Desain Komunikasi Chat

1. Metode yang digunakan:
   1. Menggunakan metode enkripsi asimetris dengan algoritma RSA untuk menjaga kerahasiaan data sekaligus berfungsi sebagai digital signature
   2. Menggunakan hash fuction SHA-512 untuk menjaga integritas data
   3. Public key distribution menggunakan metode Public Key Directory
2. Login
   1. Client : LOGIN username password
   2. Server : LOGIN ok/error
3. Logout
   1. Client : LOGOUT username
   2. Server : LOGOUT ok/error
4. Private message
   1. Client : PM src\_username dest\_username message
5. Create group
   1. Client : CG username group\_name
   2. Server : CG ok/error
6. Group message
   1. Client : GM src\_username group\_name message
7. Broadcast message
   1. Client : BM src\_username message

Keterangan :

1. Karena broadcast sehingga messagenya sendiri tidak perlu dienkripsi, hanya perlu dipastikan keaslian dan asal datanya