Aaron Hong
Prof. Poovendran
EE418 HW3
11/17/23

1. for symmetric key, there will need to be $999 + 998 + 997 + \dots + 2 + 1$ keys, which is $(499 \cdot 1000) + 500 = 499500$ keys
   for public key, there will need to be $2 \cdot 1000 = 2000$ keys

3. a $M = 25 \cdot 26 \cdot 27 = 17550$, $M_1 = 702 = 17550/25$
   $M_2 = 675$
   $M_3 = 650$

   $702^{-1} \bmod 25$, $702 = 28(25) + 2$, $25 = 12(2) + 1$
   $1 = 25 - 12(2) = 25 - 12(702 - 28(25))$
   $= 337(25) - 12(702)$
   $702^{-1} \bmod 25 = -12 = 13$

   $675^{-1} \bmod 26$, $675 = 25(26) + 25$, $26 = 1(25) + 1$
   $1 = 26 - 25 = 26 - (675 - 25(26))$
   $= 26(26) - 675$
   $675^{-1} \bmod 26 = -1 = 25$

   $650^{-1} \bmod 27$, $650 = 24(27) + 2$, $27 = 13(2) + 1$
   $1 = 27 - 13(2) = 27 - 13(650 - 24(27))$
   $= 25(27) - 13(650)$
   $650^{-1} \bmod 27 = -13 = 14$

   $X = (12 \cdot 702 \cdot 13) + (9 \cdot 675 \cdot 25) + (23 \cdot 650 \cdot 14) \bmod 17550$
   $= 109512 + 151875 + 209300 = 470687 \bmod 17550 = (14387) \bmod 17550$

   b. $13^{-1} \bmod 99$, $13 = 0(99) + 13$, $99 = 7(13) + 8$, $13 = 1(8) + 5$, $8 = 1(5) + 3$, $5 = 3 + 2$, $3 = 2 + 1$
   $1 = 3 - 2 = 3 - (5 - 3) = 2(3) - 5$
   $= 2(8 - 5) - 5 = 2(8) - 3(5)$
   $= 2(8) - 3(13 - 8) = 5(8) - 3(13)$
   $= 5(99 - 7(13)) - 3(13)$
   $= 5(99) - 35(13) - 3(13) = 5(99) - 38(13)$
   $13^{-1} \bmod 99 = -38 = 61$
   $13x = 4 \bmod 99 \rightarrow x = (4 \cdot 61) \bmod 99 = 241 \bmod 99 = 43 \bmod 99$

   $15^{-1} \bmod 101$, $101 = 6(15) + 11$, $15 = 1(11) + 4$, $11 = 2(4) + 3$, $4 = 1(3) + 1$
   $1 = 4 - 1(3) = 4 - (11 - 2(4)) = 3(4) - 11$
   $= 3(15 - 11) - 11 = 3(15) - 4(11)$
   $= 3(15) - 4(101 - 6(15)) = 27(15) - 4(101)$
   $15^{-1} \bmod 101 = 27$
   $15x = 56 \bmod 101 \rightarrow x = (56 \cdot 27) \bmod 101 = 1512 \bmod 101$
   $= 98 \bmod 101$

2. b. $x = 43 \bmod 99$, $x = 98 \bmod 101$, $M = 99 \cdot 101 = 9999$, $M_1 = 101$, $M_2 = 99$

$101^{-1} \bmod 99$, $101 = 1(99) + 2$ $\quad 1 = 99 - 49(2) = 99 - 49(101 - 99)$

$99 = 49(2) + 1$ $\quad = 50(99) - 49(101)$

$101^{-1} \bmod 99 = 50$

$99^{-1} \bmod 101$, $101 = 1(99) + 2$ $\quad 1 = 50(99) - 49(101)$

$99 = 49(2) + 1$ $\quad 99^{-1} \bmod 101 = 50$

$x = (43 \cdot 101 \cdot 50) + (98 \cdot 99 \cdot 50) \bmod 9999 = 217150 + 485100 = 702250 \bmod 9999$

$= \boxed{2320 \bmod 9999}$

5 $516107^2 = 7 \bmod 642401$, $187722^2 = 2^2 \cdot 7 \bmod 642401$

$187722/2 = 90000 + 3500 + 350 + 11 = 93861 \rightarrow 93861^2 = 7 \bmod 642401$

$516107 \cdot 93861 = 48442819127 \rightarrow 48442819127 - 7 = 48442819120$

$48442819120 = 75408(642401) + 144512$

$642401 = 4(144512) + 64353$

$144512 = 2(64353) + 15806$

$64353 = 4(15806) + 1129$

$15806 = 14(1129) + 0 \longrightarrow \boxed{642401 = 1129 \cdot 569}$

8 $c = (y_1 y_3 \bmod p,\ y_2 y_4 \bmod p)$, $D(c) = y_2 y_4 ((y_1 y_3)^a)^{-1} = y_2 (y_1^a)^{-1} \cdot y_4 (y_3^a)^{-1}$

$= m_1 \bmod p \cdot m_2 \bmod p$