Name :- Akash Mete

CLass:- TE Computer

ERP :-52

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 Prisoner aka Akash

Public key:
(n=0x976c7495a43432362de688b2d916e5f77ce6fd8e5d6fd5b02432e150368edcd02c4c9dee5502c88bfd67ae7c
24a14f18c770ed2475eb04afb1a591ee1f4dc7412b950d580ab47f2873638936a8d2c3d8c02fbb6f8366b9b69974f
eb76d57f64d1a3ab009117cf772d6f520b4ee4e8db889087b06e1f53ef1001a9c58fc2b0d8e6871cf04b126aed009a
f1e4675cab1e6206c9e37c0e60c86f5c313bc012ac7525f9c5e38ed33cdba8f8f656a3727cb650f0c0c22d929c62f2
7423c1acd669ef7483792c2b8ea7c9bcb09822fd54eab79e924534ed33b5a6eaa84eadd79610ec60d26666ef31443
115901c6b8c331cda79be18e9a44cc5e4dfde9b81a44c21f6c686ef7ee1d228b1397a1fe2f4f5256c4978bb9e3c416
dd243e4567b2bdead2bd26ab8b098d3b71f06b1263a768f0fcadbfb1724ebcf90b2c2a95015b8d1df035262cff80e5
37252ec23f3efe260f565e3255a1605a114ddc9414463c844280075f9b57088ea4740dae624978a446870f2ed18ce
464e31041bf8f5f3f92d9c7fb, e=0x10001)
```

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

MIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEAl2x0laQ0MjYt5oiy2Rbl

93zm/Y5db9WwJDLhUDaO3NAsTJ3uVQLIi/1nrnwkoU8Yx3DtJHXrBK+xpZHuH03H

QSuVDVgKtH8oc2OJNqjSw9jAL7tvg2a5tpl0/rdtV/ZNGjqwCRF893LW9SC07k6N

uIkIewbh9T7xABqcWPwrDY5occ8EsSau0AmvHkZ1yrHmIGyeN8DmDIb1wxO8ASrH

Ul+cXjjtM826j49lajcny2UPDAwi2SnGLydCPBrNZp73SDeSwrjqfJvLCYIv1U6r

eekkU07TO1puqoTq3XlhDsYNJmZu8xRDEVkBxrjDMc2nm+GOmkTMXk396bgaRMIf

bGhu9+4dIosTl6H+L09SVsSXi7njxBbdJD5FZ7K96tK9JquLCY07cfBrEmOnaPD8

rb+xck68+QssKpUBW40d8DUmLP+A5TclLsI/Pv4mD1ZeMlWhYFoRTdyUFEY8hEKA

B1+bVwiOpHQNrmJJeKRGhw8u0YzkZOMQQb+PXz+S2cf7AgMBAAE=

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

Private key:
(n=0x976c7495a43432362de688b2d916e5f77ce6fd8e5d6fd5b02432e150368edcd02c4c9dee5502c88bfd67ae7c
24a14f18c770ed2475eb04afb1a591ee1f4dc7412b950d580ab47f2873638936a8d2c3d8c02fbb6f8366b9b69974f
eb76d57f64d1a3ab009117cf772d6f520b4ee4e8db889087b06e1f53ef1001a9c58fc2b0d8e6871cf04b126aed009a
f1e4675cab1e6206c9e37c0e60c86f5c313bc012ac7525f9c5e38ed33cdba8f8f656a3727cb650f0c0c22d929c62f2
7423c1acd669ef7483792c2b8ea7c9bcb09822fd54eab79e924534ed33b5a6eaa84eadd79610ec60d26666ef31443
115901c6b8c331cda79be18e9a44cc5e4dfde9b81a44c21f6c686ef7ee1d228b1397a1fe2f4f5256c4978bb9e3c416
dd243e4567b2bdead2bd26ab8b098d3b71f06b1263a768f0fcadbfb1724ebcf90b2c2a95015b8d1df035262cff80e5
37252ec23f3efe260f565e3255a1605a114ddc9414463c844280075f9b57088ea4740dae624978a446870f2ed18ce
464e31041bf8f5f3f92d9c7fb,
d=0x999bceb39edd1f0811e2ddf97b25877f05edd87a26148a7f226445bd2170d0ffe7c5dc25d231fdfa451926203
99334b2110b0b0659b8b80af8a3858e3cf8a1e6b2acd9d9de6ce1871f71c72d9e701b7788e98db314bc38d9212e0
0d758224b719be767d1f5de57b2354325e8102265678b5bac5cd1b6aacb15d7e8e891a6fb1c3947cfed153e05f31f
b5237946dfab3da5818a5f4a08153288f80424f6ea2143fc49f180be358c6b1d0727fcbff1abf0db7ad534e4d2992c
171f51e9be99c3d7ccac475dcbfa48a4a8328686d3329e48f40204678daf52ad4f6510b53687bea45f41b20ae2afcf
2e655d49162de29b06ec87abd9c61fe83a6d0e1e798c82fdd6216706069b111c1b2828b771aa80e5e933665f843b
cf4e8d25529fd2e99064c16140594d9f9fce03e193fdd15f3a8f5498ff14d893837a30720a81a684e2cd10ac1964fa9
30fdbd4c6afad3acb88b427b3b700deceac27e281e9fe88c74f602a54ae86757024d9ac41afc13c0d76b9b652c9852
bd134ebcb424514ccfcd5cd9)

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

MIIG5AIBAAKCAYEAl2x0laQ0MjYt5oiy2Rbl93zm/Y5db9WwJDLhUDaO3NAsTJ3u

VQLIi/1nrnwkoU8Yx3DtJHXrBK+xpZHuH03HQSuVDVgKtH8oc2OJNqjSw9jAL7tv

g2a5tpl0/rdtV/ZNGjqwCRF893LW9SC07k6NuIkIewbh9T7xABqcWPwrDY5occ8E

sSau0AmvHkZ1yrHmIGyeN8DmDIb1wxO8ASrHUl+cXjjtM826j49lajcny2UPDAwi

2SnGLydCPBrNZp73SDeSwrjqfJvLCYIv1U6reekkU07TO1puqoTq3XlhDsYNJmZu

8xRDEVkBxrjDMc2nm+GOmkTMXk396bgaRMIfbGhu9+4dIosTl6H+L09SVsSXi7nj

xBbdJD5FZ7K96tK9JquLCY07cfBrEmOnaPD8rb+xck68+QssKpUBW40d8DUmLP+A

5TclLsI/Pv4mD1ZeMlWhYFoRTdyUFEY8hEKAB1+bVwiOpHQNrmJJeKRGhw8u0Yzk

ZOMQQb+PXz+S2cf7AgMBAAECggGACZm86znt0fCBHi3fl7JYd/Be3YeiYUin8iZE
W9IXDQ/+fF3CXSMf36RRkmIDmTNLIRCwsGWbi4CvijhY48+KHmsqzZ2d5s4Ycfcc
ctnnAbd4jpjbMUvDjZIS4A11giS3Gb52fR9d5XsjVDJegQImVni1usXNG2qssV1+
jokab7HDlHz+0VPgXzH7UjeUbfqz2lgYpfSggVMoj4BCT26iFD/EnxgL41jGsdBy
f8v/Gr8Nt61TTk0pksFx9R6b6Zw9fMrEddy/pIpKgyhobTMp5I9AIEZ42vUq1PZR
C1Noe+pF9Bsgrir88uZV1JFi3imwbsh6vZxh/oOm0OHnmMgv3WIWcGBpsRHBsoKL
dxqoDl6TNmX4Q7z06NJVKf0umQZMFhQFlNn5/OA+GT/dFfOo9UmP8U2JODejByCo
GmhOLNEKwZZPqTD9vUxq+tOsuItCeztwDezqwn4oHp/ojHT2AqVK6GdXAk2axBr8
E8DXa5tlLJhSvRNOvLQkUUzPzVzZAoHBAMRns+b73+bkYBEAh/1VJ1nUgsc0+8E/
KE06MNAXY0WL3vPLDw/THZwZtLylkDdTOtVVLI4zay/2ChE6PWha8HRertxDjqGz
RsUweUL4s6pRMwevhsm5qmK4K6eqdUf/UuFx9xkanHFLgzduzhhAhrshcq/Nd8D7
o2Oisn3W6IgjuqK5dt3WZ40liPrDtcsSCkLE7kaOF/pe563+QR/CC+1Kl61EKz7l
3NTLuqfIwdLDVyphuCWauTBAfi2Kqa1OswKBwQDFXrKnyc35OyWsP5gdvhPGom+H
UfM8k8bK+Bt4Mm4KSCnsWI+1rvgj9LKRgubwN3WL5Ag20VG5Jvulw0HpE8ZkTNWM
8gfGA4GZrOcPDvJ7c9Gg+cexvjRXNgdpXeVUFZu4W27bmXSiWJfLJUD0ZIBH6n5z
zKi+otltzlLoaB+BxD+/euACt4sVO/eRf4/j0+3Wk7tNp1XZdPLdNRZ9H+mgcfhl
nxa5dhjXBA74ek68r8RO3G9ojFadqAlaTLtyxZkCgcEAt7ahCvCTMTBxw7WRfp/G
XTpw0dF3o/1lv0ctHZii3QzGkZhhEFZTng5Vhxf+3CFYKPCw6pqiKoykQhUOF6zo
upFOUu5GXm6JRi3fX4uu0yN87jV7iPnIrOrEuuKxLZVge0zU64B+0WLm7FUTJpBE
9omE83joCXXYEXzAJQF/JMj27Ps6eqrw1ZBEnvut8rN/MZFvqEOFnkZjw9bOJ9yk
t2NMmV/oa78rX0jp4cPhuTnLMPOTAmnFy6Kn5AWOTXQNAoHBALLJE4DWV1Sa9YdQ
nBTlJ7jZT7n+zB1lp8AYe5mn5PI/aGqF1rg3ZOP9NvyE3XlgY4Ry7dXqSuMzouUH
ON9PYHle+FsSq2P9rRpt+2gynAikY5I0cWZa68LMWG5j9ebzI/oeKQ+XtIWTRv1o
I6y+lU2P5zgyffEiR18mdQe9ujysbyqevej4Jm73wUz1hnxUb6/eZt7y49t2CsHC
4zo4/EKwutgjAkzB48JyFLWU5VoaxfLBz9Gevp9VphM8StiukQKBwD8YvVqJzntE
5d3OADTb0V0hwWKpbpkQyXMcMWIGWf5j8tmdmR30pMLHKdLvAHTSzrgpSn/2MZ7e
6PH+qvymwYLya5qGWIag7CJ092e/YA5gqv0ZAFGGjh69hzA1vxnr5i2Gl6ymZu1+
2PixJGRJDrbqYEqM6Fvy9YUT7doNfq6027cs6L/ao3KjvRS923ueKqjLSpguENty
vHQz8BirzWHjPdIeelQyqSdeTvtnWoUrbkmvD4XDghtRzUH2DacWJw==

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

Encrypted:
b'48a6bf527656ab6f0871b4ccfe437b024896cccab9d8a5201b358c9a06e04037a296f3459ed88bc857548574cef3
7952fbe148734fc0e171d177f54e35e4945020e489afe1c387614e202cc0d3a16066b28709cf1f75eeb4a1c3e5cd46

```
0895df08caf3a2a5e92d6c3cf59c46803a9059c55c9fffde8b537674107306e7a0da75ff49325a5fa5e851a024b8ebc
1e81ed921fcc5ed743ba62e81e31c4d1afcfa0c42385ec519c6b4a7e7bddb6ecd0d72ede793a09414d4cfeff368f6e1
2800ea4a180080d74af19cfb159efd4c9dc7b7fbe9a117d148efcccde7012292e02a0603b070b2b29f77fb45bc3d79
313b26c8ac3719b7c65c542e46b7108654ec86feb4256e23f3e89f7f84c48d5f7ecd5b5a11692c5e73f3fef95c956c
01457490bdf84b0828ee9b0374b599b8c56783e1a037e8f511df2297b7c8821c313bbff9d7d4189da92a4639f86b5
ff5d485b13252b686e2a1184a059df0b6fdfc59aa4357258c8c1989f1a7bd19ab1b2605239609576f2b23a22d89f1
857b2b8268bd3a9547'
```

Decrypted: b'Its Prisoner aka Akash'

```
Process finished with exit code 0
```