Tugas Diskusi Instant Messaging.

* Diasumsikan bahwa semua user memiliki Public Key milik Server
* Diasumsikan juga bahwa Public Key dari semua user disimpan oleh Server
* Semua pesan yang dikirimkan, baik oleh server maupun client, akan menggunakan Digital Signature untuk menjaga integritas data, kecuali bila dinyatakan sebaliknya.
* Proses Login:
  + Pertama, Client akan mengirimkan pesan berisi ID dan Password (hashed) (lalu diberi digital signature), lalu dienkripsi asimetris menggunakan Public Key milik Server
  + Server akan mendecrypt pesan dari Client, mengecek integritas Digital Signature, lalu mencocokkan ID dan Password.
    - Bila gagal, maka Server akan mengirimkan error message.
    - Bila berhasil, maka server akan merubah status User menjadi Online, sehingga user lain dapat mengkontak nya
* Proses Handshake 2:
  1. Ketika seorang user ingin men-*chat* user lainnya, maka ia (pihak pertama) akan meminta public key user target (pihak kedua) ke Server, lalu mengirim pesan request (berisi ID pihak pertama, lalu sebuah string acak N1) ke user target. pesan akan di enkripsi dengan public key dari Target.
  2. Target akan menerima pesan, membuka pesan request tersebut, lalu meminta public key Pihak Pertama ke Server, lalu mengirim pesan ke Pihak Pertama yang berisi string acak N1, lalu ditambah string acak N2. pesan diberi digital signature, dienkripsi menggunakan public key dari pihak pertama, lalu dikirim ke pihak pertama.
  3. Pihak pertama akan menerima pesan, mendecrypt, mengencek digital signature, lalu mengecek kebenaran N1. lalu ia akan mengirimkan pesan N2 yang diberi digital signature , lalu dienkripsi dengan public key target.
  4. Target menerima pesan, men-decrypt, mengecek digital signature, lalu mengecek N2. bila benar, maka akan masuk ke proses **chat**
* Proses Chat:
  + Setelah proses Handshake berhasil. maka akan melakukan chat biasa yang mana setiap pesan akan diberi digital signatrure, lalu dienkripsi asimetris menggunakan public key dari pihak kedua.
* Kelemahan:
  + Too reliant to server
  + Cara mengakhiri sesi chat, maupun Disconnected, hanya menggunakan fitur socket bawaan java (kalo socket mati, berarti off)
  + Hanya dapat melakukan chat bila kedua pihak Online, tidak dapat melakukan sistem Inbox (seperti email)
  + Bisa terjadi “tabrakan” (aku login pake ID ku, terus ada orang login pake ID ku juga, gatau deh gimana hasilnya ntar, enaknya gimana?)
* Pertanyaan:
  + Chat nya mau lewat server? apa dikirim peer2peer? jadi server cuma buat autentikasi aja?
  + Bisa ndak diimplementasiin di kodingan bapaknya? :v
* Todo:
  + Nentukan metode enkripsi asimetris dan belajar metode tersebut
  + Nentukan metode hash, digital signature, dan mempelajarinya
  + Mencari kelemahan
  + Berdoa semoga ada fungsi2 nya enkripsi di java :’v
  + Mencari fungsi2 enkripsi yang dibutuhkan di java (kalo ada :’v)