Diskusi KIJ

5113100059 Joshua Kevin R

5113100132 Gian Sebastian

5113100167 Rahmat Nazali S

1. Asumsi
   1. Saat melakukan login pertama kali, sebuah key digenerate oleh aplikasi klien dan ikut dikirimkan ke server. Setelah itu, server menyimpan key yang digenerate aplikasi dan disimpan. Key tersebut berlaku selama sesi akun tersebut hidup. Sementara untuk counter juga berlaku hal yang sama layaknya key.
2. Login
   1. Client : LOGIN username password

Alasan :

* + 1. K dan counter digenerate random oleh aplikasi pada saat pengiriman
    2. Untuk informasi penting akan digunakan metode block cipher AES
    3. Blok cipher menyediakan kemanan tinggi dan integritas tinggi
    4. Menggunakan AES counter mode karena cocok untuk data streaming dan dapat dilakukan secara pararel
  1. Server : LOGIN ok/error

1. Logout
   1. Client : LOGOUT username
   2. Server : LOGOUT ok/error
2. Private message
   1. Client : PM src\_username dest\_username message
3. Create group
   1. Client : CG username group\_name
   2. Server : CG ok/error
4. Group message
   1. Client : GM src\_username group\_name message

Alasan :

* + 1. Karena group message tidak terlalu memiliki informasi sepenting private message maka dapat menggunakan stream cipher karena lebih cepat dalam hal komputasi dibandingkan block cipher

1. Broadcast message
   1. Client : BM src\_username message

Alasan :

1. Karena broadcast sehingga tidak perlu secure