$PK = Y_A = a^{x_A} \bmod 2$
$= 7^{16} \bmod 15$
$= 1$

Given $q = 15,\ m = 13,\ k = 31$

$\gcd(k, q-1) = 1 \Rightarrow \gcd(31, 14) = 1$

Temp key: $S_1 = a^k \bmod q$
$= 7^{31} \bmod 15$
$= 13$

$k^{-1} = k \bmod (q-1) = 61 \bmod 14 = 5$

$S_2 = k^{-1}(m - x_A S_1) \bmod (q-1)$
$= 5(73 - 16 \times 3) \bmod 14$
$= 9$

verification:
$V_1 = a^m \bmod q = 7^{13} \bmod 15 = 7$
$V_2 = Y_A^{S_1} S_1^{S_2} = 1^{13}\ 13^9 \bmod 15 = 13$

Soln

iii.3: $k1(u1 \cdot v) + k2(u2 \cdot v)$.

$u1 \cdot v \Rightarrow (2, 4, 5) \cdot (5, 3, 2) = (2 \cdot 5 + 4 \cdot 3 + 5 \cdot 2) = (10 + 12 + 10) = 32$

$u2 \cdot v \Rightarrow (7, 1, 2) \cdot (5, 3, 2) = (7 \cdot 5 + 1 \cdot 3 + 2 \cdot 2) = (35 + 3 + 4) = 42$

$k1(u1 \cdot v) = 3 \times 32 = 96$

$k2(u2 \cdot v) = 4 \times 42 = 168$

$\therefore k1(u1 \cdot v) + k2(u2 \cdot v) = 96 + 168 = \underline{\underline{264}}$

$x \equiv 3 \pmod 4$ $\quad a_1 = 3$

$x \equiv 4 \pmod 7$ $\quad a_2 = 4$

$x \equiv 1 \pmod 9$ $\quad a_3 = 1$

~~$x \equiv 0 \pmod{11}$ $\quad a_4 = 0$~~

$M = 2772$ $\quad m_1 = 4$

$M_1 = 693$ $\quad m_2 = 7$

$M_2 = 369$ $\quad m_3 = 9$

$M_3 = 308$

~~$M_4 =$~~

$M_1 y_1 \equiv 1 \pmod{m_1}$ $\quad M_2 y_2 \equiv 1 \pmod{m_2}$

$693 y_1 \equiv 1 \pmod 4$ $\quad 369 y_2 \equiv 1 \pmod 7$

$y_1 = 1$ $\quad y_2 = 3$

$M_3 y_3 \equiv 1 \pmod{m_3}$

$308 \times y_3 \equiv 1 \pmod 9$

$y_3 = 5$

$x = 693 \times 3 \times 1 + 369 \times 3 \times 4 + 308 \times 5 \times 1 \pmod{2772}$

$8047 \pmod{2772}$

$x \equiv 3 \pmod 5$
$x \equiv 1 \pmod 7$
$x \equiv 6 \pmod 8$

$a_1 = 3$ $m_1 = 5$
$a_2 = 1$ $m_2 = 7$
$a_3 = 6$ $m_3 = 8$

$M = 5 \times 7 \times 8 = 280$

$M_1 = \frac{280}{5} = 56$

$M_2 = \frac{280}{7} = 40$

$M_3 = \frac{280}{8} = 35$

$x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \pmod M$

$M_1 y_1 \equiv 1 \pmod{m_1}$

$56 y_1 \equiv 1 \pmod 5$

$1 y_1 \equiv 1 \pmod 5$

$y_1 = 1$

$M_2 y_2 \equiv 1 \pmod{m_2}$

$40 y_2 \equiv 1 \pmod 7$
$5 y_2 = 1 \pmod 7$
$15 y_2 \equiv 3 \pmod 7$
$1 y_2 \equiv 3 \pmod 7$

$y_2 = 3$

$M_3 y_3 \equiv 1 \pmod{m_3}$
$35 y_3 \equiv 1 \pmod 8$
$3 y_3 \equiv 1 \pmod 8$
$9 y_3 \equiv 3 \pmod 8$
$1 y_3 \equiv 3 \pmod 8$
$y_3 = 3$

$x = 3 \times 56 \times 1 + 1 \times 40 \times 3 + 6 \times 35 \times 3 \pmod{280}$
$= 918 \pmod{280}$