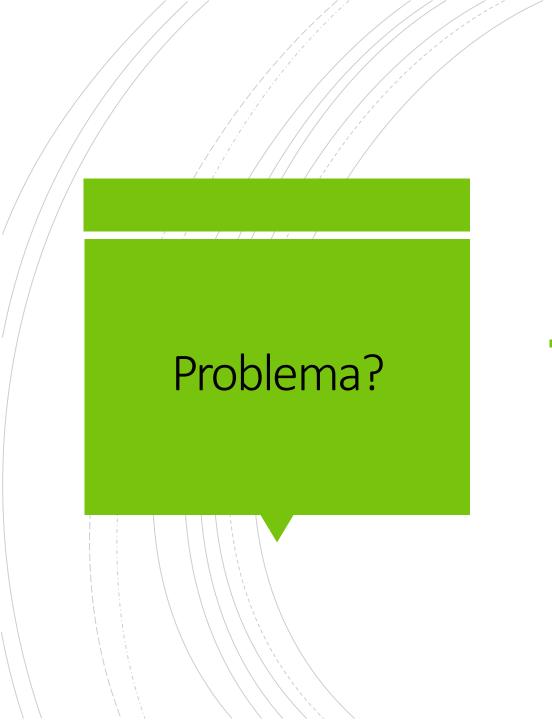
## Sistema de Comunicação Anônima

Eduardo Britto da Costa, Rodrigo Valente

Bernardes, Andrey Carvalho e Morgana Silva Prado



A interceptação de mensagens em sistemas de comunicação online.

## Proposta

 Solução: Proposta de desenvolvimento de um sistema de comunicação instantânea criptografado.

## Ideia:

- Todas as mensagens trocadas serão criptografados pela criptografia simétrica (AES).
- A realização de um login com usuário e senha, caso o usuário não tenha cadastro no sistema, momento do login é criado um novo usuário e um par chave de criptografia assimétrica (RSA), onde a chave privada é armazenada em disco e a chave pública no banco de dados.
- Os usuários cadastrados terão uma lista de amigos que poderão trocar mensagem de forma segura.
- Mensagens trocadas serão apagadas do banco de dados no final da comunicação.
- Teste: Sniffer (Wireshark).

