Q - 4:

$p = 6961$, $g = 437$, $s = 6104$

- What is the value of v?

  $v = g^s = 437^{6104} \pmod{6961}$

  $v = 2065$

- $m = 5584$, $e = 4451$

  $S_1 \equiv g^e \equiv 437^{4451} \pmod{6961}$

  $S_1 \equiv 3534$

  $S_2 \equiv (m - sS_1)\, e^{-1} \pmod{p - 1}$

  $S_2 \equiv [5584 - (6104)(3534)]\, e^{-1} \pmod{6960}$

  $S_2 \equiv [5584 - 21571536]\,(491) \pmod{6960}$

  $\{e^{-1} = 491,\ 491 * 4451 \bmod(6960) = 1\}$

  $S_2 \equiv [5584 - 21571536]\,(491) \pmod{6960}$

  $S_2 \equiv -10588882432 \pmod{6960}$

  $S_2 \equiv 5888$

  $(S_1 , S_2) = (3534, 5888)$