**Entities (Note there will be more entities):**

1. Server
2. ClientA
3. ClientB

**Items**

1. SRSA – Servers RSA public and private key pair
2. NA – nonce from A, server and ClientA remember this for their session
3. NB – nonce from B, server and ClientB remember this for their session
4. KSA – Session key between Server and ClientA
5. KSB – Session key between Server and ClientB
6. KAB – Session key between ClientA and ClientB
7. EA – Encryption key for ClientA communication to ClientB
8. DB – Decryption key for ClientA communication from ClientB
9. EB – Encryption key for ClientB communication to ClientA
10. DA – Decryption key for ClientB communication from ClientA
11. AuthA – MAC for messages ClientA sends
12. AuthB – MAC for messages ClientB sends

**Scenario:**

ClientA wants to talk to ClientB

**Step 1 - Initial Exchange (Login):**

1. ClientA wants to log in 🡪 sends SRSA{uname, pw, NA} 🡪 Server
2. Server decrypts and checks database for ClientA information.
3. ClientA 🡨 SRSA[gs mod p, NA] 🡨 Server
4. Client 🡪 SRSA{ga mod p, NA} 🡪 Server
5. Both agree on KSA = gsa mod p

**Step 2 - Server Gives ClientA Buddy List**

1. KSA{ClientA buddy list}
2. ClientA receives his buddy list

**Step 3 - ClientA Requests to talk to ClientB**

1. ClientA 🡪 KSA{NA, ClientA, “Want to talk to ClientB”} 🡪 Server
2. ClientA 🡨 KSA{NA , KAB , “ClientB”, ticket to ClientB = KSB{ClientA, NB KAB}} 🡨 Server

**Step 4 – ClientA sends ticket to ClientB (Mutual Authentication)**

1. ClientA 🡪 “ClientA wants to talk”, KAB{ClientA, ClientB, NA}, ticket to ClientB 🡪 ClientB
2. ClientA 🡨 KAB{ClientA, ClientB, NA + KAB, NB} 🡨 ClientB
3. ClientA 🡪 KAB{ClientB, ClientA, NB + KAB} 🡪 ClientB

**Step 5 – Derive Encryption and Decryption keys and well as message authentication keys**

1. ClientA computes EA = KAB + NA for encryption and DB = KAB + NB for decryption
2. ClientB computers EB = KAB + NB for encryptions and DA = KAB + NA for decryption
3. ClientA computes AuthA = EA + KAB
4. ClientB computes AuthB = EB + KAB

**Step 6 – Communication**

ClientA and ClientB communicate with their derived keys.