An organization wants to achieve encryption of data using Asymmetric key cryptography. The Public key will be available to all employee, and private key will be individual for each employee for communication. Your task is to find out Public key for organization and private key for 1 employee. Also provide how data will be encrypted using this public key & private key

CODE:

```
def check_prime(num):
    if num > 1:
        for i in range(2, num):
            if (num % i) == 0:
                return 0
                break
        else:
            return 1

    else:
        return 0

def gcd(a, b):
    i = 1
    while(i <= a and i <= b):
      if(a % i == 0 and b % i == 0):
        gcd = i
      i = i + 1
    return gcd

def modInverse(a, m) :
    a = a % m;
```

```
    for x in range(1, m) :
        if ((a * x) % m == 1) :
            return x
    return 1

p=int(input("Enter value of p: "))
q=int(input("Enter value of q: "))
n=q*p
message=[int(i) for i in input('Enter integers: ').split(" ")]
_n=(p-1)*(q-1)
l1=[]
primes=[]
e=[]
for i in range(1,n):
    l1.append(i)

for i in l1:
    if check_prime(i)==1:
        primes.append(i)

if 2 in primes:
    primes.remove(2)

for i in primes:
    if gcd(i, n)==1:
        e.append(i)
```

```
fin_e=min(e)
print('\nSelected value of e: ', fin_e)
d=modInverse(fin_e, _n)
public_key=[fin_e, n]
private_key=[d, n]
print(f'\nPublic_key: {public_key}')
print(f'\nPrivate_key: {private_key}')

cipher=[]
decrypted=[]
for i in message:
    cipher.append(i**fin_e)

for i in cipher:
    decrypted.append(i**d)

for i in range(len(decrypted)):
    decrypted[i]=decrypted[i]%n

for i in range(len(cipher)):
    cipher[i]=cipher[i]%n

print('\nCipher_text: ', *cipher)
print(f'\nplain_text: ', *decrypted)
```

OUTPUT:

Tejas Tripathi

```
In [1]: runfile('C:/Users/Admin/study material/sem5/Practicals/Cryptography/
Practical-8/RSA_alg0.py', wdir='C:/Users/Admin/study material/sem5/
Practicals/Cryptography/Practical-8')

Enter value of p: 3

Enter value of q: 7

Enter integers: 1 2 3 4 5 6 7 8 9 10 11

Selected value of e:  5

Public_key: [5, 21]

Private_key: [5, 21]

Cipher_text:  1 11 12 16 17 6 7 8 18 19 2

plain_text:  1 2 3 4 5 6 7 8 9 10 11

In [2]:
```