Bonus Project (*Computer Networks*) [Mahavir Jhawar]
Submission Deadline: May 3, 2017

The goal of this assignment is to implement a TCP client and server for INTERACTIVE LOGIN SYSTEM.

- **Setting up the system:**
  - Pick two different primes p, q and compute $n = p \cdot q$.
  - Choose $a_1, a_2, a_3 \in \mathbb{Z}_n^*$ and compute $b_i = a_i^2 \bmod n$, $1 \leq i \leq 3$.
- **Server:**
  - Initialize the server with the following three entries:

Login Id	Corresponding Information
Name-1	(b_1, n)
Name-2	(b_2, n)
Name-3	(b_3, n)

  - Wait for a client connection on a specific port
- **Client:**
  - The client will connect to the server at the listening port
  - It then executes a 3-step interaction with the server and establishes log in access for Name-i, $i \in \{1, 2, 3\}$ to the server
- **3-step Interaction:** Open a terminal and run the server. Suppose, Name-1 wants login access to the server. Open another terminal and run the client on this. The following interaction between client and server will ensure that Name-1 gets access to the server.
  - Client: It will pass the server a number $y = x^2 \bmod n$ (x is known to the user and picked randomly) and the id Name-1.
  - Server: On receiving $(y, \text{Name-1})$, the server will pick a random bit $t \in \{0, 1\}$ and pass t to the client.
  - Client: On receiving t, it will pass $z = x$ to the server if $t = 0$ or $z = a_1 \cdot x$ if $t = 1$.
  - Server: On receiving z, it will check if $z^2 \bmod n = y$ if $t = 0$ or $z^2 \bmod n = b_1 \cdot y$ if $t = 1$. If successful, it will pass the msg "Welcome Name-1" to the client; otherwise it will pass the msg "Access denied" to the client.
- **Support Concurrent Access:** At any time, server can interact with three client running simultaneously for login access.