Server	**Client**
	Send “ClientAuth”
Send server's public Key	
	Verify server's public key, generate a new random shared AES key, encrypt this key with public key and send it back to the server
decrypt shared AES Key with server private key	
All communication from now on is encrypted via this shared AES Key	
	send the username say, “alsnyder”
send random nonce for alsnyder encrypted with alsnyder's public key	
	decrypt nonce with alsnyder's private key and send it back
send back “OK” or “auth failure”	
	receive OK Handshake done

Mail Protocol begins:
Client can send:

- “Send” + username +”\n” + email
- “Upd” to get largest email number
- “Retr” + # to get a list of those emails
- “import” to import a public key from the server