1) $m > 2$ users $m = 1000$

<u>symmetric key cryptosystem:</u>

$$\text{num Keys} = \binom{m}{2} = \frac{m(m-1)}{2} = \frac{1000(1000-1)}{2} = \boxed{499500}$$

<u>public key cryptosystem:</u>

- each user needs 2 keys (public/private)

$$\text{num keys} = m(2) = 1000(2) = \boxed{2000}$$

3) CRT

a) $x = 12 \bmod 25$ $\quad GCD(12,25)=1$

$x = 9 \bmod 26$ $\quad GCD(9,26)=1$

$x = 23 \bmod 27$ $\quad GCD(23,27)=1$

$M = 25 \cdot 26 \cdot 27 = 17550$

$a_1 = 12 \quad M_1 = \frac{17550}{25} = 702 \quad N_1 = 702^{-1} \bmod 25 \Rightarrow p = \frac{1}{702} \bmod 25 \Rightarrow 702p = 1 \bmod 25 \quad p = 13$

$N_1 = 13 \bmod 5$

$a_2 = 9 \quad M_2 = \frac{17550}{26} = 675 \quad N_2 = 675 \bmod 26 \Rightarrow 675p = 1 \bmod 26 = 25$

$N_2 = 25 \text{ m } 26$

$a_3 = 23 \quad M_3 = \frac{17550}{27} = 650 \quad N_3 = 650^{-1} \bmod 27 \Rightarrow 650p = 1 \bmod 27 = 14$

$N_3 = 14$

$x = (a_1 \cdot M_1 \cdot N_1 + a_2 M_2 N_2 + a_3 M_3 N_3) \bmod M$

$= (12 \cdot 702 \cdot 13 + 9 \cdot 675 \cdot 25 + 23 \cdot 650 \cdot 14) \bmod 17550$

$= 470687 \text{ m } 17550 = \boxed{14387 \text{ m } 17550}$

b) $13x = 4 \bmod 99$ $\quad 13 - 4 = 9$ which is a multiple of 99

$15x = 56 \bmod 101$ $\quad 15 - 56 = 41$ which is a mult of 101

$13^{-1} \bmod 99 \Rightarrow 13p = 1 \text{ m } 99 = 61 \text{ m } 99$

$15^{-1} \text{ m } 101 \Rightarrow 15p = 1 \text{ m } 101 = 27 \text{ m } 101$

$\Rightarrow$ $x = 61 \cdot 4 \bmod 99 = 244 \bmod 99 = 46 \bmod 99$

$x = 27 \cdot 56 \bmod 101 = 1512 \bmod 101 = 98 \bmod 101$

$M = 99 \cdot 101 = 9999$

$a_1 = 46 \quad m_1 = 9999/99 = 101 \quad N_1 = 101^{-1} \bmod 99 \Rightarrow 101p = 1 \text{ m } 99 \Rightarrow p = 50$

$N_1 = 50$

$a_2 = 98 \quad m_2 = 9999/101 = 99 \quad N_2 = 99^{-1} \bmod 101 \Rightarrow 99p = 1 \text{ m } 101 \Rightarrow p = 50$

$N_2 = 50$

$x = (a_1 m_1 N_1 + a_2 m_2 N_2) \text{ m } M$

$= (46 \cdot 101 \cdot 50 + 98 \cdot 99 \cdot 50) \text{ m } 9999$

$= 717400 \text{ m } 9999 = \boxed{7471 \bmod 9999}$

note if $x^2 = y^2 \mod n$ $x \not\equiv \pm y \mod n$ then $GCD(x-y, n)$ is non trivial factor of n

5) $n = 642401$

$516107^2 = 7 \mod n$ $187722^2 = 2^2 \cdot 7 \mod n$

$(516107^2 \cdot 187722^2) = 2^2\, 7 \cdot 7 \mod 642401$

$(9.688463825E10)^2 = 2^2 \cdot 7^2 \mod 642401$

mod 642401 $(289038)^2 = (14)^2 \mod 642401$

$GCD(x-y, n) = GCD(289038-14, 642401) = 1129$

$\Rightarrow$ 1129 is non-trivial factor of N

2^{nd} factor $= \frac{N}{1129} = \frac{642401}{1129} = 569$

$\boxed{\Rightarrow \text{prime factors of } N = 642401 \text{ are } (1129, 569)}$

$1129 \cdot 569 = 642401$

8) $PK = (p, \alpha, \beta)$ $SK = \alpha$ A chooses prime p and α of Z_p

A computes $\beta = \alpha^{\alpha}$

encryption m $E_{PK}(m,k) = c = (Y_1, Y_2)$ $Y_1 = \alpha^K \bmod p$

$Y_2 = m\beta^K \bmod p$

$$D_{SK}(c) = Y_2 (Y_1^{a})^{-1} \bmod p$$

$$E_{PK}(m_1, K_1) = (Y_1, Y_2)$$
$$E_{PK}(m_2, K_2) = (Y_3, Y_4)$$

B transmits $c = (Y_1 Y_3 \bmod p,\ Y_2 Y_4 \bmod p) \longrightarrow A$ (find message after A decrypts (P.T))

$$Y_1 Y_3 \bmod p = \alpha^{K_1} \alpha^{K_2} \bmod p = \alpha^{K_1 + K_2} \bmod p$$
$$Y_2 Y_4 \bmod p = m_1 \beta^{K_1} m_2 \beta^{K_2} \bmod p = m_1 m_2 \beta^{K_1 + K_2}$$

$$D_{SK}(c) = Y_2 (Y_1^{a})^{-1} \bmod p$$
$$D_{SK}(c) = (m_1 m_2 \beta^{(K_1+K_2)}) (\alpha^{a(K_1+K_2)})^{-1} \bmod p$$

because $\beta = \alpha^a$

$$D_{SK}(c) = (m_1 m_2 \alpha^{a(K_1+K_2)})(\alpha^{aK_1+K_2})^{-1} \bmod p$$
$$D_{SK}(c) = \frac{m_1 m_2 \cancel{\alpha^{a(K_1+K_2)}}}{\cancel{\alpha^{a(K_1+K_2)}}} \bmod p$$

$$\boxed{PT:\ D_{SK}(c) = m_1 m_2 \bmod p}$$