Name: Ahmed Ahmed

Server:

```
C:\Users\ahmed\AppData\Local\Programs\Python\Python38\python.exe C:/Users/ahmed/OneDrive/Documents/coe817/lab2/Lab2/lab3/chat_server.py
Key distribution messages:
Message 2: b'mookl4le|d1zbqmt9'
**Key distribution messages end here**

Enter a message: hello
Enter a message:
Cypher received: b'\xec\xbc\xb6\x1fs\xf6w\x17\x0c4Z\x91\xd5\xa1R!'
Message received: hey there
Enter a message:
bye
Enter a message:
```

Client:

```
C:\Users\ahmed\OneDrive\Documents\coe817\lab2\Lab2\lab3>python chat_client.py
Key distribution messages:
Message 1: b'INITIATOR A|mookl4le'
Message 3: b'd1zbqmt9'
Message 4: b'292rl6ya'
**Key distribution messages end here**

Enter a message:
Cypher received: b'V\xe6.Itd\xd5G'
Message received: hello
Enter a message:
hey there
Enter a message:
Cypher received: b'B\x01\x0c\xa0\xc6\xd2-H'
Message received: bye
Enter a message:
```

How to prevent replay attacks:

```
nonceList.append(msg.decode().split('|')[-1])

msgToSend = f'{nonceList[0]}|{generate_key()}'
cypherMsg = rsa_encrypt(msgToSend, pubKeyA)
s.send(cypherMsg)

msg = rsa_decrypt(s.recv(1024), keyPairB)
while msg.decode().split('|')[-1] in nonceList:
    msg = rsa_decrypt(s.recv(1024), keyPairB)
print(f'Message 3: {msg}')
nonceList.append(msg.decode())

msg = rsa_decrypt(s.recv(1024), keyPairB)
while msg.decode() in nonceList:
    msg = rsa_decrypt(s.recv(1024), keyPairB)
print(f'Message 4: {msg}')
keyS = msg.decode()
```

In this portion of the code, the client checks to see if the nonce of the sent message matches one of the nonces of the already sent messages. If it does, then the client ignores the message and waits to receive another one using the while loop.