1. Attacker.java – Run one attack at a time
   1.1. Masquerade As client Attack
   1.1.1 Run the android app
   1.1.2 Call Attack_m_c() in main of Attacker.java and run it.(You will get the encrypted data.)
   1.2 Replay Attack
   1.2.1 Run MerchantServer.java
   1.2.2 Call login_attack() in main of Attacker.java and run it.(the timestamp will act as a nonce and merchant server will not accept the attacker.)
   1.3 Masquerade As merchant Attack
   1.3.1 Run the MerchantServer.java till login.
   1.3.1 Run the android app request the list of products.
   1.3.2 Call products_attack() in main of Attacker.java and run it.(as it does not have the session key the client rejects this list).

2. Limitations:

`` 2.1 One port is reserved for one entity at a time.

2.2 Key exchange through Certificate is not defined.