**Question 1**

Correct

Mark 1.00 out of 1.00

Let $G$ be a multiplicative group of order $n$ with identity $e$. Let $g \in G$. Let $1 \leq m < n$. And suppose that $g^m = e$. Then $g$ is a generator of the group $G$.

Select one:

- True
- False ✔

Check

Correct. For $g$ to be a generator it should not be equal to the identity element for any power lower than $n$ (except 0). Otherwise it cannot generate all elements of $G$, which are $n$.

Correct

Marks for this submission: 1.00/1.00.

**Question 2**

Correct

Mark 2.00 out of 2.00

Let $p = 23$ and let $G$ be the group $\mathbb{Z}_{23}^* = \{1, 2, \ldots, 22\}$ with multiplication modulo $p$. Clearly $4 \in G$. Also, note that $4^{11} \equiv 1 \pmod{23}$. Then 4 is a generator of the group.

Select one:

- True
- False ✔

Check

Correct. For 4 to be a generator, it should cycle through all the elements of the group as we raise powers from 0 to 22 inclusive. But we already have $4^{11} \equiv 1 \pmod{23}$.

Correct

Marks for this submission: 2.00/2.00.

**Question 3**

Correct

Mark 1.00 out of 1.00

Let $p = 23$ and let $G$ be the group $\mathbb{Z}_{23}^* = \{1, 2, \ldots, 22\}$ with multiplication modulo $p$. Clearly $5 \in G$. Is 5 a generator of the group.

Select one:

- (•) True ✔
- ( ) False

Check

Correct. 5 is a generator of the group as it cycles through all elements of $G$. You can see that by raising 5 to all powers between 0 and 22 inclusive. Alternatively, you can use the command znorder in PARI.

Correct

Marks for this submission: 1.00/1.00.

**Question 4**

Correct

Mark 1.00 out of 1.00

In the Basic ElGamal Cryptosystem, what is kept secret?

Select one:

- ( ) a. the modulus $p$
- (•) b. $x$ such that $g^x \equiv h \pmod{p}$ ✔ Correct. This is the secret key.
- ( ) c. $g$
- ( ) d. all of the above

Clear my choice

Check

Your answer is correct.

Correct

Marks for this submission: 1.00/1.00.

**Question 5**

Correct

Mark 1.00 out of 1.00

In the ElGamal cryptosystem, let $p = 21806107020153883717$ be the prime and $g = 7$ be the generator. Let $h = 19528466032350125108$ be Alice's public key. Let the encryption of the message $m = 12345$ using Alice's public key and the random integer $k = 17073977654843913067$ be $(c_1, c_2)$. For the following question only enter the integer, i.e., (not a Mod element). Calculate $c_1$.

Answer: 62323095223919703 47 ✔

Check

Correct. $c_1$ is simply $g^k$. Remember to first define $g$ as a modulo $p$ element by using the Mod command in PARI.

Correct

Marks for this submission: 1.00/1.00.

**Question 6**

Correct

Mark 2.00 out of 2.00

In the ElGamal cryptosystem, let $p = 21806107020153883717$ be the prime and $g = 7$ be the generator. Let $h = 19528466032350125108$ be Alice's public key. Let the encryption of the message $m = 12345$ using Alice's public key and the random integer $k = 17073977654843913067$ be $(c_1, c_2)$. For the following question only enter the integer, i.e., (not a Mod element). Calculate $c_2$.

Answer: 51830743559526970 20 ✔

Check

Correct. $c_2$ is $M \cdot h^k$. Make sure to first define $h$ as a modulo $p$ element by using the Mod command in PARI.

Correct

Marks for this submission: 2.00/2.00.

**Question 7**

Correct

Mark 2.00 out of 2.00

In the ElGamal cryptosystem, let $p = 21806107020153883717$ be the prime and $g = 7$ be the generator. Let $h = 19528466032350125108$ be Alice's public key and let $x = 17786592339868908823$ be Alice's private key. Alice receives the ciphertext $(c_1, c_2) = (6232309522391970347, 11325912141421457351)$. What is the plaintext? Only enter the integer, i.e., (not a Mod element).

Answer: 10000

Check

Correct. To decrypt you have to simply compute $c_2 \cdot (c_1^x)^{-1}$. In PARI this should be C2/C1^x. Make sure to define C1 as a Mod element in PARI.

Correct

Marks for this submission: 2.00/2.00.