Name : Harsh Verdhan singh
Roll no : 20mcs009
NS assignment

Client Side :

Input :
Message: 0b1101011100101000 (55080)
Secret Key: 0b0100101011110101
Public Key parameters: (101, 221)
Private key parameters: (173, 221)
Encrypted Secret Key: [36, 44, 36, 173, 44]
Cipher text: 29241
Digest: 9d2e4f426787e2582742d4c3c45740cb313722bcba53d7f26d9a10bc2a3196bb
Digital Signature: [44, 172, 33, 186, 52, 85, 52, 33, 97, 191, 88, 191, 186, 33, 66, 88, 33, 191, 52, 33, 172, 52, 73, 51, 73, 52, 66, 191, 52, 107, 73, 115, 51, 121, 51, 191, 33, 33, 115, 73, 115, 184, 66, 51, 172, 191, 85, 33, 97, 172, 44, 184, 121, 107, 115, 73, 33, 184, 51, 121, 44, 97, 115, 115]

Server Side:

Input:
Public Key parameters: (61, 221)
Private key parameters: (85, 221)
Decrypted Secret key: 19189
Decrypt Message: 55080 (0b1101011100101000)
Message Digest: 9d2e4f426787e2582742d4c3c45740cb313722bcba53d7f26d9a10bc2a3196bb
Signature verified/ Signature Not Verified : verified

```
(ghost㉿in-the-shell)-[~/stuff/iiitdmj/classes/SEM-2/1.crypto/project/assignment-2/ass2]
$ python3 server.py
Connection to ('127.0.0.1', 48210) has been established!!

please send server public key
<class 'str'>
[36, 44, 36, 173, 44]
b'29241'
[44, 172, 33, 186, 52, 85, 52, 33, 97, 191, 88, 191, 186, 33, 66, 88, 33, 191, 52, 33, 172, 52, 73, 51, 73, 52, 66, 191, 52, 107, 73, 115,
51, 121, 51, 191, 33, 33, 115, 73, 115, 184, 66, 51, 172, 191, 85, 33, 97, 172, 44, 184, 121, 107, 115, 73, 33, 184, 51, 121, 44, 97, 115,
115]
<class 'list'>
[36, 44, 36, 173, 44]
<class 'str'>
55080
333333333
public key (61, 221)
private key (85, 221)
dec sec key  19189
dec message 55080
message digest
Verification successful:
9d2e4f426787e2582742d4c3c45740cb313722bcba53d7f26d9a10bc2a3196bb  =  9d2e4f426787e2582742d4c3c45740cb313722bcba53d7f26d9a10bc2a3196bb
```

```
(ghost㉿in-the-shell)-[~/stuff/iiitdmj/classes/SEM-2/1.crypto/project/assignment-2/ass2]
$ python3 client.py
64
[36, 44, 36, 173, 44]
[44, 172, 33, 186, 52, 85, 52, 33, 97, 191, 88, 191, 186, 33, 66, 88, 33, 191, 52, 33, 172, 52, 73, 51, 73, 52, 66, 191, 52, 107, 73, 115,
51, 121, 51, 191, 33, 33, 115, 73, 115, 184, 66, 51, 172, 191, 85, 33, 97, 172, 44, 184, 121, 107, 115, 73, 33, 184, 51, 121, 44, 97, 115,
115]
client pub key : (101, 221)
clinet private key : (173, 221)
enc sec key:  [36, 44, 36, 173, 44]
cihper text:  29241
digest is  9d2e4f426787e2582742d4c3c45740cb313722bcba53d7f26d9a10bc2a3196bb
digital sign :  [44, 172, 33, 186, 52, 85, 52, 33, 97, 191, 88, 191, 186, 33, 66, 88, 33, 191, 52, 33, 172, 52, 73, 51, 73, 52, 66, 191, 52
, 107, 73, 115, 51, 121, 51, 191, 33, 33, 115, 73, 115, 184, 66, 51, 172, 191, 85, 33, 97, 172, 44, 184, 121, 107, 115, 73, 33, 184, 51, 12
1, 44, 97, 115, 115]
(ghost㉿in-the-shell)-[~/stuff/iiitdmj/classes/SEM-2/1.crypto/project/assignment-2/ass2]
$ >
```