Encrypted Chat

Robert Bierbauer

Firstname.Secondname@uibk.ac.at

01.12.2014

Quality and Security Program

University of Innsbruck

QSP TIROL

Topic

- Create chat program
  - Users can communicate with other users
  - Messages are sent over a server
- Provide end to end encryption
  - Server does not store any keys
  - Server can't read messages

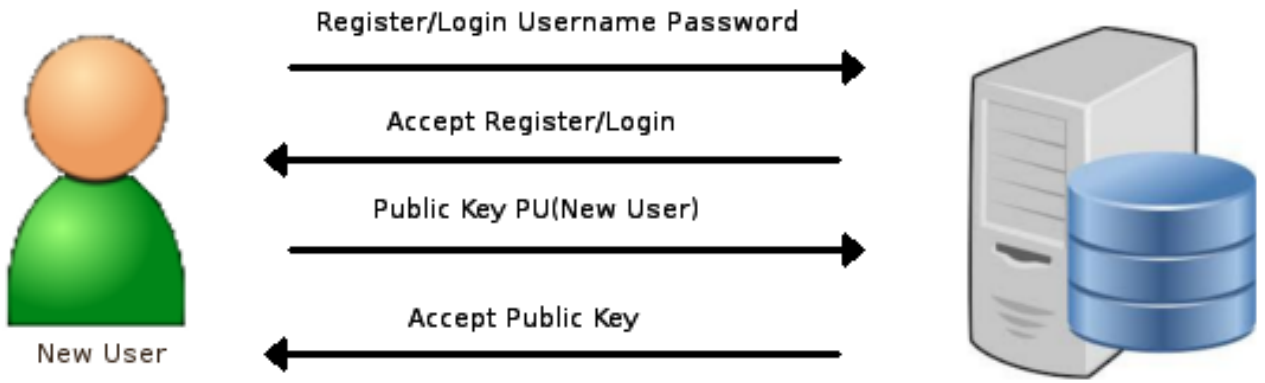
Realisation

- Program in Java
  - Using Java Swing and Crypto
- Centralised Network
  - All messages are sent over one server
- Communication through chatrooms
  - Users can create and join chatrooms
- Symmetric and asymmetric encryption

Login/Register

- Unique Username and password
- Users stored persistently in database
- If successful client generates public key
- Public key is sent to the server
  - Server stores public key of users temporarily
  - Used when the user joins a chatroom

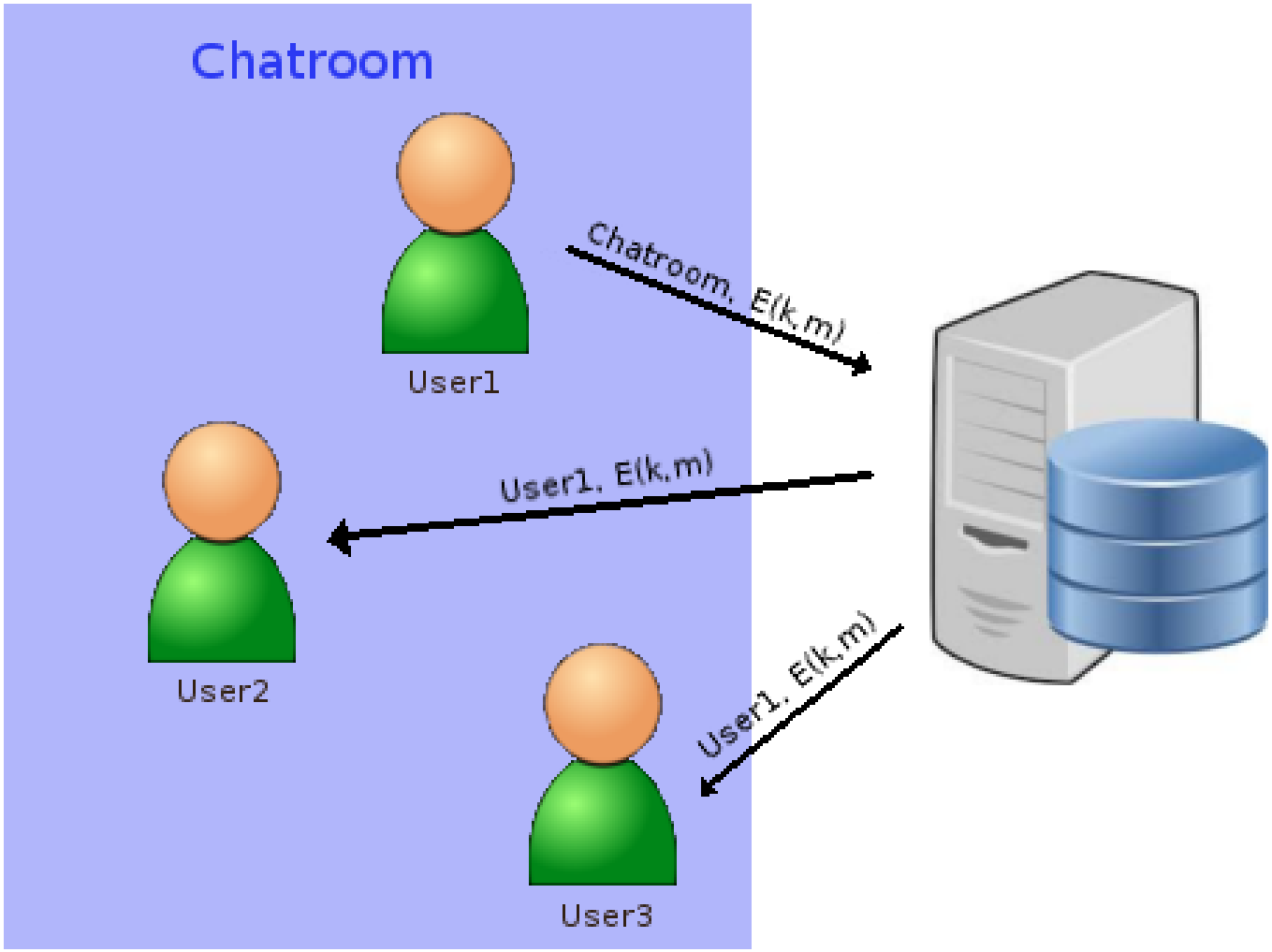
Login/Register (cont.)



Encryption of the messages

- Symmetric encryption
- Using a shared key
  - Get exchanged when joining a chatroom
- Encryption with AES
  - Secure encryption method
  - Provided by the Crypto library

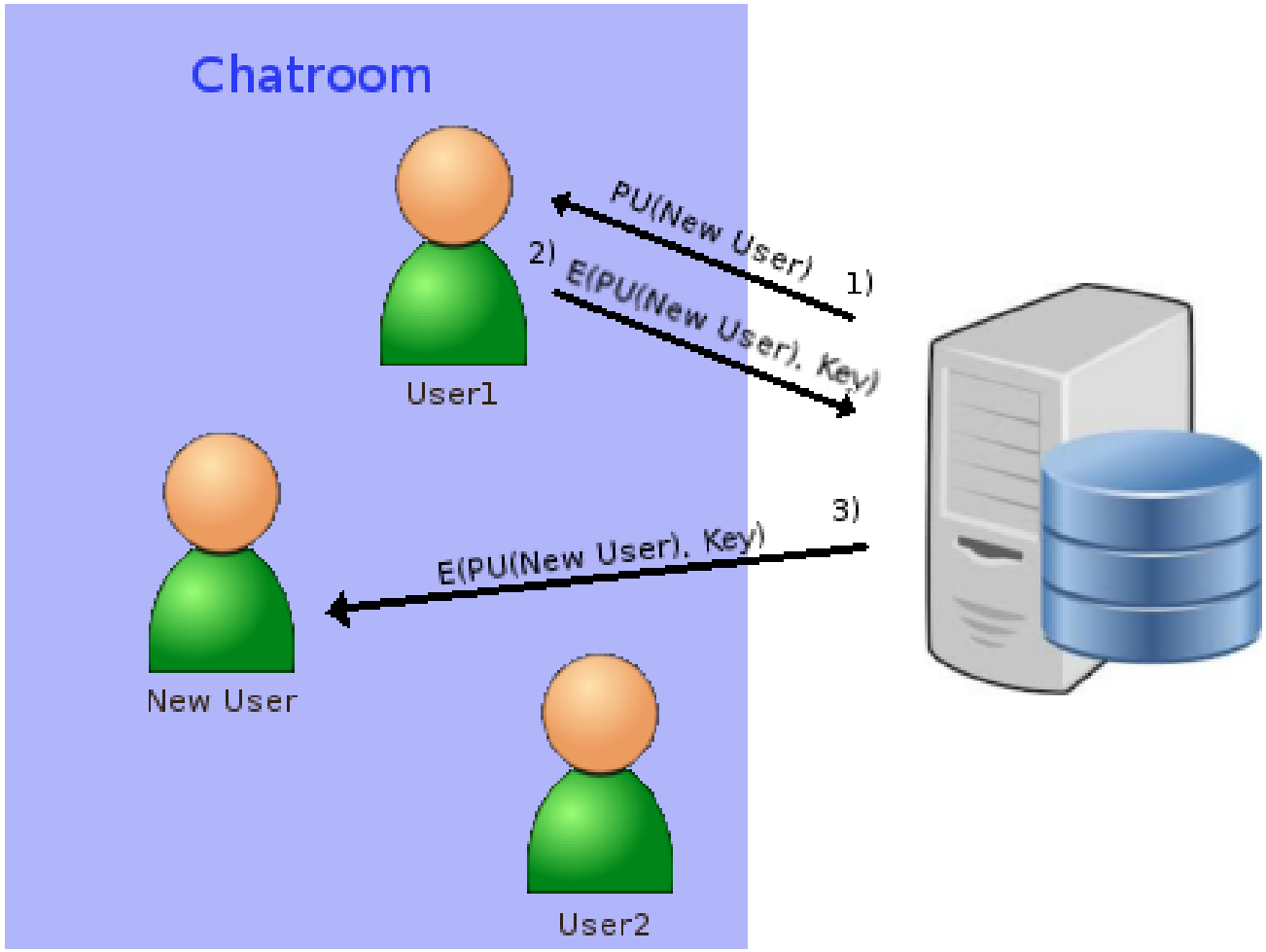
Encryption of the messages (cont.)



Key exchange

- New users need the message key
- Key should not be known by the server
  - can not be sent in plaintext
- Key is encrypted with asymmetric encryption
  - Using RSA as encryption method
  - Public and private key can be produced in advance
  - Provided by the Crypto library

Key exchange (cont.)



Demo

Thank you for your attention!
Questions?