Explanation part:
First we generate n by using the fact that n=p*q

And then we define the euler totient function and use it to find phi(n)

To find the public key we just use the e given in the question and create a tuple(n,e) as the public key

To find the private key we just iterate from 1 to phi(n) till we find a suitable d such that eXd=1 mod phi(n)

Then we set this e as the private key

I have designed a hash function along the lines mentioned by sir in the powerpoint presentation

It takes a string and iterates over it and builds a sum according to the ASCII code of each character and finally checks that the sum is less than n.

Next we generate signature by using our private key and then representating it in base 256 representation and send it to Bob

Next we use the public key and decode the signature by converting back to base 10 and then match it with the hash value of the message calculated by using the hashing function.

```
#Part 1
import math
import hashlib
def isPrime(x):
    for i in range(2,x):
        if(x%i==0):
            return False
    return True



def phi(n):
    pro=n
    for i in range(2,n+1):
        if(isPrime(i) and n%i==0):
            pro=pro*(i-1)/i;
    pro=math.floor(pro)
    return (pro)


p,q,e=43,47,155
phin=phi(p*q)


d=0
for i in range(1,phin):
    if((i*e)%phin==1):
        d=i
        break
publickey=(p*q,e)
privatekey=(p*q,d)
```

```
#Part 2
n=p*q
def hashing(s,n):
    sumi=0
    po=1
    m=256
    for i in s:
        sumi=sumi+ord(i)*po
        po=po*m
    return sumi%n
#Alice part
m="2101-CON101 INTRODUCTION TO COMP.SC. amp; ENG"

hashcode=0
hashcode=hashing(m,n)

x=(hashcode**d)%(n)

s=""
s=s+str(x%256)
x=x//256

while(x>0):
    s=s+"."+str(x%256)
    x=x//256
signature=s
#Bob part
a1=s.split(".")

sum2=0
po=1
for i in a1:
    sum2=sum2+int(i)*po
    po=po*256
hashcode2=hashing(m,n)
y=(sum2**e)%n
#Output
print("Euler's phi function is",phin)
print("public key is",publickey)
```

```
print("private key is",privatekey)
print("signature is",signature)
print("digest of hash is",hashcode)
print("h generated by Bob is",y)
```

Output:

```
Euler's phi function is 1932
public key is (2021, 155)
private key is (2021, 1583)
signature is 143.4
digest of hash is 767
h generated by Bob is 767
```