



UNIVERSIDADE FEDERAL DA BAHIA  
INSTITUTO DE COMPUTAÇÃO

IGOR TEIXEIRA PASSOS FALCÃO

PROJETO PARTE 2 - APLICAÇÃO DE CHAT  
CLIENTE-SERVIDOR

SALVADOR  
2025

## Introdução

Este projeto tem como objetivo o desenvolvimento de um sistema cliente-servidor que permite comunicação entre usuários por meio de mensagens de texto e transferência de arquivos. Este sistema foi projetado com foco em aplicações de redes de computadores, utilizando protocolos TCP e implementando mecanismos de segurança, como criptografia AES para transmissão de mensagens seguras. A iniciativa busca não apenas reforçar os conceitos teóricos da disciplina de redes, mas também explorar a prática criativa no desenvolvimento de soluções tecnológicas.

## Metodologia

- **Configuração do Ambiente:**
  - Utilizou-se a linguagem Python e bibliotecas como *socket* para comunicação, *threading* para gerenciamento de conexões simultâneas, *tkinter* para a interface gráfica e *pycryptodome* para criptografia.
- **Arquitetura Cliente-Servidor:**
  - O servidor gerencia autenticações, envio de mensagens e transferência de arquivos(incompleto).
  - O cliente oferece uma interface gráfica para login, registro, seleção de usuários e troca de mensagens.
- **Protocolos e Segurança:**
  - A comunicação entre cliente e servidor foi realizada via TCP.
  - Mensagens e comandos foram criptografados usando AES em modo CBC, garantindo confidencialidade.
- **Funcionalidades Implementadas:**
  - Registro e autenticação de usuários.
  - Envio e recebimento de mensagens em tempo real.
  - Transferência de arquivos.
  - Listagem dinâmica de usuários conectados.

- **Desafios Enfrentados:**

- Grande dificuldade ao integrar o programa com a interface visual.
- Implementação robusta de criptografia no fluxo de comunicação.
- Implementação completa do sistema de troca de arquivos.
- Gerenciamento e limite de conexões por cliente.

## **Resultados e Discussão**

O sistema demonstrou ser funcional em vários aspectos relevantes:

### **1. Funcionalidades Atendidas:**

- Registro e Login: O sistema permitiu o registro de novos usuários e autenticação segura.
- Envio de Mensagens: Mensagens criptografadas foram enviadas e recebidas com sucesso.
- Atualização de Lista de Usuários: A listagem de usuários conectados foi sincronizada dinamicamente.

### **2. Funcionalidades Não Completamente Implementadas:**

- Recepção de Arquivos: A transferência de arquivos apresentou inconsistências na entrega ao destinatário final.
- Sincronização Completa do Chat: Algumas mensagens podiam ser perdidas ou não exibidas em tempo real dependendo da carga do servidor.

### **3. Segurança:**

- A criptografia AES garantiu a proteção das mensagens, mas a troca de chaves e a gestão de IV poderiam ser otimizadas para maior robustez.

### **4. Interface Gráfica:**

- A interface foi funcional, mas a usabilidade poderia ser melhorada, especialmente no gerenciamento de erros e feedback ao usuário.

O projeto representou uma aplicação prática dos conceitos de redes de computadores, como gerenciamento de conexões TCP e criptografia, demonstrando a viabilidade de criar um sistema funcional utilizando ferramentas acessíveis. Apesar de algumas limitações, como falhas na transferência de

arquivos e na sincronização de mensagens, o desenvolvimento foi uma experiência enriquecedora.

#### Aspectos Positivos:

- Integração de múltiplas tecnologias.
- Implementação básica de segurança.
- Estimulação da criatividade e resolução de problemas.

#### Melhorias Futuros:

- Revisão do sistema de transferência de arquivos para maior confiabilidade.
- Refinamento do protocolo de comunicação para evitar perda de mensagens.
- Melhorias na usabilidade da interface.

Este trabalho destaca a complexidade e a riqueza dos sistemas de redes de computadores, incentivando a continuidade do aprendizado e a exploração de soluções mais robustas e sofisticadas.