Lab 10 Shor’s factoring algorithm - full version

Exercise 1:
Use period finding function from last exercise to break RSA algorithm using the full version of the algorithm (by factoring i.e. finding p and q, where p*q=N)

1. Find p and q, (see section H of the document , to be explained during the lab)
2. Find d inverse modulo of c in G_(p-1)(q-1)
3. Calculate a=b^d (mod N)