Nathan Walzer - nwalzer@wpi.edu

1a)

Consider Z_{43}^* = {1, 2, ….. 42}, that is there are 42 elements from 1-42 (we ignore 0). The possible element orders are those that can divide 42.

42 = 2 * 3 * 7
= 2 * 21
= 3 * 14
= 7 * 6
= 1 * 42

Possible element orders are 1, 2, 3, 6, 7, 14, 21, and 42. We can calculate the number of elements in each order using Euler's totient function

Element Order (O)	Possible # Elements [$\phi(o)$]
1	$\phi(1) = 1$
2	$\phi(2) = 1$
3	$\phi(3) = 2$
6	$\phi(6) = \phi(2) * \phi(3) = 2$
7	$\phi(7) = 6$
14	$\phi(14) = \phi(2) * \phi(7) = 6$
21	$\phi(21) = \phi(3) * \phi(7) = 12$
42	$\phi(42) = \phi(2) * \phi(21) = 12$

1b)

Now that we know how many elements are in each order, we can try, for each $\alpha \in Z$, $\alpha^m \% 42 = 1$.

We know that:

- The values of *m* can only be those found to be possible element orders
- If multiple values of *m* exist for a given α, α belongs only to the lowest order *m*
- The only element belonging to order 1 is 1

With that, we can now check all α against the possible values of *m*. For this brute force approach I made a simple python script to do the work. It is included in the submission, but this document will only showcase the results:

Element Order	Elements of Order
1	1
2	42
3	6, 36
6	7, 37
7	4, 11, 16, 21, 35, 41
14	2, 8, 22, 27, 32, 39
21	9, 10, 13, 14, 15, 17, 23, 24, 25, 31, 38, 40
42	3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34

1c)
All of the generators of Z^*_{43} are those with order 42. Since we found those in 1b, the generators are 3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, and 34

2a)
Z^*_{59}, q = 59-1 = 58, t = floor($\sqrt{58}$) = 7

Giant steps:

k = 0, 1, ….. floor(q/t) = floor(58/7) = 8

K_i	$G_i = 2^{i*t} \% 59$
0	$2^0 \% 59 = 1 \% 59$
1	$2^7 \% 59 = 10 \% 59$
2	41
3	56
4	59
5	54
6	9

7	31
8	15

G = {1, 10, 41, 56, 59, 54, 9, 31, 15}

Baby steps:
I = 0, 1, ….. t = 7
H = 5, g = 2

i	$H_i = H * g^i \% 59$
0	$5 * 2^0 \% 59 = 5 \% 59$
1	$5 * 2^1 \% 59 = 10 \% 59$
2	Unnecessary
3	Unnecessary
4	Unnecessary
5	Unnecessary
6	Unnecessary
7	Unnecessary

We find that $H_i = G_k$ for i = 1 and k = 1, and therefore do not need to continue with our calculations past i = 1 for the baby step table. Now we can compute kt-i % q = 1*7 - 1 = 6 % 58

And for a final check, $2^6 \% 59 = 5$. Therefore X = 6

2b)
Z^*_{79}, q = 79-1 = 78, t = floor($\sqrt{78}$) = 8, g = 11, H = 3

Giant steps:
k = 0, 1, ….. floor(q/t) = floor(78/8) = 9

K_i	$G_i = g^{i*t} \% 79$
0	1
1	44

2	40
3	22
4	20
5	11
6	10
7	45
8	5
9	62

G = {1, 44, 40, 22, 20, 11, 10, 45, 5, 62}

Baby steps:
I = 0, 1, ….. t = 8
H = 3, g = 11

i	$H_i = H * g^i \% 79$
0	11
1	33
2	47
3	43
4	78
5	68
6	37
7	12
8	53

We do not find any $H_i = G_k$ for any (i, k), therefore $x = \log_{11} 3 \% 79$ has no solution

2c)
Z^*_{103}, q = 103-1 = 102, t = floor($\sqrt{102}$) = 10, g = 31, H = 47

Giant steps:
k = 0, 1, ….. floor(q/t) = floor(102/10) = 10

K_i	$G_i = g^{i*t}$ % 103
0	1
1	64
2	79
3	9
4	61
5	93
6	81
7	34
8	13
9	8
10	100

G = {1, 64, 79, 9, 61, 93, 81, 34, 13, 8, 100}

Baby steps:
I = 0, 1, ….. t = 10
H = 47, g = 31

i	$H_i = H * g^i$ % 103
0	47
1	15
2	53
3	98
4	51
5	36
6	86

7	91
8	40
9	4
10	24

We do not find any $H_i = G_k$ for any (i, k), therefore $x = \log_{31} 47 \ \% \ 103$ has no solution

2d)

Z^*_{101}, q = 101-1 = 100, t = floor($\sqrt{100}$) = 10, g = 31, H = 5

Giant steps:

k = 0, 1, ….. floor(q/t) = floor(102/10) = 10

K_i	$G_i = g^{i*t} \ \% \ 101$
0	1
1	36
2	84
3	95
4	87
5	1 ← new cycle begins here
6	36
7	84
8	95
9	87
10	1

G = {1, 36, 84, 95, 87}

Baby steps:

I = 0, 1, ….. t = 10

H = 5, g = 31

i	$H_i = H * g^i \% 101$
0	5
1	54
2	58
3	81
4	87
5	Unnecessary
6	Unnecessary
7	Unnecessary
8	Unnecessary
9	Unnecessary
10	Unnecessary

We find that $H_i = G_k$ for i = 4 and k = 4, and therefore do not need to continue with our calculations past i = 4 for the baby step table. Now we can compute kt-i % q = 4*10 - 4 = 36 % 100

And for a final check, $31^{36} \% 101$. Although X = 36 works, we also know (as found out through the giant step calculations) that $31^y \% 101$ is cyclic. Since, we know that y = 50 is equivalent to y = 0, we know that the cycle is either 50 elements long or is some factor of 50 elements long. The factors of 50 are 1, 2, 5, 10, 25, 50. I went through and tested $31^y \% 101 = 1$ for each factor and found that the cycle $31^{25} \% 101 = 1$. Since 36 > 25, we can reduce 36 to modulo 25 space, and arrive at a final answer of X = 36 % 25 = 11.

3)
P = 709, a = 2, $K_{pr(A)} = 17$, $K_{pr(B)} = 41$

3a)
$K_{pub(A)} = a^{Kpr(a)} \% P = 2^{17} \% 709 = 616$

3b)
$K_{pub(B)} = 2^{41} \% 709 = 323$

3c)
$K_{AB} = K_{pub(A)}^{Kprb} = K_{pub(B)}^{Kpra} = 616^{41} \% 709 = 350$

3d)
Alice and Bob are able to establish the common key in several steps. Firstly, they have agreed upon a P and a, which are necessary to share between the two sides. From there, both of them select some *b* in Z_P. It does not matter what this *b* is, but each side will select their own *b* which will be their private key. Then, each side calculates a^b % P using the agreed upon a and P and their own private b. They each then send this calculated number (henceforth C) to the other person. Then each of them computes C^b % P using the C they just received, their private b, and the agreed upon P to arrive at the final shared key.

This key exchange is made possible because of the composition of C. Since C = a^b % 709 for both sides, when performing the final calculation, C^b % P = $a^{b1 * b2}$ % 709. Both sides are essentially performing the exact same calculation without ever having to know what the other person's b value is.

4a)
Find public key using g^x % P. g = 314, x = 23, p = 971
B = 314^{23} % 971 = 865
K_{pub} = (p, g, B) = (971, 314, 865)

Encrypt using public key, k = 21
$Y_1 = g^k$ % p = 314^{21} % 971 = 575
Y_2 = m * B^k % p = 49 * 865^{21} % 971 = 751
Encrypted message = (Y_1, Y_2) = (575, 751)

Decrypt ciphertext
M = $Y_2(Y_1^x)^{-1}$ % P = 751 * 575^{-23} % 971 = 751 * 575^{970-23} % 971 = 751 * 575^{947} % 971 = 49

4b)
Same as 4a) → Find public key using g^x % P. g = 314, x = 23, p = 971
B = 314^{23} % 971 = 865
K_{pub} = (p, g, B) = (971, 314, 865)

Encrypt using public key, k = 51
$Y_1 = g^k$ % p = 314^{51} % 971 = 7
Y_2 = m * B^k % p = 49 * 865^{51} % 971 = 285
Encrypted message = (Y_1, Y_2) = (7, 285)

Decrypt ciphertext
M = $Y_2(Y_1^x)^{-1}$ % P = 285 * 7^{-23} % 971 = 285 * 7^{970-23} % 971 = 285 * 7^{947} % 971 = 49