Name :- Harsh Shah

CLass:- TE Computer

ERP :-67

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 Lonewolf aka Harsh

Public key:

(n=0x8c03a2f69315827592841a74e8485d7867d3e2b858df4e368efceacf6e9012c12585c34e89b41b248eb4
d3504daccf42f861325ba89ede647169e6a083c7a6a7a2c78e114edcccf1cb7be8875a500db57368d59550061
2c943bea36d214099b47c431a6a88b68f10f0366326573d1faad7f0a53e1a16efe07eb01ad0fc11e0232cd84b3
6500fb8a084e3642a99cd2280c227e431d633d2e361558eaa462e3574ca015f45584eee68e265f47aef7b1cb8e
24f4e7c90214b679ec7aed88018c1867770f74919c54f5af0bfaa948dac8fefab25e0232d1e46a2cef7e2bd386b
c59875e334ad00ac41310909b2a771b42fd7c0daafd3e110f038a5d7eff4ccce5f0e844c3981ad8a1bb2c6cfecd
65fbd3f3adf927ff124e7f2ea301bd6ad13dcabc5afc01ae3050e463bfaa3153de10e6940ab1e04fe7fd6c8a4026

8a2688971a281be56142c6cd7477da9465086f8ca3a818a4127815c93c65f84070157c850e6b28651c36b698bbf75b52a89a49d93dbacf46649cf34c4de69383ec88c546334f9, e=0x10001)

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

MIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEAjAOi9pMVgnWShBp06Ehd

eGfT4rhY3042jvzqz26QEsElhcNOibQbJI6001BNrM9C+GEyW6ie3mRxaeagg8em

p6LHjhFO3Mzxy3voh1pQDbVzaNWVUAYSyUO+o20hQJm0fEMaaoi2jxDwNmMmVz0f

qtfwpT4aFu/gfrAa0PwR4CMs2Es2UA+4oITjZCqZzSKAwifkMdYz0uNhVY6qRi41

dMoBX0VYTu5o4mX0eu97HLjiT058kCFLZ57HrtiAGMGGd3D3SRnFT1rwv6qUjayP

76sl4CMtHkaizvfivThrxZh14zStAKxBMQkJsqdxtC/XwNqv0+EQ8Dil1+/0zM5f

DoRMOYGtihuyxs/s1l+9Pzrfkn/xJOfy6jAb1q0T3KvFr8Aa4wUORjv6oxU94Q5p

QKseBP5/1sikAmiiaIlxooG+VhQsbNdHfalGUIb4yjqBikEngVyTxl+EBwFXyFDm

soZRw2tpi791tSqJpJ2T26z0ZknPNMTeaTg+yIxUYzT5AgMBAAE=

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

Private key:
(n=0x8c03a2f69315827592841a74e8485d7867d3e2b858df4e368efceacf6e9012c12585c34e89b41b248eb4d3504daccf42f861325ba89ede647169e6a083c7a6a7a2c78e114edcccf1cb7be8875a500db57368d595500612c943bea36d214099b47c431a6a88b68f10f0366326573d1faad7f0a53e1a16efe07eb01ad0fc11e0232cd84b36500fb8a084e3642a99cd2280c227e431d633d2e361558eaa462e3574ca015f45584eee68e265f47aef7b1cb8e24f4e7c90214b679ec7aed88018c1867770f74919c54f5af0bfaa948dac8fefab25e0232d1e46a2cef7e2bd386bc59875e334ad00ac41310909b2a771b42fd7c0daafd3e110f038a5d7eff4ccce5f0e844c3981ad8a1bb2c6cfecd65fbd3f3adf927ff124e7f2ea301bd6ad13dcabc5afc01ae3050e463bfaa3153de10e6940ab1e04fe7fd6c8a40268a2688971a281be56142c6cd7477da9465086f8ca3a818a4127815c93c65f84070157c850e6b28651c36b698bbf75b52a89a49d93dbacf46649cf34c4de69383ec88c546334f9,
d=0x124b055726e768089970760e712cc73d8c7f33ff76e9120c71c91c9aa66cdf6e69cb1cb5ddaaf0e2e95c39c1a3ac60d5f4a2aa542c67395231392f5f286884df2116e67a5f6ddcbef8a183436feac6a7bee0e30ae38e2f95292b36a9f2eec04642f7f77314d2994592c4e056698e7c5d3362670c82971d971ca64092ae645d7eeb04856b1eb1b7230dc9b1d4190d22a564f89649669d95bf8c7f83a8be8b9a035cc32a21e2c44944ddd3894a2890d2b35b2a166c92de2ebe6691db47c110baf3f795d3af280101f55005380ae34a5e16e19b363749e753698edded0dfe0ce71b3db54a8a6d4ba4e2ff1c18d33595c81ec2896188993d7dd9d42f0cc9a340682d14aa3fd6b19e76712553c9e2836eb28ad368ee223d0cd57f82aac6e10cf586adf99606476faf373d674c46fe4222ab7023fd2bedb5186552fb48074bea0e230a2b7bf6c0d58b2d99f4671f939dbebb9f7a716a4a5ac5c3dd447156b6451752b578d675be5c8cb85db1163f702203a1cf582c0b64bebe8992efa74cf11a43ab63)

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

MIIG5AIBAAKCAYEAjAOi9pMVgnWShBp06EhdeGfT4rhY3042jvzqz26QEsElhcNO

ibQbJI6001BNrM9C+GEyW6ie3mRxaeagg8emp6LHjhFO3Mzxy3voh1pQDbVzaNWV

UAYSyUO+o20hQJm0fEMaaoi2jxDwNmMmVz0fqtfwpT4aFu/gfrAa0PwR4CMs2Es2

UA+4oITjZCqZzSKAwifkMdYz0uNhVY6qRi41dMoBX0VYTu5o4mX0eu97HLjiT058

kCFLZ57HrtiAGMGGd3D3SRnFT1rwv6qUjayP76sl4CMtHkaizvfivThrxZh14zSt
AKxBMQkJsqdxtC/XwNqv0+EQ8Dil1+/0zM5fDoRMOYGtihuyxs/s1l+9Pzrfkn/x
JOfy6jAb1q0T3KvFr8Aa4wUORjv6oxU94Q5pQKseBP5/1sikAmiiaIlxooG+VhQs
bNdHfalGUIb4yjqBikEngVyTxl+EBwFXyFDmsoZRw2tpi791tSqJpJ2T26z0ZknP
NMTeaTg+yIxUYzT5AgMBAAECggGAEksFVybnaAiZcHYOcSzHPYx/M/926RIMcckc
mqZs325pyxy13arw4ulcOcGjrGDV9KKqVCxnOVIxOS9fKGiE3yEW5npfbdy++KGD
Q2/qxqe+4OMK444vlSkrNqny7sBGQvf3cxTSmUWSxOBWaY58XTNiZwyClx2XHKZA
kq5kXX7rBIVrHrG3Iw3JsdQZDSKlZPiWSWadlb+Mf4OovouaA1zDKiHixElE3dOJ
SiiQ0rNbKhZskt4uvmaR20fBELrz95XTrygBAfVQBTgK40peFuGbNjdJ51Npjt3t
Df4M5xs9tUqKbUuk4v8cGNM1lcgewolhiJk9fdnULwzJo0BoLRSqP9axnnZxJVPJ
4oNusorTaO4iPQzVf4KqxuEM9Yat+ZYGR2+vNz1nTEb+QiKrcCP9K+21GGVS+0gH
S+oOIwore/bA1YstmfRnH5OdvrufenFqSlrFw91EcVa2RRdStXjWdb5cjLhdsRY/
cCIDoc9YLAtkvr6Jku+nTPEaQ6tjAoHBALbx/mrsACpwMF4pfw0T/2j4acNtZDJb
dfIgdpXZVVNeTD8IqEWqbwq9XWds1njRRGUlyQAKBytxKjEuF5xNpXjYVf+KW1xI
f0for8ca9U+LxtOSh+jJjrvoUXouwJCFL0oIvBEJwWGAmsgouN0bVhJog/NErFZE
E/k7B6aZU5fzta54fX7mX0YLsKm5P2ggIh03LgyaYiSeMWWJqUqs0TtsTCtv0dBO
KXB3CM3S0w3GZn377LFjKnV1ci6rinDslwKBwQDD7OnMxcupvk8csUqATeX7SzX7
HrFUKbHt8YpiBx3Thnt8T4umNggviLyLlvp06qVG+7ZomnKSnbb45wGmD0ek+/GM
HK35vb8JI0RYfm7AeYGazz04Qn3So4IkSm14f/8yN6LS8ICxlpGwfX41t3EJHUPc
gusLIGD1ZoM+oZbXKpAlyOUUmTo5FJcpetKmwJkoGQk0RGFcD/mINtR7WdqDTG58
2xmXRMwz1zNVIGradVjISB7uvHpmUpIaaWLCzO8CgcEAqCAUs6ZXMKkRijeQbzBl
lM5WRCcP4cdzySRUVrn4VDlg0LzgB8Xtbm1AnX/EShvnQx1KbyLIHABPygqV4Crr
WvdVcRZxh4mIj0kj4VLBBm1qN51+EUzKQ53o4uR8S1RadSs5yl6wvS43EKN74Jby
rtAmEzaVOmIuCOlaypw12ns6CDDrA+gqvnCX1iJMRyDguQCw7Rwj/Yrz0mCEl//h
+T45ceG9bDWol5aNHLoXA53FKxqOFycPKgrY+FLlU4nZAoHAOxH/v4RXDhtZoM33
J03VK/mWEdtEHZrgkVvEnB+HJ5IhQu58rSUXPLWeGvvvETb5k7gqW8lNB9VTKCIF
xjpPIHfxcIvpDCXgJfIjFgcwfwljQPiAfajWZJ51i1mBPdZha5OInM50DpbV3/9G
AQ4In3XaUu6JzPX7JaG9qjFv1/l2Ml4qaxZzjmgd1xy3zBy/UG6T7tU7AVWzpxTY
5UPG9NUjbrNkOM4+PtcAHAdFEA5XMTNFWDctNBJrCFmDtDWzAoHBALVHem1UIWPF
gDdoX0Q+E6uwtA4N5nnRRIkBhl4Jl+EFcSiamwrhsAuaJrkclrtkLvnIpeWWgxJc
F6KwpjmEHggczkYDCjJsA3IhxC3UIXfApXkPdqexKS/y16PCHmzFePOQTwk9Ycwm

yyE0VeDZlE2qmVnPqmjF9QghJwiQR6vBKL5WVA8xfN4pPP0RWfDlDE2VbiLLlzcO

6eGUxOVOuBNsGbykjofOXnkcBJ7zpK495nptnFeXlMDaTIIPBwGJyA==

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

Encrypted:
b'4bb51a5a7dac372b0d82ebbce2755e6660d13e5777fa6894c42fb377ab63a9ebb9a7ac75fc2c83a5ffcb11746
42317dc30deeb4818742d581654e9488919e24da3e20f7d79a8a4bfe0daee349ab8540f6ee43eea8918f089f06
5ee3f01bf4170f4423c4c828222a3230529ec3bfd248de59972e040816ea1b26ff6f8cf73ed5cd7abf9eb7e6853
8aab450984a04e87dff98cc3a15ee4a405284f4c863a42c4b8b1a29b5983470fb985a4e5cd667311718c9e812
1cef54085ea41f5a0a24f37bf8614fcc799df90136e92abd19f1d4432fb89c2aafa56fa65b93670aba9abbf53c64
c799e31eb1c0e14e70c99ac72692d50256b919fac37476ca32906b78161cc867409e456cc745f172e4a29d053
7b8b96c7779eb8ae372c4b4e5c08fc66a7cad137540896ff2b7ffa9d9b08498e07990e4b0754f4d52160726c9c
a90f40568a0e58529ca9a57d1aca4944879f46d00c0b72f09b55c0a50407d888fb860459a39e42ee597878612
f37701c3b3aa870d3d1de56dd912c29822c57dae12d95207c'

Decrypted: b'Its Lonewolf aka Harsh'

Process finished with exit code 0