CS 4021 Number Theory and Cryptography

Assignment Problem

C1)

A) Construct two programs: Server and Client to realize remote loginsystems.

- It takes input username and password on client and send a login_req to server.
- The server maintains a login table to manage its access control.

B) Implement different cryptographic algorithms to enhance the security of your system

- Instead of plaintext storage utilize SHA-1 to protect the password on the server.
- Instead of plaintext communication utilize AES to encrypt the communication between client and server.(Assume that the key has been established)

B) Implement key agreement algorithm in your system

List of Tools

T1) Cryptool	**T2) OpenSSH**	**T3) TrueCrypt**	**T4) GnuPG**	**T5) OpenSSL**	**T6) Stunnel**
T 7) Palcrypt	**T 8) Android Privacy Guard**	**T9) BestCrypt**	**T10) CrossCrypt**	**T 11) Enigmail**	**T 12) gnoMint**
T13) Cain and Abel	**T14)BackTrack**	**T15) OpenPuff**	**T 16) AxCrypt**	**T17) Cloudfogger**	**T18) AES Crypt**
T19) DiskCryptor	**T 20) Sophos free encryption**	**T 21) GPG**	**T 22) Steg**	**T23) iSafeguard**	