

# **19AD713 – BIG DATA SECURITY**

**CB.EN.P2AID19023**

## **Observations :**

### **Q1:generating prime numbers of order $10^{20}$**

The observations that i found was the original code was for a higher order prime numbers, so there was nearly 85 iterations done to get a 10 digit no as the original 20 digit number was of a higher computational requirement. Simply to say , this is a prolonged process so it is time consuming.

### **Q2:primitive roots**

The minimum primitive root values can be found along with the total no of primitive roots present or can be calculated from the given value.

### **Q3:DH**

The DH algorithm is used to assign a private and public key and the sharing of the encrypted data that takes place between the two persons.

### **Q4: modulo congruency**

The mathematical calculative analysis is done in this model to assign the a,b,m values so that the assigned k integer is found and verified

### **Q5:cracking of the key pair**

The key value pair is assigned to maintain the secrecy of the client and the company/seller in the normal cases. But here we can find that the value of the p and g assigned along with the text value determines the speed of cracking that occurs as the no of digits increases the time of processing increases hence the chance of mistake decreases and as the computational analysis takes more time there will be a necessary systems inbuilt in case of a real time scenario.