Name: $\qquad$
Directions: Show all work. No credit for answers without work.

1. [2 points] Compute $\log _{6}(2)$ in $\mathbb{F}_{13}$.
2. [2 points] Suppose that $g_{1}$ is a primitive root in $\mathbb{F}_{p}$ and $g_{2}$ is not. What is different between the functions $\log _{g_{1}}(y)$ and $\log _{g_{2}}(y)$ ?
3. [2 parts, 3 points each] You want to use the Diffie-Hellman protocol to share a private key with your friend. You and your friend agree to use prime $p=11$ and base $g=2$.
(a) You choose the random element 8 . What do you send to your friend?
(b) Your friend responds with the number 5. What is your shared secret?
