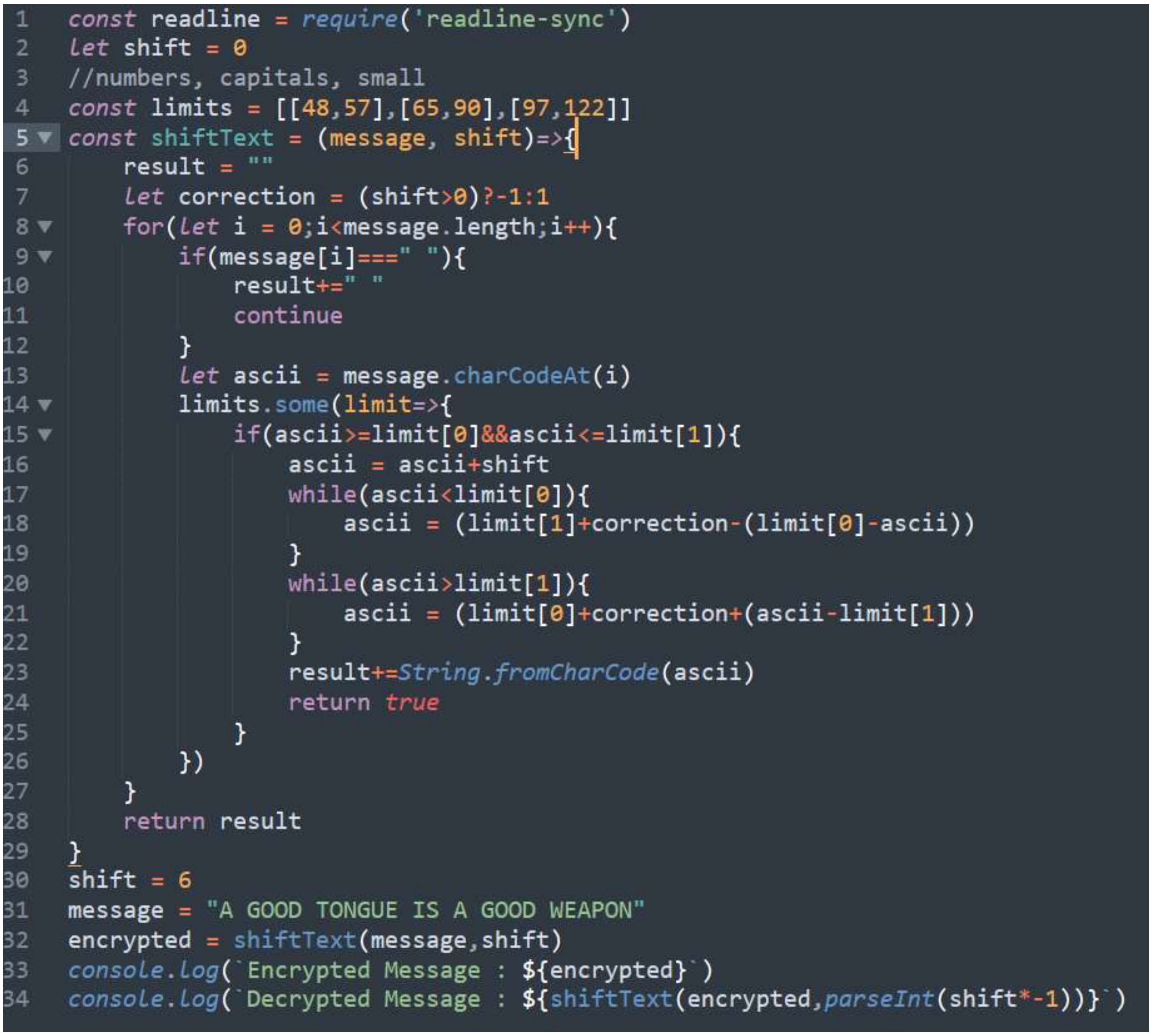
Ebenezer Isaac Veeraraju (2020178014)

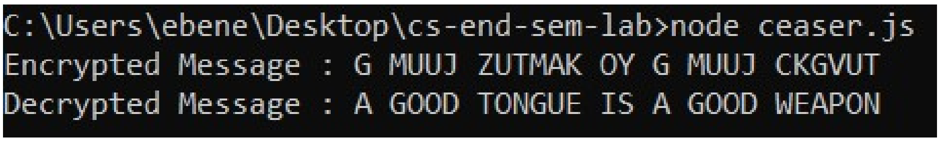
Cyber Security End Sem Lab Exam

Question 1.



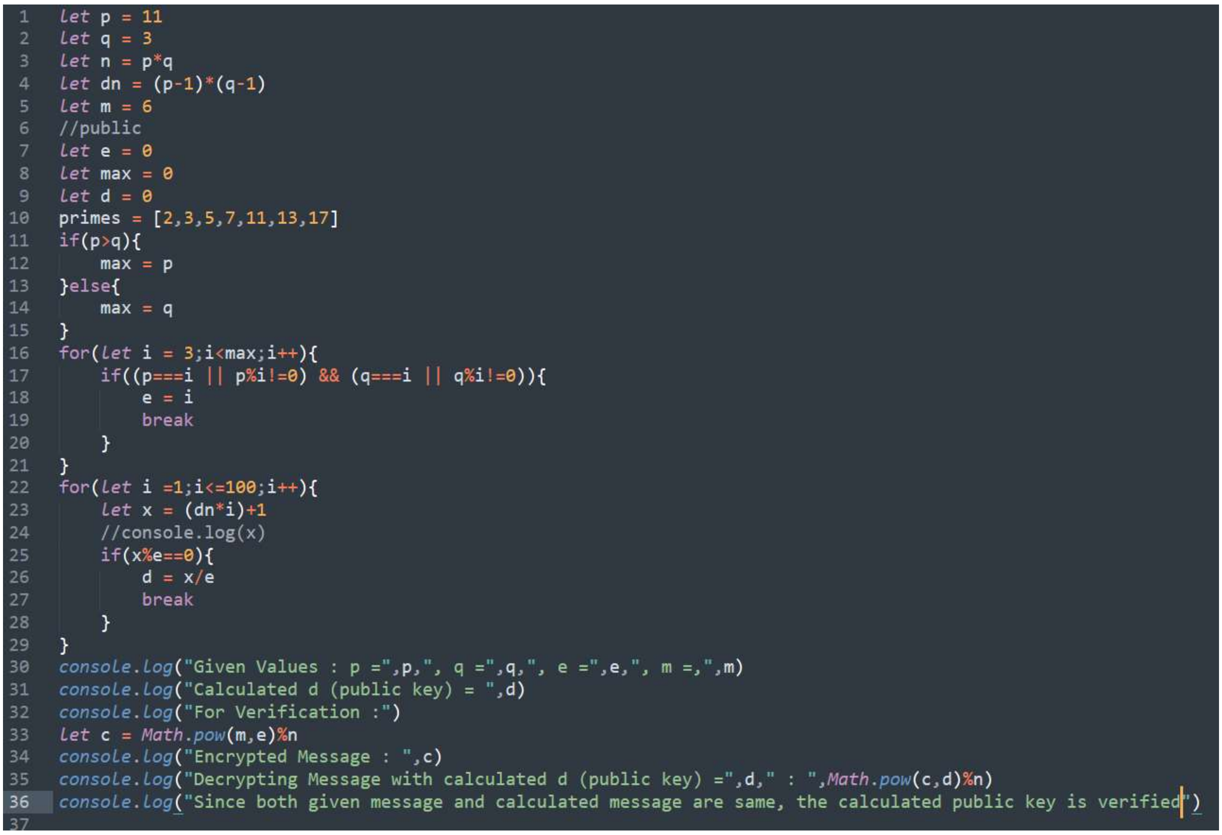
```
const readline = require('readline-sync')
let shift = 0
//numbers, capitals, small
const limits = [[48,57],[65,90],[97,122]]
const shiftText = (message, shift)=>{
    result = ""
    let correction = (shift>0)?-1:1
    for(let i = 0;i<message.length;i++){
        if(message[i]===" "){
            result+=" "
            continue
        }
        let ascii = message.charCodeAt(i)
        limits.some(limit=>{
            if(ascii>=limit[0]&&ascii<=limit[1]){
                ascii = ascii+shift
                while(ascii<limit[0]){
                    ascii = (limit[1]+correction-(limit[0]-ascii))
                }
                while(ascii>limit[1]){
                    ascii = (limit[0]+correction+(ascii-limit[1]))
                }
                result+=String.fromCharCode(ascii)
                return true
            }
        })
    }
    return result
}
shift = 6
message = "A GOOD TONGUE IS A GOOD WEAPON"
encrypted = shiftText(message,shift)
console.log(`Encrypted Message : ${encrypted}`)
console.log(`Decrypted Message : ${shiftText(encrypted,parseInt(shift*-1))}`)
```

Output :



```
C:\Users\ebene\Desktop\cs-end-sem-lab>node ceaser.js
Encrypted Message : G MUUJ ZUTMAK OY G MUUJ CKGVUT
Decrypted Message : A GOOD TONGUE IS A GOOD WEAPON
```

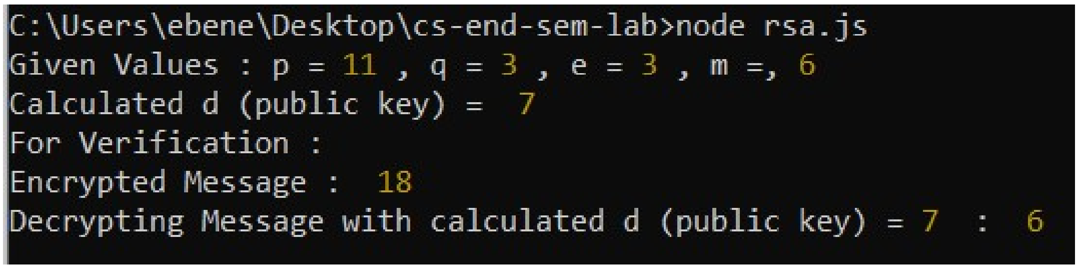
Question 2 :



```
let p = 11
let q = 3
let n = p*q
let dn = (p-1)*(q-1)
let m = 6
//public
let e = 0
let max = 0
let d = 0
primes = [2,3,5,7,11,13,17]
if(p>q){
    max = p
}else{
    max = q
}
for(let i = 3;i<max;i++){
    if((p===i || p%i!=0) && (q===i || q%i!=0)){
        e = i
        break
    }
}
for(let i =1;i<=100;i++){
    let x = (dn*i)+1
    //console.log(x)
    if(x%e==0){
        d = x/e
        break
    }
}
console.log("Given Values : p =",p,", q =",q,", e =",e,", m =,",m)
console.log("Calculated d (public key) = ",d)
console.log("For Verification :")
let c = Math.pow(m,e)%n
console.log("Encrypted Message : ",c)
console.log("Decrypting Message with calculated d (public key) =",d," : ",Math.pow(c,d)%n)
console.log("Since both given message and calculated message are same, the calculated public key is verified")

```

Output :



```
C:\Users\ebene\Desktop\cs-end-sem-lab>node rsa.js
Given Values : p = 11 , q = 3 , e = 3 , m =, 6
Calculated d (public key) =  7
For Verification :
Encrypted Message :  18
Decrypting Message with calculated d (public key) = 7  :  6
```