Question 1

4 / 4 pts

Let's say you generated RSA keys and you chose p=103, q=151, and the smallest encryption exponent that qualifies for this p and q. (You will have to follow the key generation algorithm to fill in the details.)

If someone gives you 343 as the ciphertext they created using your public key, what is the plaintext you get when you use your private key to decrypt?

You may use https://www.wolframalpha.com to help with this quiz. Some example queries that might be useful are "34^20 mod 123", "gcd(23, 25)", "123 prime?", "order of 7 mod 15", "inverse of 5 mod 13".

What is the encryption exponent? 7

What is the decryption exponent? 8743

What is the resulting plaintext? 9540

$p = 103$, $q = 151$, $e = ?$

$\Phi(n) = (p-1)(q-1) = (102)(150) = 15,300$

$\gcd(e, 15,300) = 1$

$\gcd(7, 15,300) = 1 \quad \therefore e = 7$

Given: ciphertext = 343

plaintext = ?, $d = ?$

$d = e^{-1} \bmod \Phi(n)$

$d = 7^{-1} \bmod 15,300 = 8743$

To decrypt: $x = y^d \bmod n$ $\qquad n = pq$

$x = 343^{8743} \bmod 15,553 \qquad n = (103)(151) = 15553$

$x = 9540$

Question 2

4 / 4 pts

Consider the multiplicative group Z^*_{18}.

List all of its elements in increasing numerical order, separating each with a comma but no space. 1,5,7,11,13,17

List all of the elements generated by 7 in this group, listed in increasing numerical order, separating each with a comma but no space.

1,7,13

Z^*_{18} does have at least one element that generates the entire group (ie, a "primitive" element). Tell me one. 5

a) $18 = 2 \cdot 3^2$

~~0~~ 1 ~~2~~ ~~3~~ ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ 10

11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~

1, 5, 7, 11, 13, 17

b) $7^1 \bmod 18 = 7$

$7^2 \bmod 18 = 13$

$7^3 \bmod 18 = 1$

$\therefore$ 1, 7, 13

c)

$5^1 \bmod 18 = 5$
$5^2 \bmod 18 = 7$
$5^3 \bmod 18 = 17$
$5^4 \bmod 18 = 13$
$5^5 \bmod 18 = 11$
$5^6 \bmod 18 = 1$

1, 5, 7, 11, 13, 17 ⇐ generator

$7^1 \bmod 18 = 7$
$7^2 \bmod 18 = 13$
$7^3 \bmod 18 = 1$

1, 7, 13

$11^1 \bmod 18 = 11$
$11^2 \bmod 18 = 13$
$11^3 \bmod 18 = 17$
$11^4 \bmod 18 = 7$
$11^5 \bmod 18 = 5$
$11^6 \bmod 18 = 1$

1, 5, 7, 11, 13, 17 ⇐ generator

$13^1 \bmod 18 = 13$
$13^2 \bmod 18 = 7$
$13^3 \bmod 18 = 1$

1, 7, 13

$17^1 \bmod 18 = 17$
$17^2 \bmod 18 = 1$

1, 17

Question 3

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=7. Let's say that Alice chooses secret exponent x=5 and receives the number 123 from Bob.

What number should Alice send to Bob? 340

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

294

Express each of your answers as an integer.

$p = 499, \quad g = 7$

Alice — $b = 123$ ← — Bob

chooses $x = 5$ — chooses $y = ?$

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

$a = 7^5 \bmod 499 = 340$

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

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

$b^x \bmod p = 123^5 \bmod 499 = 294$

Question 4

4 / 4 pts

Let's say that you wanted to find a subgroup of size 10 to 15 elements of a group Z^*_p where p is 50 to 60 following the technique seen in class.

What p would you choose? 53

What size subgroup would you find? 13

What number do you find that generates the subgroup? 16

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

Choose q: 13 * q must be prime

Choose p: Wolfram: "primes between 50 and 60"

Primes available between 50 to 60 are 53 and 59

we will use 53

q = 13 p = 53

Find generator of subgroup of size q:

$p = Nq + 1$

$N = \frac{p-1}{q} = \frac{53-1}{13} = 4$ N = 4 g = ?

Algorithm:

```
for (i=2; i< p ; i++)
   if(i^N mod p != 1)
      g = i^N mod p
      exit
```

$2^4 = 16 != 1$ ✓

g = 16

Verify Algorithm: (Python)

```
[ g **i % p for i in range(1, q+1)]
```

*Last element should be the only 1 in the list

```
[16 ** i % 53 for i in range(1, 14)]
```

Result: [16, 44, 15, 28, 24, 13, 49, 42, 36, 46, 47, 10, 1]

Question 5

4 / 4 pts

Decrypt ciphertext (kx mod p = 7, g^e mod p = 8). The ciphertext was created using Elgamal encryption over group Z^*_p with your public key (p=13, g=2, g^d mod p=12) and your private key is d=6.

What is the shared k value? 12

What is k^{-1} mod p? 12

What is the plaintext x? 6

Type each of your answers as an integer.

$p = 13 \quad g = 2$

$g^d \bmod p = 12 \quad ; \quad e = 12$

$d = 6$

a) Given:

$C_1 = g^e \bmod p$

$C_2 = kx \bmod p$

$C_1 = g^e \bmod p = 8$

$C_2 = kx \bmod p = 7$

$k = c_1^d \bmod p$

$= 8^6 \bmod 13$

$= 12$

b) $k^{-1} \bmod p = 12^{-1} \bmod 13$

$= 12$

c) $x = C_2 \cdot k^{-1} \bmod p$

$= 7 \cdot 12^{-1} \bmod 13$

$x = 6$