Name :- Onasvee Banarse

CLass:- TE Computer

ERP :-09

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 OrionOriginal aka Onasvee

Public key:

(n=0xd28fb8466404a25918fa62ceb454a7a2ecc4fa1fab0ef0ab3ce5afb29499cac1c860765a5680d6dfb598588e
7f75e1996ca74636ff0b3d5c18679f9609c94645e3157b330b1e4aba50f7a990e58cddd5a0d1521c9b772e6c3c0
d72f721a74495da5874e12d7fe5bd1a9f419b0cfc52a77597a51fbf687186029b323d97540281c2f954573480a81
071bff175298ae97371cb700c3ff4dc5afab62799490fd2259e648bc2af0d6163f3c533558cfef08e1d5bd3d7d238
c9e279ffd50c555ca9e11865fa7bfc8088fed2fe6b0ecdab26621f1e08734d7f58634c628d3989663afbb6c2f89c4d
cd4042652d5ca23aa3b90ab7d0f3582c011130b890f7d106466f8e1ac4ff5ec55c3f1ad6c5727f34afb39f2559082
b0156a569d1a449a8ceda4aa656ba61ab1963df7c3cd64cdcb013e28bfff416419fb94406a15dc08c6ef97deb9e8

30221fc321fc3d65ac669a101ce754f81b5e6e6e7d7768646e90620801906f646ce7cdcec421e4c0c166a6b57023
8118ba9fb53acbe8e5ae85ca270ca48fb, e=0x10001)

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

MIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEA0o+4RmQEolkY+mLOtFSn

ouzE+h+rDvCrPOWvspSZysHIYHZaVoDW37WYWI5/deGZbKdGNv8LPVwYZ5+WCclG

ReMVezMLHkq6UPepkOWM3dWg0VIcm3cubDwNcvchp0SV2lh04S1/5b0an0GbDPxS

p3WXpR+/aHGGApsyPZdUAoHC+VRXNICoEHG/8XUpiulzcctwDD/03Fr6tieZSQ/S

JZ5ki8KvDWFj88UzVYz+8I4dW9PX0jjJ4nn/1QxVXKnhGGX6e/yAiP7S/msOzasm

Yh8eCHNNf1hjTGKNOYlmOvu2wvicTc1AQmUtXKI6o7kKt9DzWCwBETC4kPfRBkZv

jhrE/17FXD8a1sVyfzSvs58lWQgrAValadGkSajO2kqmVrphqxlj33w81kzcsBPi

i//0FkGfuUQGoV3AjG75feuegwIh/DIfw9ZaxmmhAc51T4G15ubn13aGRukGIIAZ

BvZGznzc7EIeTAwWamtXAjgRi6n7U6y+jlroXKJwykj7AgMBAAE=

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

Private key:
(n=0xd28fb8466404a25918fa62ceb454a7a2ecc4fa1fab0ef0ab3ce5afb29499cac1c860765a5680d6dfb598588e
7f75e1996ca74636ff0b3d5c18679f9609c94645e3157b330b1e4aba50f7a990e58cddd5a0d1521c9b772e6c3c0
d72f721a74495da5874e12d7fe5bd1a9f419b0cfc52a77597a51fbf687186029b323d97540281c2f954573480a81
071bff175298ae97371cb700c3ff4dc5afab62799490fd2259e648bc2af0d6163f3c533558cfef08e1d5bd3d7d238
c9e279ffd50c555ca9e11865fa7bfc8088fed2fe6b0ecdab26621f1e08734d7f58634c628d3989663afbb6c2f89c4d
cd4042652d5ca23aa3b90ab7d0f3582c011130b890f7d106466f8e1ac4ff5ec55c3f1ad6c5727f34afb39f2559082
b0156a569d1a449a8ceda4aa656ba61ab1963df7c3cd64cdcb013e28bfff416419fb94406a15dc08c6ef97deb9e8
30221fc321fc3d65ac669a101ce754f81b5e6e6e7d7768646e90620801906f646ce7cdcec421e4c0c166a6b57023
8118ba9fb53acbe8e5ae85ca270ca48fb,
d=0x2d24d92a665944017c447a98bcbb05b1fdb781b4f674de8ea820ca99ac18890b210de5721ae7c6a9f20236c
25e7b84a1e354bdce1ec267266ea910e317380b1402cae13e215d1e4272079758548eee24d634eab8ed701108
ed9b2891e9aa361f36d00e4714fd3de15c6ad6a30a96b295eab55796c5effb9ef2c21974711476f1213f59a0d4c5
dcc2a1d0b85119560a1551497fbd709cebfda991124e6006bf5487702132dd5b2e0d42ff7db112e8b9e48e50d8c
b85ebdd04ec8938414baff14fc8b8c364f96e242c821fb2ceb8815dc445bb9100797b693ec330d7815044276cf97
7be385f8f23c837848024224a7070d2cf4773588cbe57ecdcffeec2a5fa0c0e0ff4e5829221777dce02ae1828fffc3
4369e5157fe3fcf1066a3132d2d7182aac909eb3dbf2f5cc297762896ec4cfb149ad2b879667960117c80f65ff1c8
7d1ba0831761676d4201bf042e94c49ccd8b797bbc79e46d3a55f9b25d2632d3d4a352beee58ed56d1e9debcff
b6febdcf44f977ac43f421415a83a9bbe0352981)

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

MIIG5AIBAAKCAYEA0o+4RmQEolkY+mLOtFSnouzE+h+rDvCrPOWvspSZysHIYHZa

VoDW37WYWI5/deGZbKdGNv8LPVwYZ5+WCclGReMVezMLHkq6UPepkOWM3dWg0VIc

m3cubDwNcvchp0SV2lh04S1/5b0an0GbDPxSp3WXpR+/aHGGApsyPZdUAoHC+VRX

NICoEHG/8XUpiulzcctwDD/03Fr6tieZSQ/SJZ5ki8KvDWFj88UzVYz+8I4dW9PX

0jjJ4nn/1QxVXKnhGGX6e/yAiP7S/msOzasmYh8eCHNNf1hjTGKNOYlmOvu2wvic
Tc1AQmUtXKI6o7kKt9DzWCwBETC4kPfRBkZvjhrE/17FXD8a1sVyfzSvs58lWQgr
AValadGkSajO2kqmVrphqxlj33w81kzcsBPii//0FkGfuUQGoV3AjG75feuegwIh
/DIfw9ZaxmmhAc51T4G15ubn13aGRukGIIAZBvZGznzc7EIeTAwWamtXAjgRi6n7
U6y+jlroXKJwykj7AgMBAAECggGALSTZKmZZRAF8RHqYvLsFsf23gbT2dN6OqCDK
mawYiQshDeVyGufGqfICNsJee4Sh41S9zh7CZyZuqRDjFzgLFALK4T4hXR5CcgeX
WFSO7iTWNOq47XARCO2bKJHpqjYfNtAORxT9PeFcatajCpayleq1V5bF7/ue8sIZ
dHEUdvEhP1mg1MXcwqHQuFEZVgoVUUl/vXCc6/2pkRJOYAa/VIdwITLdWy4NQv99
sRLoueSOUNjLhevdBOyJOEFLr/FPyLjDZPluJCyCH7LOuIFdxEW7kQB5e2k+wzDX
gVBEJ2z5d744X48jyDeEgCQiSnBw0s9Hc1iMvlfs3P/uwqX6DA4P9OWCkiF3fc4C
rhgo//w0Np5RV/4/zxBmoxMtLXGCqskJ6z2/L1zCl3YoluxM+xSa0rh5ZnlgEXyA
9l/xyH0boIMXYWdtQgG/BC6UxJzNi3l7vHnkbTpV+bJdJjLT1KNSvu5Y7VbR6d68
/7b+vc9E+XesQ/QhQVqDqbvgNSmBAoHBANuhVjk2UR2Q+HZtolCu0Bm4BGjgmHSm
Juho6+kGSiRS5Hg7hRccm+fjQd0kGk0yJTcHU8g5UF+hlMT7jHhQlcNWttQVVvdc
SWgQaoEUcZnpAyFMqTL4eNezCHOyvnRh4h2RFoxrDPE5DlPVQab+GSVMorHp28g0
v5WwrSHdjcdoXXObgCWlq5WfbsshQuJF1FhsTtdsb5Y/JAvoDpi76tAIbvhrr0u0
SouZv7+ucH/bFJFwFNRVHw0ZCQPNVlEvOwKBwQD1be8FA4cUgtGU7UrCLmFwjI/f
KGgfLgPUafU63yneMgPajLKu7acBz24eY+ab0etBfeF371YSkKFLA6/7wUHOQw/r
PMKg77AWCu01VV5T6yX5YE081tOCSHtziy9OFYLdd/z408pweiHOhPD02Gz8V+50
etE0zaQ9dYj86FL7PPGO0Fxp0bGJDl14nvJoKfCiIFSRjZVnTJGw98TaIuurRmZ9
MQKP9fbdtpcxDQ6mZqFSGsALDykyqcuXu+g5MUECgcEAjpvR2tBUFzicvHkvnegE
o86Cvn6nP4brWJlYJTS6S5+vTgqHvpwK96TujWL12Q4ob/TICAh/EblfWhBkA3N/
6xiRGmDI2VEJMRMHtMzLfr54E9UtQDVqcdSENmvnkrZEFiKxW3ffLXp4vSKJwJ7Z
QQjj01YgKX1msRHJOWYcu1Ae7gQYT1mlcj/Vtvvf7ACfgtLA1sxIIGzbQQfrAm1y
aKYxOAjkB+oHRWINya7AyaQ9VLpMLBshUGXjHp7j308lAoHBAK/GOU509VSqUKIB
xO4Hu7+Y3B2uWcwi75k8/eZZGCpL1di7tel0yYyRXEOltu7YTE5OcqGsJxAKx4nr
LSn4gkHQY+FNVfNfVtSipLry1ijyG/NbllXBYiBH+yqIf6vD2kL1gZdQUAd4YSgA
rHYfXwbnjx+bKqRPt5ZQzHidh3jqb/Khpd4f0a/gOu99nw0dJHto/kh0h5FBFIMT
IMg+BF1ZgWOeK0Chn1mxQN1fhaOFk3ozMGF7TT08wFR+vtXfQQKBwA8bkaOFL7e4
9vw75920f8CXFLoP5uOEOvTvucFcpLyJ45WWE5o98N9mNH093gW9oNLCPFcr7eiD

dl6WtjbS82UXMlDGDJv+7al71AY/wTQbeMvqKKtzzBXeoNADcXsVRsqbBB7KPJb4

uJq6Rr9rPzcv8TeIPXG7t0FS4V7jwwgCdFsOT6M1Zh9dLwdsSydWcyl3N4x1gQzE

PrHA1jVVkPdQZ5492piZo6V1XMS36F9FiC9IyxJ1840LwTV/rvtsnw==

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

Encrypted:
b'cb47be1bba8b1153b1a2ba8edd59e87bcaf3c764749ce049ae3b1c3e3c69e8a441750f12109e50e4c2295d518
9a337f600e4563918c903c014fb5ea63d4ad0e99bdf83ccb4ce7e5a9437044f58b88568e59071895c128288cbfb
9136b287da8e1abd1bee1f1104877f2bcf8db12fa80018f1f7a1afcd29f6bb405e152b8eae65746dc26f87e87b2e
a7ac8e5ed06df14053b597ff53b33bf00be482b34f24ebeb5a3b4b6290ba700c86e9fd6517d3aab06cd8fa403c0e
1dcd1e8790b886a8a50453656cc8feb46bd7fdd9ba31781b98362af57e9f13a159c2fdcac54ce9e5d05cf578c935
5603fe4c1e6e6aefd8939f25eeb1a4472d8ccfd513c1dab0c1772bdc6de6af67c623d6d89f8534d11088e4267dc5
8101db696d4ef8b48228e363e1831ab8850561b3e54d605b4efb0b903767002e95276e22279dd02e17e4b489ff
3e9938fdc16694097fcbd4692fa5660d4bbec55d6aa3342f31f52b3744a0a75b3dabe271eaf04a182feb49bb2480
da6226de00b8bfcef02654d88589b94442b450'

Decrypted: b'Its OrionOriginal aka Onasvee'

Process finished with exit code 0