Question 1

4 / 4 pts

Let's say that Alice and Bob are exchanging keys using Diffie-Hellman key exchange using multiplicative group Z^*_{499} and generator g=10. Let's say that Alice chooses secret exponent x=4 and receives the number 123 from Bob.

What number should Alice send to Bob? 20

What number do Alice and Bob compute as their shared secret?

331

Express each of your answers as an integer.

$p = 499$, $g = 10$

Alice — $b = 123$ ← — Bob

chooses $x = 4$ — chooses $y = ?$

a) $a = g^x \bmod p$

$a = 10^4 \bmod 499 = 20$

b) Shared key formula for Diffie-Hellman exchange is,

Shared Key $= a^y \bmod p = b^x \bmod p$

$b^x \bmod p = 123^4 \bmod 499 = 331$

Question 2

4 / 4 pts

Consider the multiplicative group Z^*_{22}.

List all of its elements in increasing numerical order, separating each with a comma but no space. 1,3,5,7,9,13,15,17,1

List all of the elements in the subgroup generated by 5 in this group, listed in increasing numerical order, separating each with a comma but no space.

1,3,5,9,15

Z^*_{22} does have at least one element that generates the entire group (ie, a "primitive" element). Tell me one. 7

a) $22 = 2 \cdot 11$

1, ~~2~~, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, 9, ~~10~~, ~~11~~, ~~12~~, 13, ~~14~~, 15, ~~16~~, 17,

~~18~~, 19, ~~20~~, 21, ~~22~~

b)

$5^1 \bmod 22 = 5$
$5^2 \bmod 22 = 3$
$5^3 \bmod 22 = 15$
$5^4 = 9$
$5^5 = 1$

c)

$7^1 \bmod 22 = 7$
$7^2 \bmod 22 = 5$
$7^3 = 13$
$7^4 = 3$
$7^5 = 21$
$7^6 = 15$
$7^7 = 17$
$7^8 = 9$
$7^9 = 19$
$7^{10} = 1$

1, 3, 5, 7, 9, 13, 15, 17, 19, 21

Question 3

4 / 4 pts

Let's say that you wanted to find a subgroup of size 50 to 60 elements of the group Z*p where p is 100 to 110 following the technique seen in class.

What p would you choose? 107

What size subgroup would you find? 53

What number do you find that generates the subgroup? 4

You may find this list of primes useful: https://primes.utm.edu/lists/small/1000.txt

Input into program

Question 4

4 / 4 pts

Let's say your Elgamal public key is (p, g, g^d mod p) = (13, 2, 3) and your private key is d = 4.

You receive a ciphertext (kx mod p, g^e mod p) = (6, 4).

What is the shared k value? 9

What is k^{-1} mod p? 3

What is the plaintext x? 5

Type each of your answers as an integer.

$p = 13 \quad g = 2$

$g^d \bmod p = 3 \; ; \; e = 3$

$d = 4$

a) given:

$C_1 = g^e \bmod p \qquad C_1 = g^e \bmod p = 4$

$C_2 = kx \bmod p \qquad C_2 = kx \bmod p = 6$

$k = c_1^d \bmod p$

$= 4^4 \bmod 13$

$= 9$

b) $k^{-1} \bmod p = 9^{-1} \bmod 13 = 3$

c) $x = c_2 \cdot k^{-1} \bmod p$

$= 6 \cdot 3 \bmod 13$

$= 5$

Question 5

0 / 4 pts

Consider the elliptic-curve group defined by { (x,y) | x,y ∈ Z_{17} and x^2 mod 17 = x^3 + 2x + 2 mod 17 } (ie, the group you get when a=2, b=2, and p=17).

What is (0,11) + (5,1) in this group?

What value do you get for s?

What value do you get for x_3?

What value do you get for y_3?

You may find these slides useful: https://www.crypto-textbook.com/download/Understanding_Cryptography_Chptr_9---ECC.pdf

$x_3 = s^2 - x_1 - x_2 \mod p$ $\quad y_3 = s(x_1 - x_3) - y_1 \mod p$

where

$$s = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \mod p & ; \text{ if } P \neq Q \text{ (point addition)} \\ \frac{3x_1^2 + a}{2y_1} \mod p & ; \text{ if } P = Q \text{ (point doubling)} \end{cases}$$

a) $s = \frac{1 - 11}{5 - 0} \mod 17 = 15$

b) $x_3 = (15)^2 - 0 - 5 \mod 17$

$= 16$

c) $y_3 = 15(0 - 16) - 11 \mod 17$

$= 4$