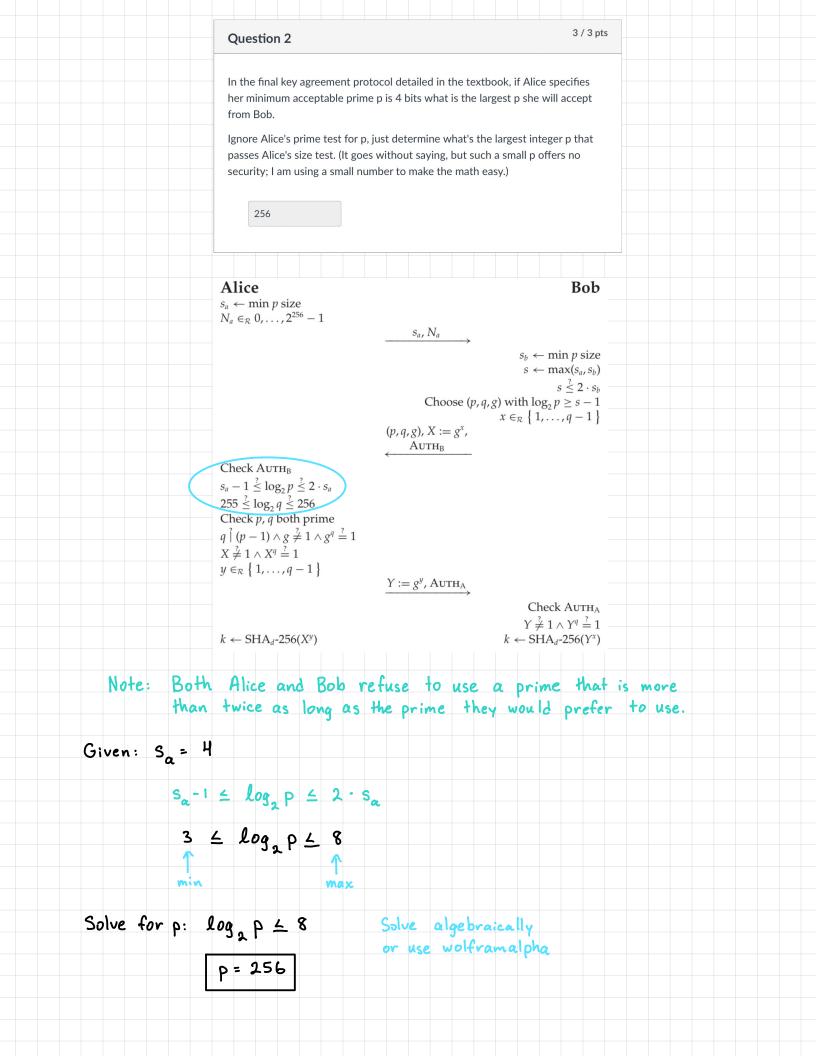
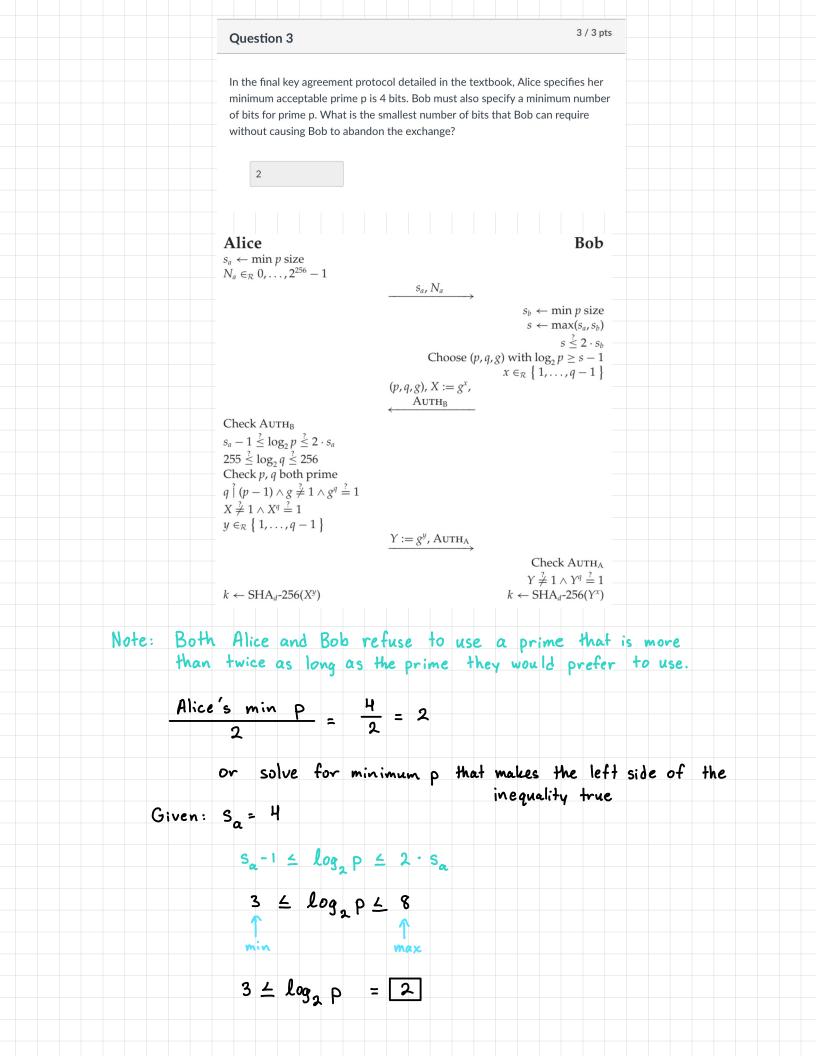
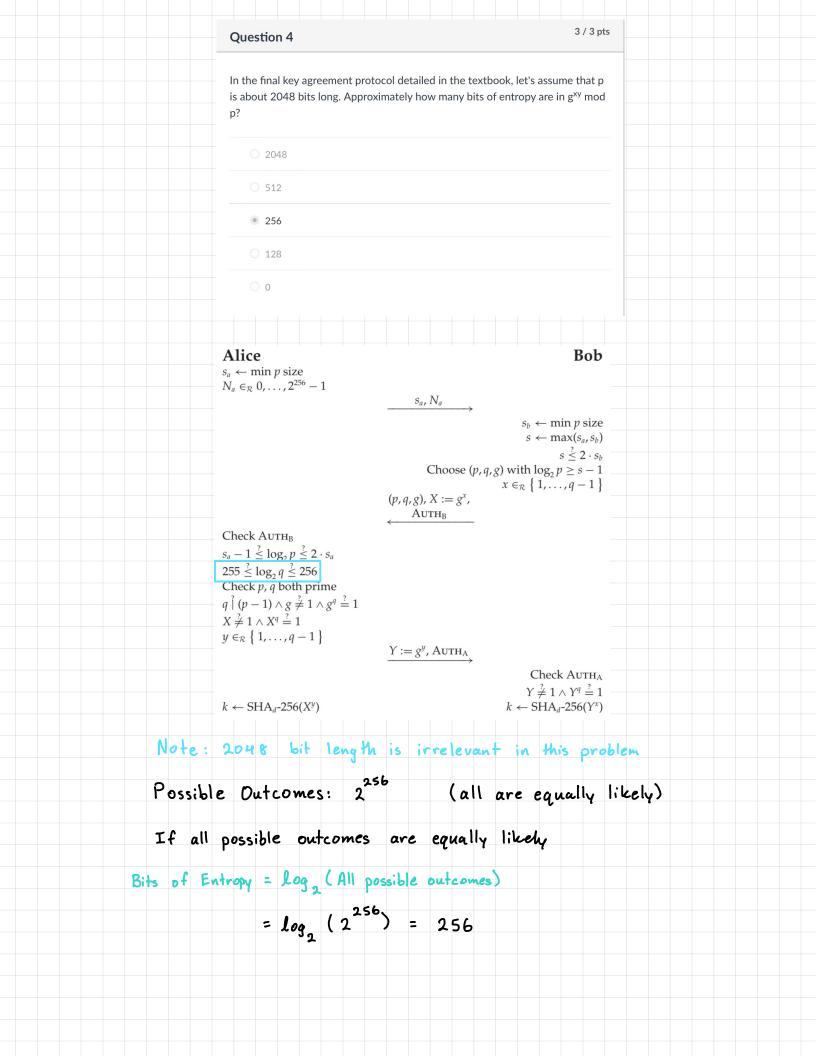
Question 1 3 / 3 pts
In the final key agreement protocol detailed in the textbook, if Alice specifies her minimum acceptable prime p is 4 bits what is the smallest p she will accept from Bob.
Ignore Alice's prime test for p, just determine what's the smallest integer p that passes Alice's size test. (It goes without saying, but such a small p offers no security; I am using a small number to make the math easy.)
8
Alice declares her minimum acceptable prime p is 4 bits
the smallest p she would accept from Bob is 11
however we are asked to ignore Alice's prime test
for p The smallest p of length 4 bits is 8
in binary 8 = 1000







3 / 3 pts **Question 5** In the final key agreement protocol detailed in the textbook, let's assume that p is about 2048 bits long. Approximately how many bits of entropy are in k? 2048 0 512 256 0 128 0 Alice Bob $s_a \leftarrow \min p \text{ size}$ $N_a \in_{\mathcal{R}} 0, \ldots, 2^{256} - 1$ s_a , N_a $s_b \leftarrow \min p \text{ size}$ $s \leftarrow \max(s_a, s_b)$ $s \stackrel{?}{\leq} 2 \cdot s_b$ Choose (p, q, g) with $\log_2 p \ge s - 1$ $x \in_{\mathcal{R}} \left\{ 1, \ldots, q-1 \right\}$ $(p,q,g), X := g^x,$ $Auth_B$ Check AUTHB $s_a - 1 \stackrel{?}{\leq} \log_2 p \stackrel{?}{\leq} 2 \cdot s_a$ $255 \stackrel{?}{\leq} \log_2 q \stackrel{?}{\leq} 256$ Check p, q both prime $q \mid (p-1) \land g \neq 1 \land g^q \stackrel{?}{=} 1$ $X \stackrel{?}{\neq} 1 \wedge X^q \stackrel{?}{=} 1$ $y \in_{\mathcal{R}} \left\{ 1, \ldots, q-1 \right\}$ $Y := g^y$, AUTH_A Check Autha $Y \stackrel{?}{\neq} 1 \wedge Y^q \stackrel{?}{=} 1$ $k \leftarrow \mathrm{SHA}_d\text{-}256(Y^x)$ $k \leftarrow \text{SHA}_d\text{-256}(X^y)$ Note: 2048 bit length is irrelevant in this problem Entropy = min length of the output of the hash function or Entropy = Entropy going into the hash function from the previous problem, we know that 256 bits of Entropy is coming in : k has 256 bits of Entropy

