Readme for Phase III

1. Read the readme file for (phase I) to know how the chat app works and how it can be tested using two virtual machines.
2. Read the readme file for (phase II) to know how the AES_256_CBC works and how exchanging of messages happen.
3. Bob is the server and Alice is the client
4. Alice_id is her IP address that replaces the name “Alice” in the protocol.
5. Bob_id is his IP address that replaces the name “Bob” in the protocol.
6. When Alice clicks connect to Bob the following will happen:
    a. Alice will do the following:
        i. Send initialization vector (IV) for AES cryptosystem (from ph II)
        ii. Chooses her secret key randomly as specified (a)
        iii. Computes her key (g^a mod m)
        iv. Computes her response as specified (RA)
        v. Sends her key and RA to Bob
    b. Then Bob will do the following:
        i. Chooses his secret key randomly as specified (b)
        ii. Computes his key (g^b mod m)
        iii. Computes the shared key using Alice’s key to be (g^ab mod m)
        iv. Destroys b by equating it to zero
        v. Computes H that is the hash of (Alice_id, Bob_id, RA, RB, Alice’s key, Bob’s key, the shared key)
        vi. Computes SB that is the signing of the Bob_id and H
        vii. Sends his key, RB and SB to Alice
    c. Then Alice will do the following:
        i. Verifies SB using Bob’s public key (e_Bob, N_Bob) from the RSA
        ii. Extract H that computed by Bob(H_Bob) from SB
        iii. Computes the shared key using Bob’s key to be (g^ab mod m)
        iv. Destroys a by equating it to zero
        v. Computes SA that is the signing of the Alice_id and H
        vi. Computes H that is the hash of (Alice_id, Bob_id, RA, RB, Alice’s key, Bob’s key, the shared key)
        vii. Now she compares H against H_Bob, if they equal she will proceeds to step 3 otherwise she will not authenticate Bob and she will terminate the session.
        viii. If the comparison matches she will send E(Alice_id, SA, k) encrypted by AES_256_CBC with k as the key.

d. Then Bob will do the following:
   i. Decrypts E(Alice_id, SA, k) and verifies SA using Alice's public key (e_Alice, N_Alice)
   ii. Extract H_Alice from SA
   iii. Now he compares H against H_Alice, if they equal he will proceeds to step 4 otherwise he will not authenticate Alice and he will terminate the session.
   iv. If the comparison matches then the chat program will start and they can exchange messages with AES_256_CBC cryptosystem.