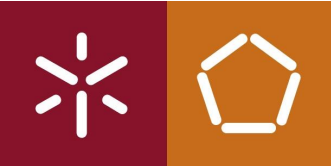
****

Universidade do Minho

Departamento de Informática

**Criptografia e Segurança em Redes**

**Engenharia de Telecomunicações e Informática**

Trabalho Prático 2

Grupo :

Diogo Araújo a101778

Fernando Mendes a101263

Junlin Lu a101270

Conteúdo

* [Introdução 3](#_Toc150608870)

# 1.Introdução

O objetivo deste trabalho pratico é aprofundar o nosso conhecimento, no âmbito da unidade curricular de CSR, sobre Criptografia simétrica e Criptografia das chaves. Desenvolvemos um sistema de comunicação (uma arquitetura cliente-servidor) onde o servidor aceita conexão via *socket* em um endereço IP e porta conhecidos pelo cliente, e aplicamos diferentes níveis de garantia de segurança descordo com os requisitos.



Figura 1: Esquema básico do serviço de chat

Após o estabelecimento de comunicação entre as duas entidades, o servidor deverá enviar uma lista de opções de comunicação com os diferentes tipos de garantia de segurança suportadas. o cliente e o servidor iniciarão a troca dos parâmetros exigidos pelo o mecanismo de segurança escolhido pelo cliente

# 2.Modo de segurança

O serviço desenvolvido deverá suportar três modos de garantia de segurança:

A - **Integridade**: neste modo, o serviço garante a integridade das mensagens trocadas entre os utilizadores, mas não implementa um mecanismo de garantia da confidencialidade;

B - **Confidencialidade e Integridade**: neste modo, além da garantia da integridade das mensagens, o serviço deverá implementar um mecanismo para a garantia da confidencialidade suportado por uma cifra simétrica;

C **- Confidencialidade, Integridade e autenticidade**: no modo mais seguro, o serviço deverá suportar mecanismos que garantam a confidencialidade, a integridade e a autenticidade da origem da mensagem. Para isso, recorra a uma cifra de chave pública.