$p = 2q + 1 = 23$

$q = 11$

$g = 2$

$sk = a = 7$

$pk = g^{sk} = 2^7 \bmod p = 128 \bmod 23 = 13$

$k = g^k \bmod p = 2^4 \bmod p = 16 \bmod 23 = 16$

$s_1 = r_0$

$s_2 = k - a \cdot s_1 \bmod q = 4 - 7 \cdot 10 = 4 - 70 = -66 \bmod q = -66 \bmod 11 = 0$

$s = (s_1, s_2) = (10, 0)$

$H(m \| g^{s_2} (pk)^{s_1} \bmod p)$

$= H(m \| 2^0 \cdot 13^{10} \bmod 23)$

$= H(m \| 16)$

$= H(m \| k)$

$= s_1$ ✓

$13^{10} \bmod 23$

$= \ldots$

$10 = [1010]_2$

$(((13)^2 \cdot 13)^2)^2 \bmod 23$

$= ((16 \cdot 9)^2 \cdot 13)^2 \bmod 23$

$= ((8)^2 \cdot 13)^2 \bmod 23$

$= (64 \cdot 13)^2 \bmod 23$

$= (18 \cdot 13)^2 \bmod 23$

$= 234^2 \bmod 23$

$= 54756 \bmod 23$

$= 16 \bmod 23$

---

now, $s_1' = H(m' \| k) = 11$

$s_2' = k - a \cdot s_1' \bmod q = 4 - 7 \cdot 11 = 4 - 77 = -73 \bmod 11 = 4$

$(s_1', s_2') = (11, 4)$

$k - a \cdot s_1 \bmod q = 4$

$k - a \cdot s_2 \bmod q = 0$ → [illegible]

$k = 4 + a \cdot s_1' \bmod 11$

$k = 0 + a \cdot s_1 \bmod 11$ → $a \cdot s_1' + 4 = a \cdot s_1 \bmod 11$

$a \cdot (s_1' - s_1) = -4 \bmod 11$

$a = \frac{-4}{s_1' - s_1} \bmod 11$

$= \frac{-4}{11 - 10} = \frac{-4}{1} \bmod 11 = -4 \bmod 11$

$= 7$ ✓