Assignment 5 Simon Razniewski

Chat with RSA Encryption

This programming assignment gives you the opportunity to extend one of your previous chat applications with RSA encryption.

Instructions: You are allowed to work alone or in teams of two students. Extend one of your previous chat client solutions (TCP or RMI) to encrypt and decrypt messages using RSA.

RSA requires each peer to have a private and a public key. The private key is used to decrypt messages locally, while the public key will be shared over the network so that communication partners can encrypt messages.

Deliverables

1. A 2-3 pages report containing
    - A discussion of how you extended your previous chat application to include RSA-encryption.
    - A discussion of the security of the communication in your chat application
    - A discussion of the security of your chat application wrt. other threats than just the decryption of messages.
2. Code of your extended program

Submission: Friday, 8th of May 2015, 10:00 am via Moodle