Desain Komunikasi Chat

KIJ F

Joshua Kevin Rachmadi 5113100059

Gian Sebastian Anjasmara 5113100132

Rahmat Nazali Salimi 5113100167

1. Metode yang digunakan:
   1. Menggunakan metode enkripsi asimetris dengan algoritma RSA untuk menjaga kerahasiaan kunci simetris RC4 sekaligus berfungsi sebagai digital signature yang dikirimkan pada awal kali client bergabung. Kemudian kunci RC4 tersebut digunakan untuk mengamankan isi pesan
   2. Menggunakan hash fuction SHA-512 untuk menjaga integritas data
   3. Penyimpanan kunci simetris RC4 diimplementasikan dengan penggunaan ArrayList <Pair <Socket, Pair<Username, RC4 Key>>>
2. Client bergabung (terkoneksi)

Server membuatkan Key simetris untuk RC4 (KRC4), lalu di enkripsi dengan RSA menggunakan private key milik server

Kemudian hasil enkripsi tersebut dikirim langsung ke client, lalu setelah diterima dilakukan dekripsi menggunakan public key server untuk mendapatkan key RC4

1. Login
   1. Client : LOGIN username password

DS = digital signature =

Selanjutnya, pesan dibuat dengan format : message + “ “ + DS, dengan “ “ adalah sebuah spasi yang membedakan DS dengan message

* 1. Server : LOGIN ok/errors

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