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

Question 2

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 largest p she will accept from Bob.

Ignore Alice's prime test for p, just determine what's the largest 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.)

256

Alice		**Bob**
$s_a \leftarrow \min p$ size		
$N_a \in_{\mathcal{R}} 0, \ldots, 2^{256} - 1$		
	$\xrightarrow{s_a,\, N_a}$	
		$s_b \leftarrow \min p$ size
		$s \leftarrow \max(s_a, s_b)$
		$s \overset{?}{\leq} 2 \cdot s_b$
		Choose (p, q, g) with $\log_2 p \geq s - 1$
		$x \in_{\mathcal{R}} \{1, \ldots, q-1\}$
	$\xleftarrow{(p,q,g),\, X := g^x,\, \text{AUTH}_B}$	
Check AUTH_B		
$s_a - 1 \overset{?}{\leq} \log_2 p \overset{?}{\leq} 2 \cdot s_a$		
$255 \overset{?}{\leq} \log_2 q \overset{?}{\leq} 256$		
Check p, q both prime		
$q \overset{?}{\mid} (p-1) \wedge g \overset{?}{\neq} 1 \wedge g^q \overset{?}{=} 1$		
$X \overset{?}{\neq} 1 \wedge X^q \overset{?}{=} 1$		
$y \in_{\mathcal{R}} \{1, \ldots, q-1\}$		
	$\xrightarrow{Y := g^y,\, \text{AUTH}_A}$	
		Check AUTH_A
		$Y \overset{?}{\neq} 1 \wedge Y^q \overset{?}{=} 1$
$k \leftarrow \text{SHA}_d\text{-}256(X^y)$		$k \leftarrow \text{SHA}_d\text{-}256(Y^x)$

Note: Both Alice and Bob refuse to use a prime that is more than twice as long as the prime they would prefer to use.

Given: $s_a = 4$

$$s_a - 1 \leq \log_2 p \leq 2 \cdot s_a$$

$$\underset{\text{min}}{3} \leq \log_2 p \leq \underset{\text{max}}{8}$$

Solve for p: $\log_2 p \leq 8$

$$\boxed{p = 256}$$

Solve algebraically
or use wolframalpha

Question 3 — 3 / 3 pts

In the final key agreement protocol detailed in the textbook, Alice specifies her minimum acceptable prime p is 4 bits. Bob must also specify a minimum number of bits for prime p. What is the smallest number of bits that Bob can require without causing Bob to abandon the exchange?

2

Alice | **Bob**

$s_a \leftarrow \min p$ size

$N_a \in_{\mathcal{R}} 0, \ldots, 2^{256}-1$

$\xrightarrow{s_a,\, N_a}$

$s_b \leftarrow \min p$ size

$s \leftarrow \max(s_a, s_b)$

$s \overset{?}{\leq} 2 \cdot s_b$

Choose (p, q, g) with $\log_2 p \geq s - 1$

$x \in_{\mathcal{R}} \{1, \ldots, q-1\}$

$\xleftarrow[\textsc{Auth}_B]{(p,q,g),\, X := g^x,}$

Check $\textsc{Auth}_B$

$s_a - 1 \overset{?}{\leq} \log_2 p \overset{?}{\leq} 2 \cdot s_a$

$255 \overset{?}{\leq} \log_2 q \overset{?}{\leq} 256$

Check p, q both prime

$q \overset{?}{\mid} (p-1) \wedge g \overset{?}{\neq} 1 \wedge g^q \overset{?}{=} 1$

$X \overset{?}{\neq} 1 \wedge X^q \overset{?}{=} 1$

$y \in_{\mathcal{R}} \{1, \ldots, q-1\}$

$\xrightarrow{Y := g^y,\, \textsc{Auth}_A}$

Check $\textsc{Auth}_A$

$Y \overset{?}{\neq} 1 \wedge Y^q \overset{?}{=} 1$

$k \leftarrow \text{SHA}_d\text{-}256(X^y)$ | $k \leftarrow \text{SHA}_d\text{-}256(Y^x)$

Note: Both Alice and Bob refuse to use a prime that is more than twice as long as the prime they would prefer to use.

$$\frac{\text{Alice's min } p}{2} = \frac{4}{2} = 2$$

or solve for minimum p that makes the left side of the inequality true

Given: $s_a = 4$

$$s_a - 1 \leq \log_2 p \leq 2 \cdot s_a$$

$$3 \leq \log_2 p \leq 8$$

min | max

$$3 \leq \log_2 p = \boxed{2}$$

Question 4

3 / 3 pts

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 g^{xy} mod p?

- ○ 2048
- ○ 512
- ● 256
- ○ 128
- ○ 0

Alice		Bob
$s_a \leftarrow$ min p size		
$N_a \in_{\mathcal{R}} 0, \ldots, 2^{256} - 1$		
	$\xrightarrow{s_a, N_a}$	
		$s_b \leftarrow$ min p size
		$s \leftarrow \max(s_a, s_b)$
		$s \overset{?}{\leq} 2 \cdot s_b$
		Choose (p, q, g) with $\log_2 p \geq s - 1$
		$x \in_{\mathcal{R}} \{1, \ldots, q-1\}$
	$\xleftarrow[\text{AUTH}_B]{(p, q, g),\, X := g^x,}$	
Check AUTH_B		
$s_a - 1 \overset{?}{\leq} \log_2 p \overset{?}{\leq} 2 \cdot s_a$		
$\boxed{255 \overset{?}{\leq} \log_2 q \overset{?}{\leq} 256}$		
Check p, q both prime		
$q \overset{?}{\mid} (p-1) \wedge g \overset{?}{\neq} 1 \wedge g^q \overset{?}{=} 1$		
$X \overset{?}{\neq} 1 \wedge X^q \overset{?}{=} 1$		
$y \in_{\mathcal{R}} \{1, \ldots, q-1\}$		
	$\xrightarrow{Y := g^y,\, \text{AUTH}_A}$	
		Check AUTH_A
		$Y \overset{?}{\neq} 1 \wedge Y^q \overset{?}{=} 1$
$k \leftarrow \text{SHA}_d\text{-256}(X^y)$		$k \leftarrow \text{SHA}_d\text{-256}(Y^x)$

Note: 2048 bit length is irrelevant in this problem

Possible Outcomes: 2^{256} (all are equally likely)

If all possible outcomes are equally likely

Bits of Entropy = $\log_2$ (All possible outcomes)

$= \log_2(2^{256}) = 256$

Question 5

3 / 3 pts

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
- ( ) 512
- (•) 256
- ( ) 128
- ( ) 0

Alice | **Bob**

Alice:
$s_a \leftarrow \min p \text{ size}$
$N_a \in_{\mathcal{R}} 0, \ldots, 2^{256} - 1$

$\xrightarrow{s_a,\, N_a}$

Bob:
$s_b \leftarrow \min p \text{ size}$
$s \leftarrow \max(s_a, s_b)$
$s \overset{?}{\leq} 2 \cdot s_b$
Choose (p, q, g) with $\log_2 p \geq s - 1$
$x \in_{\mathcal{R}} \{1, \ldots, q - 1\}$

$\xleftarrow{(p, q, g),\, X := g^x,\, \text{AUTH}_\text{B}}$

Alice:
Check AUTH_B
$s_a - 1 \overset{?}{\leq} \log_2 p \overset{?}{\leq} 2 \cdot s_a$
$255 \overset{?}{\leq} \log_2 q \overset{?}{\leq} 256$
Check p, q both prime
$q \overset{?}{\mid} (p - 1) \wedge g \overset{?}{\neq} 1 \wedge g^q \overset{?}{=} 1$
$X \overset{?}{\neq} 1 \wedge X^q \overset{?}{=} 1$
$y \in_{\mathcal{R}} \{1, \ldots, q - 1\}$

$\xrightarrow{Y := g^y,\, \text{AUTH}_\text{A}}$

Bob:
Check AUTH_A
$Y \overset{?}{\neq} 1 \wedge Y^q \overset{?}{=} 1$

Alice: $k \leftarrow \text{SHA}_d\text{-256}(X^y)$ | Bob: $k \leftarrow \text{SHA}_d\text{-256}(Y^x)$

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

$\therefore$ k has 256 bits of Entropy

Question 6

5 / 5 pts

Which of the following are contained in a public-key infrastructure certificate? Check all that apply.

- [ ] Owner's secret key
- [x] Owner's public key
- [x] Owner's name
- [ ] A signature from the owner
- [ ] Issuer's secret key
- [ ] Issuer's public key
- [x] Issuer's name
- [x] A signature from the issuer