Student Number: [redacted] Name: Bryan Hoang

7. (10 points)

(a) **Answer:**
Samantha's public verification key is

$$\begin{aligned} A &\equiv g^a \pmod{p} \\ &\equiv 4488^{674} \pmod{22531} \\ &\equiv 4940 \pmod{22531}. \end{aligned}$$

(b) **Answer:**

$$\begin{aligned} S_1 &\equiv (g^k \pmod{p}) \pmod{q} \\ &\equiv (4488^{574} \pmod{22531}) \pmod{751} \\ &\equiv 444 \pmod{751}, \\ S_2 &\equiv (D + aS_1)k^{-1} \pmod{q} \\ &\equiv (244 + 674 \cdot 444)574^{-1} \pmod{751} \\ &\equiv (602)297 \pmod{751} \\ &\equiv 56 \pmod{751}. \end{aligned}$$

Therefore, the signature is $\boxed{(444, 56)}$.