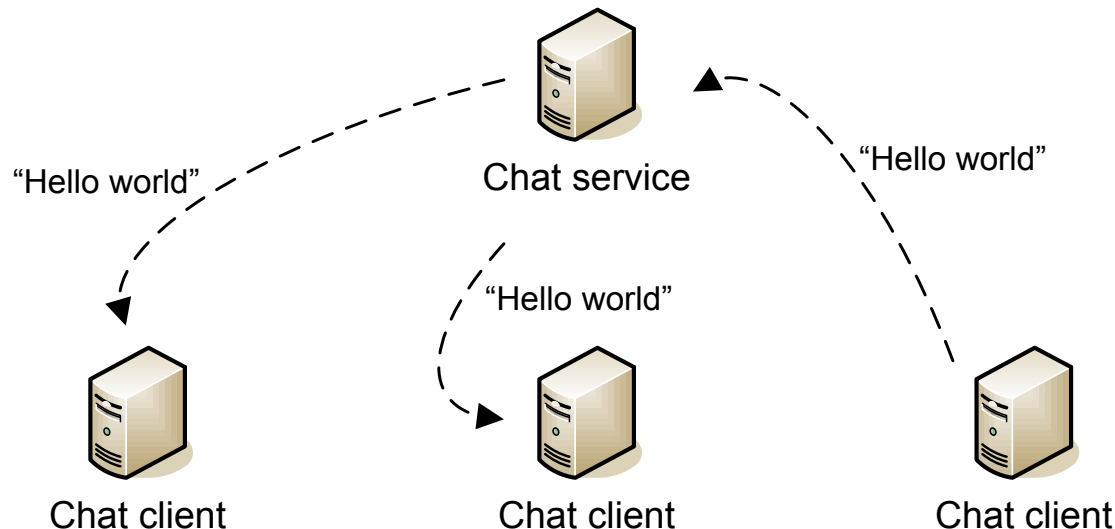# SSC/STI 2014/2015

Practical class #10

- **Practical Assignment #3 (Programming and Security)**
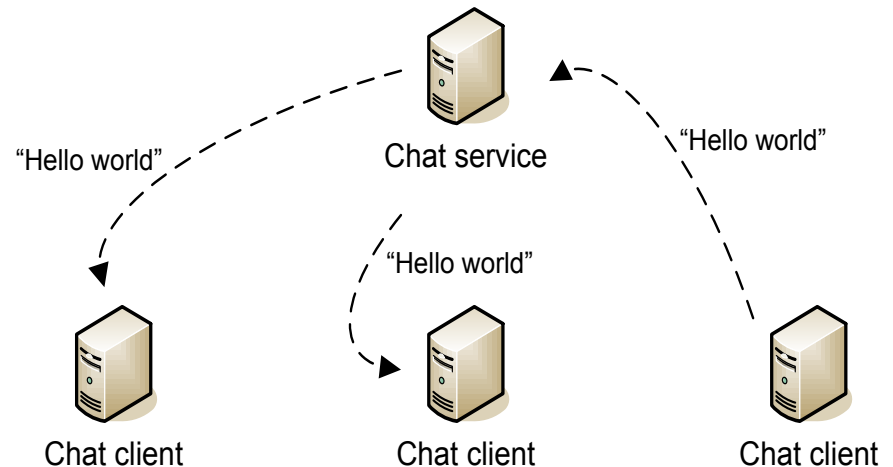
Practical Assignment #3

- A simple Chat service on top of which security will be applied
- Our goal is **security**, not to improve the Chat service
- Source code in Java provided

Practical Assignment #3

Security requirements:
- Confidentiality
- Authenticity
- Integrity
- Non-repudiation
- Key management, support:
  - Security provisioning
  - Key negotiation
  - Key renewal
- Secure management of confidential information

Chat service

"Hello world"

"Hello world"

"Hello world"

Chat client

Chat client

Chat client

Practical Assignment #3

- Important aspects
    - What is the **security model**?
    - What are the **security procedures**?
    - What are the **cryptographic algorithms** employed, and how are they employed (usage mode, key size, …)?

"Hello world"   Chat service   "Hello world"

"Hello world"

Chat client   Chat client   Chat client
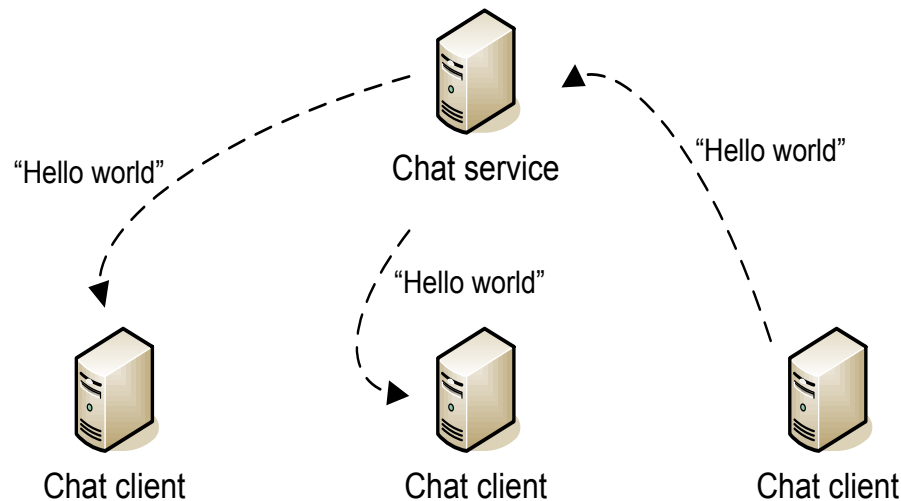
Chat service, source code in Java

Java source code provided:
- ChatClient.java
- ChatServer.java

Example usage:
java ChatServer 5555
java ChatClient 10.10.0.1 5555

"Hello world"   Chat service   "Hello world"

"Hello world"

Chat client   Chat client   Chat client