Student Number: [redacted] Name: Bryan Hoang

5. (10 points)

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

$$\begin{aligned} A &\equiv g^s \pmod{p} \\ &\equiv 437^{6104} \pmod{6961} \\ &\boxed{\equiv 2065 \pmod{6961}}. \end{aligned}$$

(b) **Answer:**

$$\begin{aligned} S_1 &\equiv D^k \pmod{p} \\ &\equiv 437^{4451} \pmod{6961} \\ &\equiv 3534 \pmod{6961}, \\ S_2 &\equiv (D - aS_1)k^{-1} \pmod{p-1} \\ &\equiv (5584 - 6104 \cdot 3534)4451^{-1} \pmod{6960} \\ &\equiv (5584 - 2496)491 \pmod{6960} \\ &\equiv 5888 \pmod{6960}. \end{aligned}$$

Therefore, the signature is $\boxed{(3534, 5888)}$.