Student Number: [redacted] Name: Bryan Hoang

6. (10 points) **Answer:**

Verifying the signature (S_1, S_2) yields

$$\begin{aligned} A^{S_1} S_1^{S_2} &\equiv 4250^{4129} \cdot 4129^{5575} \pmod{6961} \\ &\equiv 231 \pmod{6961}, \\ g^D &\equiv 437^{1521} \pmod{6961} \\ &\equiv 231 \pmod{6961}, \\ \Rightarrow A^{S_1} S_1^{S_2} &\equiv g^D \pmod{p}. \end{aligned}$$

Therefore, $\boxed{\text{the signature } (S_1, S_2) \text{ is valid}}$.

Verifying the signature (S_1', S_2') yields

$$\begin{aligned} A^{S_1'} S_1'^{S_2'} &\equiv 4250^{3145} \cdot 3145^{1871} \pmod{6961} \\ &\equiv 6208 \pmod{6961}, \\ g^D &\equiv 437^{1837} \pmod{6961} \\ &\equiv 2081 \pmod{6961}, \\ \Rightarrow A^{S_1'} S_1'^{S_2'} &\not\equiv g^D \pmod{p}. \end{aligned}$$

Therefore, $\boxed{\text{the signature } (S_1', S_2') \text{ is not valid}}$.

Verifying the signature (S_1'', S_2'') yields

$$\begin{aligned} A^{S_1''} S_1''^{S_2''} &\equiv 4250^{2709} \cdot 2709^{2994} \pmod{6961} \\ &\equiv 2243 \pmod{6961}, \\ g^D &\equiv 437^{1614} \pmod{6961} \\ &\equiv 2243 \pmod{6961}, \\ \Rightarrow A^{S_1''} S_1''^{S_2''} &\equiv g^D \pmod{p}. \end{aligned}$$

Therefore, $\boxed{\text{the signature } (S_1'', S_2'') \text{ is valid}}$.