Name :- Kaustubh Shrikant Kabra

CLass:- TE Computer

ERP :-38

Subject :-LP2(IS) (RSA)

Code:-

```
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP
import binascii

msg = (input("Enter Message to Encrypt and Decrypt : "))
msg = bytes(msg, 'utf-8')

keyPair = RSA.generate(3072)

pubKey = keyPair.publickey()
print(f"Public key:  (n={hex(pubKey.n)}, e={hex(pubKey.e)})")
pubKeyPEM = pubKey.exportKey()
print(pubKeyPEM.decode('ascii'))

print(f"Private key: (n={hex(pubKey.n)}, d={hex(keyPair.d)})")
privKeyPEM = keyPair.exportKey()
print(privKeyPEM.decode('ascii'))

# msg = input()
encryptor = PKCS1_OAEP.new(pubKey)
encrypted = encryptor.encrypt(msg)
print("Encrypted:", binascii.hexlify(encrypted))

decryptor = PKCS1_OAEP.new(keyPair)
decrypted = decryptor.decrypt(encrypted)
print('Decrypted:', decrypted)
```

Output:-

Enter Message to Encrypt and Decrypt : Its KK29 aka Kaustubh

Public key:

(n=0xc3ca908cbeadce58f8bf22a5711e1ebb14f68c72d38bea406618aad1371a34bc2ab378472a042b00a0ae2ce46
f9a395b69d164527719d8dbb5de6f78ef9a2b728702d84bd29f736106e6699df4a9e6dd44a696067920e71540ec3
684e37eb69d16f3d65a2431c05f56fbc7147e64b1a3682c2b22866b1426b18c9d8f449db0def0db75d0b26436313
6bbdcb829efc8fda7e51f8d6cd31aff2a630e6bfc16af9a7b2b50429b1443ae1b3617eda2b0cb27ede8501afabec62a
5f4f5ea2746f0bb59e8b42ab2c60c4362046ba8ac0aaed2c102f478b8643822090cf5919b63743c0220a128375945
1895220c8b526a67bc133424e06526824f82f83ac17efca35e948f0c301359e5f4ade7f8bdf0626a86ef2bb0eb6d77
dba747d7eb82a7b6ac53fba49d6c0fc2dc9d16f3d972fa7ffc5549b7a9c65b9ea54660739d2abcc0c201797d50b1ef

79a752d65d5042b9798d3323b2224a75be7a30c5af04c0deee77a09bfe7e7102c74135c253c445f699cfe42f4e4cde
642a437f4ef864e3d0197099d, e=0x10001)

-----BEGIN PUBLIC KEY-----

MIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEAw8qQjL6tzlj4vyKlcR4e

uxT2jHLTi+pAZhiq0TcaNLwqs3hHKgQrAKCuLORvmjlbadFkUncZ2Nu13m9475or

cocC2EvSn3NhBuZpnfSp5t1EppYGeSDnFUDsNoTjfradFvPWWiQxwF9W+8cUfmSx

o2gsKyKGaxQmsYydj0SdsN7w23XQsmQ2MTa73Lgp78j9p+UfjWzTGv8qYw5r/Bav

mnsrUEKbFEOuGzYX7aKwyyft6FAa+r7GKl9PXqJ0bwu1notCqyxgxDYgRrqKwKrt

LBAvR4uGQ4IgkM9ZGbY3Q8AiChKDdZRRiVIgyLUmpnvBM0JOBlJoJPgvg6wX78o1

6UjwwwE1nl9K3n+L3wYmqG7yuw621326dH1+uCp7asU/uknWwPwtydFvPZcvp//F

VJt6nGW56lRmBznSq8wMIBeX1Qse95p1LWXVBCuXmNMyOyIkp1vnowxa8EwN7ud6

Cb/n5xAsdBNcJTxEX2mc/kL05M3mQqQ39O+GTj0BlwmdAgMBAAE=

-----END PUBLIC KEY-----

Private key:
(n=0xc3ca908cbeadce58f8bf22a5711e1ebb14f68c72d38bea406618aad1371a34bc2ab378472a042b00a0ae2ce46
f9a395b69d164527719d8dbb5de6f78ef9a2b728702d84bd29f736106e6699df4a9e6dd44a696067920e71540ec3
684e37eb69d16f3d65a2431c05f56fbc7147e64b1a3682c2b22866b1426b18c9d8f449db0def0db75d0b26436313
6bbdcb829efc8fda7e51f8d6cd31aff2a630e6bfc16af9a7b2b50429b1443ae1b3617eda2b0cb27ede8501afabec62a
5f4f5ea2746f0bb59e8b42ab2c60c4362046ba8ac0aaed2c102f478b8643822090cf5919b63743c0220a128375945
1895220c8b526a67bc133424e06526824f82f83ac17efca35e948f0c301359e5f4ade7f8bdf0626a86ef2bb0eb6d77
dba747d7eb82a7b6ac53fba49d6c0fc2dc9d16f3d972fa7ffc5549b7a9c65b9ea54660739d2abcc0c201797d50b1ef
79a752d65d5042b9798d3323b2224a75be7a30c5af04c0deee77a09bfe7e7102c74135c253c445f699cfe42f4e4cde
642a437f4ef864e3d0197099d,
d=0x3826c2a112d88efaf64ffed43ae65c02e486b70e017cb99081976679fd171f73adbd6debdef17611c6835d6da0
52374befc3b5456f51f2df44400871432a507696a0eabe8827e1b3bc825d5d073ba8f1e18bf32fe5125a23becc5ff0
69bc400c3a76710dc61e9ca0db35f748f9dcd01360bf76197f3a7b7b83652414e0256781f0cac7f5b40bc87d01c90
c0aa7405540e6237092a358c1ffd73cb478a4c22ed79ba676ecbb442b0ae653f3b5dbf85f3352e852fd01d7afc69c3
20b9e84cd0a2aaa332cb57ae63658569b637daa2412c8dad3983e54d9ca7a5d433869c136093440105c316863752
e096cc8122d839adcdc0ca13a7e3007c94555703c9571bf8ada2c2634167a5666d2ded43fc9cfca128fafee93e39ad
bd54ed1320cb00d11ce5c269a3341954c9eba9120f8a15cc5ec72cdac1604d26b5fb3311659e089078f1c3d0def0a
af08124322c30e3941e6c7b5e8b519c44ed6225156fe33e40dd54999a714055a811012229f8190d1a51d7d583b78
e3fadac6e2e4d702f62f9fa333)

-----BEGIN RSA PRIVATE KEY-----

MIIG4wIBAAKCAYEAw8qQjL6tzlj4vyKlcR4euxT2jHLTi+pAZhiq0TcaNLwqs3hH

KgQrAKCuLORvmjlbadFkUncZ2Nu13m9475orcocC2EvSn3NhBuZpnfSp5t1EppYG

eSDnFUDsNoTjfradFvPWWiQxwF9W+8cUfmSxo2gsKyKGaxQmsYydj0SdsN7w23XQ

smQ2MTa73Lgp78j9p+UfjWzTGv8qYw5r/BavmnsrUEKbFEOuGzYX7aKwyyft6FAa

+r7GKl9PXqJ0bwu1notCqyxgxDYgRrqKwKrtLBAvR4uGQ4IgkM9ZGbY3Q8AiChKD

dZRRiVIgyLUmpnvBM0JOBlJoJPgvg6wX78o16UjwwwE1nl9K3n+L3wYmqG7yuw62

1326dH1+uCp7asU/uknWwPwtydFvPZcvp//FVJt6nGW56lRmBznSq8wMIBeX1Qse

95p1LWXVBCuXmNMyOyIkp1vnowxa8EwN7ud6Cb/n5xAsdBNcJTxEX2mc/kL05M3m

QqQ39O+GTj0BlwmdAgMBAAECggGAOCbCoRLYjvr2T/7UOuZcAuSGtw4BfLmQgZdm

ef0XH3OtvW3r3vF2EcaDXW2gUjdL78O1RW9R8t9EQAhxQypQdpag6r6IJ+GzvIJd

XQc7qPHhi/Mv5RJaI77MX/BpvEAMOnZxDcYenKDbNfdI+dzQE2C/dhl/Ont7g2Uk

FOAlZ4Hwysf1tAvIfQHJDAqnQFVA5iNwkqNYwf/XPLR4pMIu15umduy7RCsK5lPz

tdv4XzNS6FL9AdevxpwyC56EzQoqqjMstXrmNlhWm2N9qiQSyNrTmD5U2cp6XUM4

acE2CTRAEFwxaGN1LglsyBItg5rc3AyhOn4wB8lFVXA8lXG/itosJjQWelZm0t7U

P8nPyhKPr+6T45rb1U7RMgywDRHOXCaaM0GVTJ66kSD4oVzF7HLNrBYE0mtfszEW

WeCJB48cPQ3vCq8IEkMiww45QebHtei1GcRO1iJRVv4z5A3VSZmnFAVagRASIp+B

kNGlHX1YO3jj+trG4uTXAvYvn6MzAoHBANPyKyB+qTMnuDP2IjZFA4FBWiy2O7a/

ka5lj23/M15OE6uAxzbw9zxsDBZ3tkU87KLX68/KKs9brrs+MALlIrpDVe0z7q1N

2dLRauXRwK1KMmfgGG7sp5/1nquN7/EaTk67yFEYj+tsOXEn/RU3MX+HuAEzVoqu

MaZZ0+dhpYFFl4Ijyai9y6qktGZ/badA5iIAAunAQn/DnzoDbtstDfmqy7fD9s2x

0IXfsNBgmqiZmjZ6e6lsFngQeMMQnxwtvwKBwQDsfMpOSOdnj7fYHfDIUchyxchO

v3TkxQ/psu0hqjOOBtOqHFToEActBp9GnrGFlgVjINZPhQ1X/aQqYqs+mu0iUWwO

2OEOYXAoFwtQy77xh5jQBaGIJhSNB2+Wolv8Efz9vC76VCBSLlTcj20pzLiQLsY8

z/8b2EVo4TosLuwgBvdrteyidJfJaeHilaNxEEiIrYBOfrbU1EX820lCTLn9/tvj

SmeQBbb641N6SePl9JG3WPzdBjrI/fHq6FtmV6MCgcAbJJNjWPVASODtPqNJAfOd

9QmgWkIxeD0m8Xi55InmlOct+pMItTlkco3lvrUIDvJbNH3NoZ1z6tDox+EMLd4R

rpfthc4WQbcYqZsgDYm4Z50m8msOoZ4h/Smx3L6SyQSoTqIryJJ92uFMXYuq0OO0

6mOlO7bkkcRoAm8B3d59PLVXhE/KHWxc0TUNP1qCpewTBJ9a4jVh+WKF4nSq+w0k

ITxvr1gHJbOHwYr6VLTZzLoUKgF2RBJok+tzR8ioqi8CgcEAjH7K1d18FMuORkfr

X6cutfkIurgF40+r14RkWua6ADvQDjUMwF2dVcOkZpkrEBkDlFPS3qVGOytGF6RM

5kG2dff3gY6ZjiiXMEoYf+S7yNRtFdDymWc+OFbdlZlZmpS5P6lII5JNLWW3Jt3S

1c15LLeNMF3Fyq4e9mMwY0VxJMnevk/ziMRJ1PAhsbKCyk4JOaISIxAm4KRH/CPv

DwN0UBDUY+E1S5wJjF33nyQ8z8YPt+SXPVxRGk28Jnnqqw+PAoHAMaRAgssQ05Ba

g16ht7Zu2aLqPxhfBe8XgBG3I+kzSFUmTGfXkFxS6XA+yEwj9hDFbqFxLYjX+I5p

qdPQBVXp6X9CgY4KMokEbAaTYGslTWqATx9V5u208Xmg47Kmbfjr2RzbOqNsPc5I

yTZe2Nxd3MvE7aCJxQlN/KaUrb5NlSGgetexRsKCFALgGwF4F41PJV0R5NdfqoVd

Je9N445Lv9bGWv1hX0dHYbZryao6WuFpZde7Y7WLoxsAKbftDFCj

-----END RSA PRIVATE KEY-----

Encrypted:

b'6c810ba224b2eb60bfab6fc3c96192f640278a8e724490fab916450ef0a7bad006b90f70db810ce803352739753dc3018d0eb58a7707800808487f2004893bc3d0c5e4deb03eb587879377b6e33a2b6f44d12ac9836d1e8b2296af4c5fc97b06b090fedeeff6ea18c7ac21662cb67783f7061d914b7136d2232f03ebf6e1bc676096434ca6d883c7e8b017ea808b353933003cae78335d900b307eac919f475b903b33a1ab54a86f14ef1cf47b167cefb4391a17a91d1a9480a

3b030186872b8c2a575998231566173ff15190970d1329f99c7ce33f439580954725f7d4905c855b6a26452b47a287cc2ab1a88d29cdc5d8a80b11278ecff7e0bb1ef6aec0a9d63562be3a3132e0d89e5e1df07f3825d70681afd1951e00c66f69d29c95ff803ed298b2409066473a13362a807d35d8061c43b7574eb35960d329aad1514abaa29626b75501ff1b694ac4d1a8ceec75eafe7d68946a3f71757cc3544cb510c9236db7da53bd49240578e554fa4cd72ad92cefea895ab29ba0b3dd1da8fb44721'

Decrypted: b'Its KK29 aka Kaustubh'

Process finished with exit code 0

```
C:\Users\asus\PycharmProjects\LP2\Scripts\python.exe "C:/Users/asus/PycharmProjects/LP2(codes)/5. RSA.py"
Enter Message to Encrypt and Decrypt : Its KK29 aka Kaustubh
Public key:  (n=0xc3ca908cbeadce58f8bf22a5711e1ebb14f68c72d38bea406618aad1371a34bc2ab378472a042b00a0ae2ce46f9a395b69d164527719d8dbb5de6f78ef9a2b728702d84bd29f736106e6699df4
-----BEGIN PUBLIC KEY-----
MIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEAw8qQjL6tzlj4vyKlcR4e
uxT2jHLTi+pAZhiq0TcaNLwqs3hHKgQrAKCuLORvmjlbadFkUncZ2Nu13m9475or
cocC2EvSn3NhBuZpnfSp5t1EppYGeSDnFUDsNoTjfradFvPWWiQxwF9W+8cUfmSx
o2gsKyKGaxQmsYydj0SdsN7w23XQsmQ2MTa73Lgp78j9p+UfjWzTGv8qYw5r/Bav
mnsrUEKbFEOuGzYX7aKwyyft6FAa+r7GKl9PXqJ0bwu1notCqyxgxDYgRrqKwKrt
LBAvR4uGQ4IgkM9ZGbY3Q8AiChKDdZRRiVIgyLUmpnvBM0JOBlJoJPgvg6wX78o1
6UjwwwE1nl9K3n+L3wYmqG7yuw621326dH1+uCp7asU/uknWwPwtydFvPZcvp//F
VJt6nGW56lRmBznSq8wMIBeX1Qse95p1LWXVBCuXmNMyOyIkp1vnowxa8EwN7ud6
Cb/n5xAsdBNcJTxEX2mc/kL05M3mQqQ39O+GTj0BlwmdAgMBAAE=
-----END PUBLIC KEY-----
Private key: (n=0xc3ca908cbeadce58f8bf22a5711e1ebb14f68c72d38bea406618aad1371a34bc2ab378472a042b00a0ae2ce46f9a395b69d164527719d8dbb5de6f78ef9a2b728702d84bd29f736106e6699df4
-----BEGIN RSA PRIVATE KEY-----
MIIG4wIBAAKCAYEAw8qQjL6tzlj4vyKlcR4euxT2jHLTi+pAZhiq0TcaNLwqs3hH
KgQrAKCuLORvmjlbadFkUncZ2Nu13m9475orcocC2EvSn3NhBuZpnfSp5t1EppYG
eSDnFUDsNoTjfradFvPWWiQxwF9W+8cUfmSxo2gsKyKGaxQmsYydj0SdsN7w23XQ
smQ2MTa73Lgp78j9p+UfjWzTGv8qYw5r/BavmnsrUEKbFEOuGzYX7aKwyyft6FAa
+r7GKl9PXqJ0bwu1notCqyxgxDYgRrqKwKrtLBAvR4uGQ4IgkM9ZGbY3Q8AiChKD
dZRRiVIgyLUmpnvBM0JOBlJoJPgvg6wX78o16UjwwwE1nl9K3n+L3wYmqG7yuw62
1326dH1+uCp7asU/uknWwPwtydFvPZcvp//FVJt6nGW56lRmBznSq8wMIBeX1Qse
95p1LWXVBCuXmNMyOyIkp1vnowxa8EwN7ud6Cb/n5xAsdBNcJTxEX2mc/kL05M3m
QqQ39O+GTj0BlwmdAgMBAAECggGAOCbCoRLYjvr2T/7UOuZcAuSGtw4BfLmQgZdm
ef0XH3OtvW3r3vF2EcaDXW2gUjdL78O1RW9R8t9EQAhxQypQdpag6r6IJ+GzvIJd
XQc7qPHhi/Mv5RJaI77MX/BpvEAMOnZxDcYenKDbNfdI+dzQE2C/dhl/Ont7g2Uk
FOAlZ4Hwysf1tAvIfQHJDAqnQFVA5iNwkqNYwf/XPLR4pMIu15umduy7RCsK5lPz
tdv4XzNS6FL9AdevxpwyC56EzQoqqjMstXrmNlhWm2N9qiQSyNrTmD5U2cp6XUM4
```