{i=1}^{m} p_i$$

那么

$$\phi(n) = \prod_{i=1}^{m} (p_i - 1)$$

由条件可得

$$a = 1 + k \prod_{i=1}^{m} (p_i - 1), k \in \mathbb{Z}$$

所以

$$a \equiv 1 \mod p_i - 1, i = 1, \dots, m$$

由(b)可得

$$m^a \equiv m \mod p_i, i = 1, \dots, m$$

由(c)可得

$$m^a \equiv m \mod \prod_{i=1}^{m} p_i = n$$

因此

$$m^a \equiv m \mod n$$

对于RSA算法，

$$n = pq$$

所以原命题成立。