

General Bizantino representado através de um No.

A principal ideia é que cada No seja executado de maneira autônoma em seu próprio processo, e se comunique com todos os outros Nos Tenentes por meio de mensagens enviadas pela rede.

Qual a solução escolhida para resolver o problema?

Assinar as mensagens enviadas pelos Generais Bizantinos digitalmente evitando que as mesmas sejam interceptadas e alteradas durante a troca de mensagens.

Como assinar estas mensagens?

Pode-se utilizar o gerador de chaves digital disponibilizado nesta aplicação.

Como funciona?

O No do General envia sua mensagem (sua ordem para atacar ou recuar) com sua chave privada. Os Nos que recebem essa mensagem podem verificá-la através da chave pública do General, ou seja, se a ordem recebida pelo No Tenente realmente foi enviada e assinada pelo General, e se a mesma foi recebida de forma intacta.

Observação importante: cada No deve possuir as chaves públicas de todos os outros Nos, entretanto, a chave privada de cada um só pode ser acessada por ele próprio.