AVALIAÇÃO 2

1. IDENTIFICAÇÃO

CURSO: CIÊNCIA DA COMPUTAÇÃO **FASE:** 6ª **ANO/SEMESTRE:** 2021/2
DISCIPLINA: SEGURANÇA COMPUTACIONAL
PROFESSOR: ROBSON COSTA
DATA: 08/11/2021

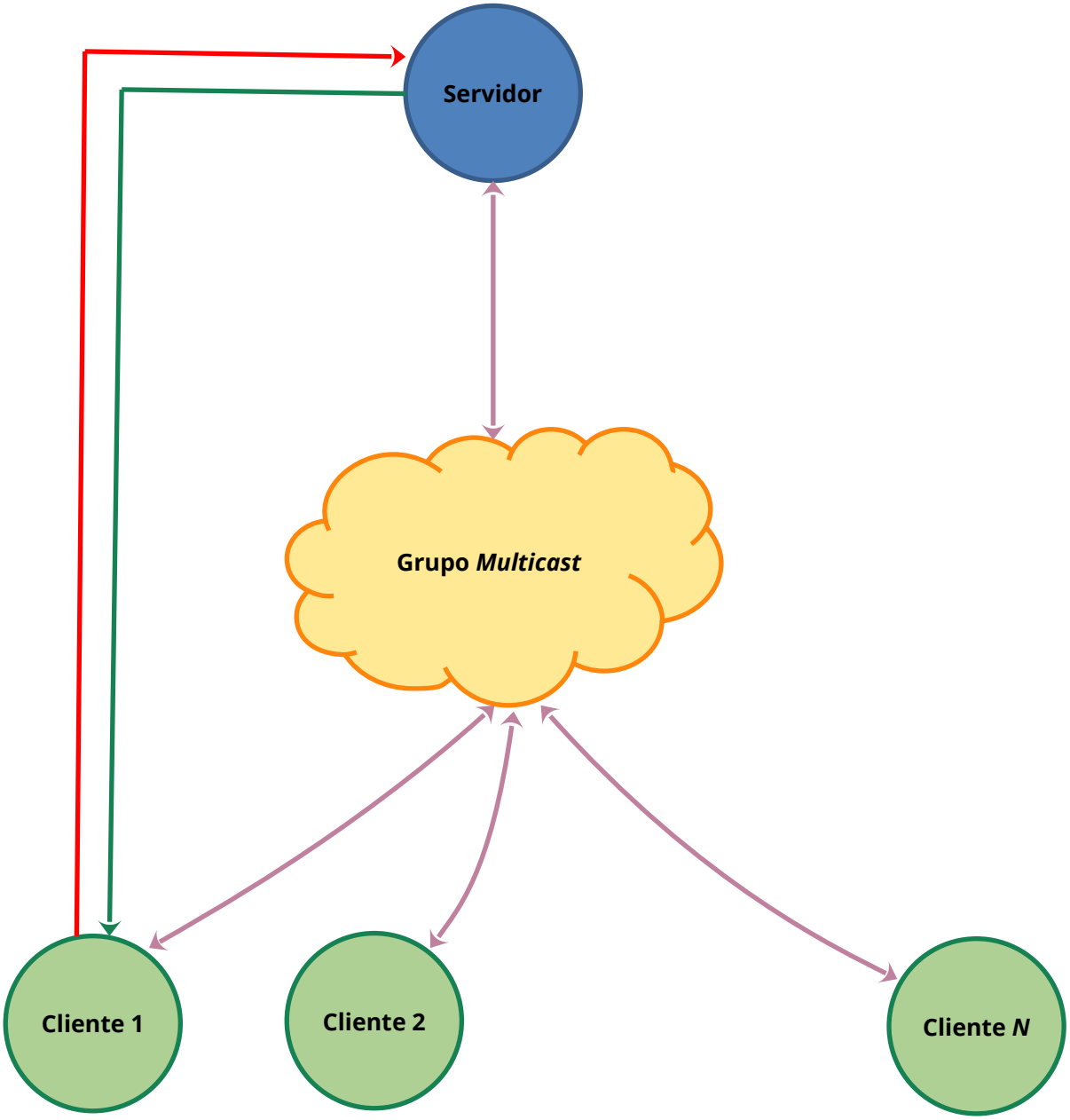
Esta avaliação deve ser realizada em **dupla** (de escolha livre dos discentes); as duplas devem informar o professor por e-mail sobre a sua composição até o dia **22/11/2021**; os códigos produzidos neste contexto devem ser entregues exlusivamente via SIGAA em um único arquivo comprimido (ZIP) até o dia **20/12/2021**; as apresentações serão realizadas nos dias **31/01/2022** e **07/02/2022**; o cronograma de apresentação das duplas será publicado no SIGAA até o dia **23/12/2021**.

Assuma que você trabalha em uma empresa de desenvolvimento de sistemas que foi contratada para implementar uma solução de **Leilão Virtual**. O arquiteto de *software* chefe selecionou você para o desenvolvimento desta tarefa e decidiu construir uma solução cliente/servidor baseada em comunicação *multicast* com um sistema de criptografia assimétrica para garantir a autenticidade dos usuários e a privacidade dos dados.

Sendo assim, você deverá desenvolver dois programas com as seguintes características:

- **Servidor**
  - responsável por publicar os itens em leilão (apenas um único item deve ser leiloado por vez), o valor do lance inicial, o valor mínimo entre lances (ex.: lances devem ter incremento mínimo de R$ 10,00), o valor do lance atual, o usuário que fez o lance atual e o tempo restante para encerar o leilão deste item;
  - criará um grupo *multicast* para o envio e recebimento de informações sobre os lances;
  - receberá as solicitações de participação dos usuários e enviará a chave simétrica (através de um envelopamento digital) a qual será utilizada nas transmissões de lances do leilão através do grupo *multicast*;

- **Cliente**
  - responsável por permitir que o cliente receba informações dos itens que estão em leilão no momento bem como enviar propostas de lances;
  - deverá primeiramente solicitar a sua entrada no leilão ao servidor, para então, receber as informações acerca do endereço do grupo *multicast* em uso no momento e a chave simétrica utilizada nas comunicações;
  - realizará o *join* no grupo *multicast* enviado pelo servidor e receberá e enviará propostas de lances neste grupo utilizando a chave simétrica previamente recebida;



requisição de entrada no leilão (cliente envia a sua chave pública ao servidor)[1].

resposta da requisição de entrada no leilão (servidor envia ao cliente o endereço do grupo multicast do leilão e a chave simétrica a ser utilizadas)[2].

Dados sobre os lances do leilão[3].

[1] comunicação *unicast* em texto claro.
[2] comunicação *unicast* cifrada utilizando-se a chave pública do cliente.
[3] comunicação *multicast* cifrada utilizando-se a chave simétrica.