Protocolos del Sistema de mensajería instantánea.

CHRISTIAN SANCHEZ, ESTEBAN FLORES

REEDME

Los comandos que se utilizan para el programa son los descritos en los requerimientos del proyecto.

Usuarios registrados previamente:

Estos son los usuarios preregistrados en el sistema (Usuario : Contraseña)

Esteban : Flores

Christian : Sanchez

E : F

C : S

Dependiencias json-simple

How to add json-simple dependency:

https://stackoverflow.com/questions/44087645/what-is-the-right-way-to-add-json-simple-library-on-intellij

Protocolo implementado

Protocolo LOGIN

- ✓ RSA 2048
- ✓ $P = h\{pwd\}$
- ✓ $P' = h\{P, username\}$
- ✓ h: $SHA256$
- ✓ K_{AS}: AES 128

Alice

Server

$LOGIN$

Guarda:
h(username), P'
Y estado de conexión
de los usuarios

$Puzzle\langle$n bits, $C_1\rangle$

Genera:
- Par RSA $\langle K_A, K_a\rangle$
- K_{AS}

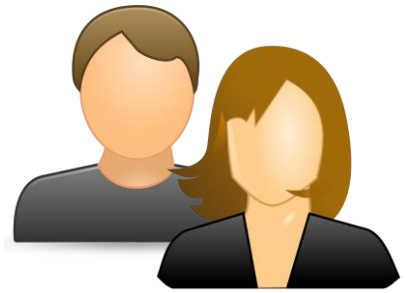
Client port, Sol, $\{K_{AS},\ P',\ username\}_S$,
$K_{AS}\{K_A, C_2, [C_2]_A\}$

$K_{AS}\{[C_2]_s\}$

Agrega a Alice a los usuarios conectados, broadcast a todos los usuarios conectados: Alice se conectó!

$K_{AS}\{USERLIST\}$

Protocolo de actualización de usuarios conectados



Users

Server

$user$

Protocolo LOGOUT

Alice

$LOGOUT$

$Puzzle\langle \text{n bits}, C_1 \rangle$

$Sol, \{username\}_S, K_{AS}\{[LOGOUT]_A\}$

Server

Protocolo de solicitud de datos de Bob

Alice

Server

$WANT\ TO\ TALK$

$proffRobot, Puzzle\langle \text{n bits}, C_1 \rangle$

$Sol,\ K_{AS}\{Bob, DH_A, C_2, [C_1]_A\}$

DH_A: Alice encoded DH public key

$ticket, K_{AS}\{puertoB, [C_2]_S\},$
$ticket\ to\ Bob = K_{BS}\{Alice, K_A, DH_A\}$

Protocolo de comunicación

Usando Diffie-Hellman

$$K_{AB} = g^{ab} mod\ p$$

$$ticket, ticket\ to\ Bob = K_{BS}\{Alice, K_A, DH_A\}$$

La implementacion para el code freeze llegó hasta aqui.

$$DH_B, K_{AB}\{C_1\}$$

$$K_{AB}\{C_2, [C_1]_A\}$$

Alice

Bob

$$K_{AB}\{m, h(m), [m]_B\}$$

$$K_{AB}\{m, h(m), [m]_A\}$$