# Computação Distribuída

**Odorico Machado Mendizabal**


Universidade Federal de Santa Catarina – UFSC
Departamento de Informática e Estatística – INE

# Falhas Bizantinas e Consenso

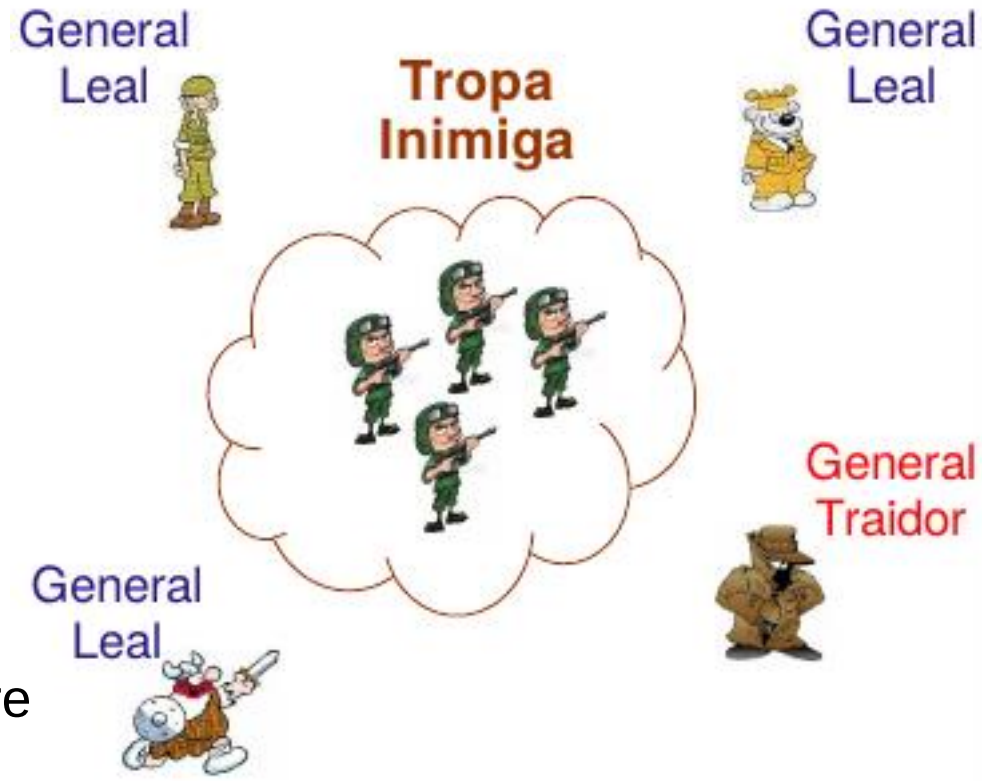
# Falhas Bizantinas

## Problema dos Generais Bizantinos:

- Um grupo de generais está distribuído fisicamente e precisa combinar um ataque:
  - Se o plano for bem sucedido, eles terão sucesso
  - Se o plano falhar, as chances de vitória são mínimas

- Entre os generais, alguns são leais e outros são bizantinos (maliciosos)

- Os generais bizantinos tentarão comprometer o plano de ataque:
  - Não enviando mensagens,
  - Enviando mensagens erradas,
  - Alternando seu comportamento entre o correto e o malicioso,
  - etc ...



# Consenso assumindo falhas Bizantinas

- Lamport apresenta o problema e soluções considerando mensagens orais e mensagens assinadas

- Os processos devem atingir um consenso sobre qual valor utilizar
- Um processo comporta-se como comandante e os demais como tenentes

**Propriedades**:

- Término: cada processo correto acaba por configurar sua variável de decisão
- Acordo: o valor de decisão de todos os processos corretos é o mesmo: se `pi` e `pj` são corretos e entraram no estado decidido, então `di = dj`
- Integridade: se o comandante é correto, então todos os processos corretos decidem pelo valor proposto pelo comandante

# Falhas Bizantinas: “Mensagens orais”

- Os processos devem atingir um consenso sobre qual valor utilizar

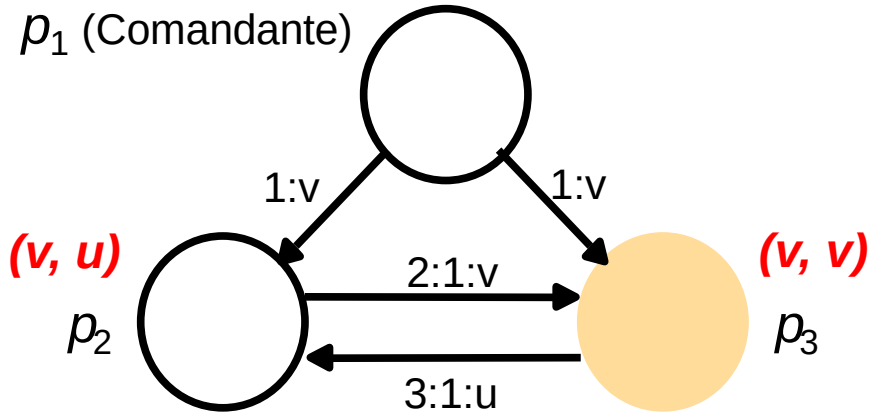
- Um processo comporta-se como comandante e os demais como tenentes
  - Comandante envia valor para os tenentes
  - Tenentes trocam mensagens entre si para confirmar se o comandante não é o traidor
  - O valor observado pela maioria é escolhido

# Falhas Bizantinas: “Mensagens orais”

- Os processos devem atingir um consenso sobre qual valor utilizar

- Um processo comporta-se como comandante e os demais como tenentes
  - Comandante envia valor para os tenentes
  - Tenentes trocam mensagens entre si para confirmar se o comandante não é o traidor
  - O valor observado pela maioria é escolhido

Processos corretos não conseguem determinar um valor!



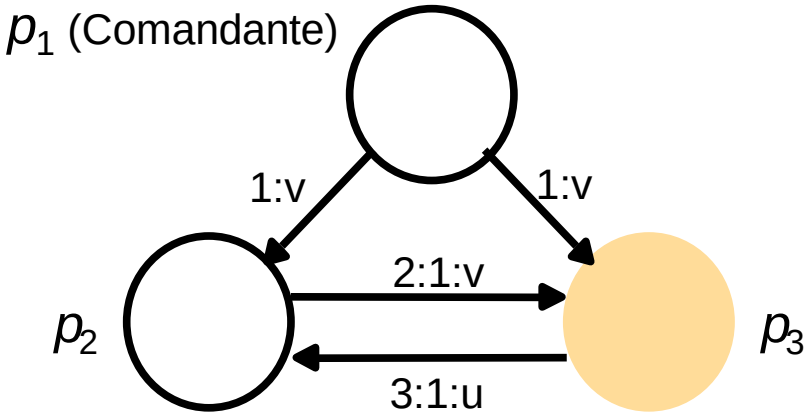

Processos bizantinos aparecem em laranja

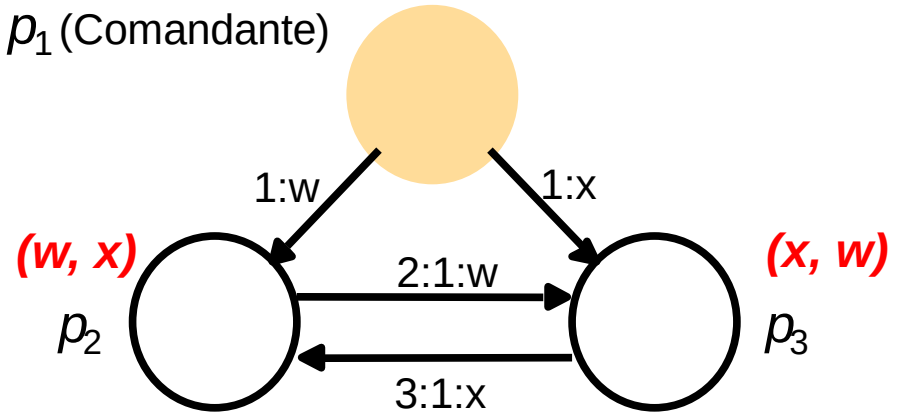
# Falhas Bizantinas: “Mensagens orais”

- Os processos devem atingir um consenso sobre qual valor utilizar

- Um processo comporta-se como comandante e os demais como tenentes
  - Comandante envia valor para os tenentes
  - Tenentes trocam mensagens entre si para confirmar se o comandante não é o traidor
  - O valor observado pela maioria é escolhido

Processos corretos não consegue determinar um valor!




Processos bizantinos aparecem em laranja

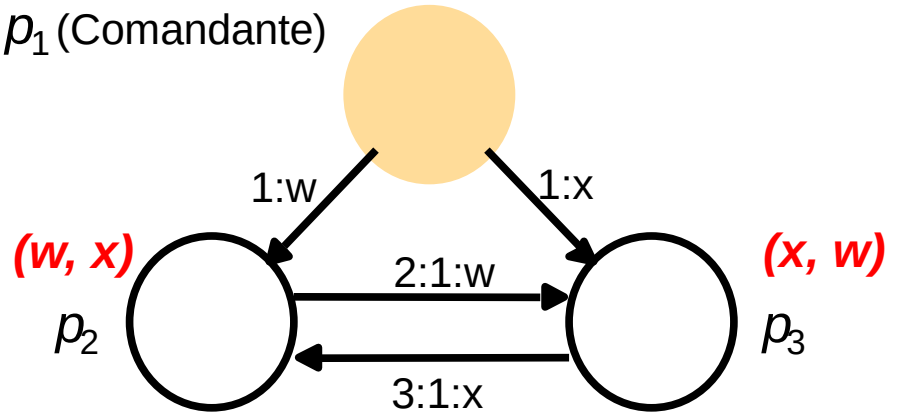
# Falhas Bizantinas: “Mensagens orais”

- Os processos devem atingir um consenso sobre qual valor utilizar

- Um processo comporta-se como comandante e os demais como tenentes
  - Comandante envia valor para os tenentes
  - Tenentes trocam mensagens entre si para confirmar se o comandante não é o traidor
  - O valor observado pela maioria é escolhido

Processos corretos não consegue determinar um valor!

Lembre da propriedade Integridade:
se o comandante é correto, então todos os processos corretos decidem pelo valor proposto pelo comandante



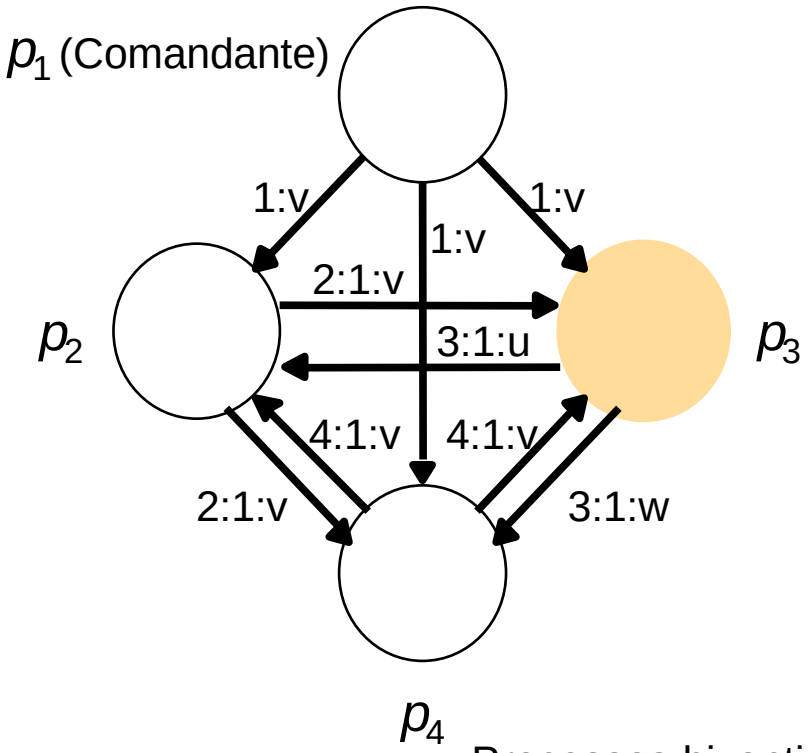

Processos bizantinos aparecem em laranja

# Falhas Bizantinas: “Mensagens orais”

- Com mensagens orais apenas, resolver o problema de consenso com falhas bizantinas requer **$n \geq 3f + 1$**

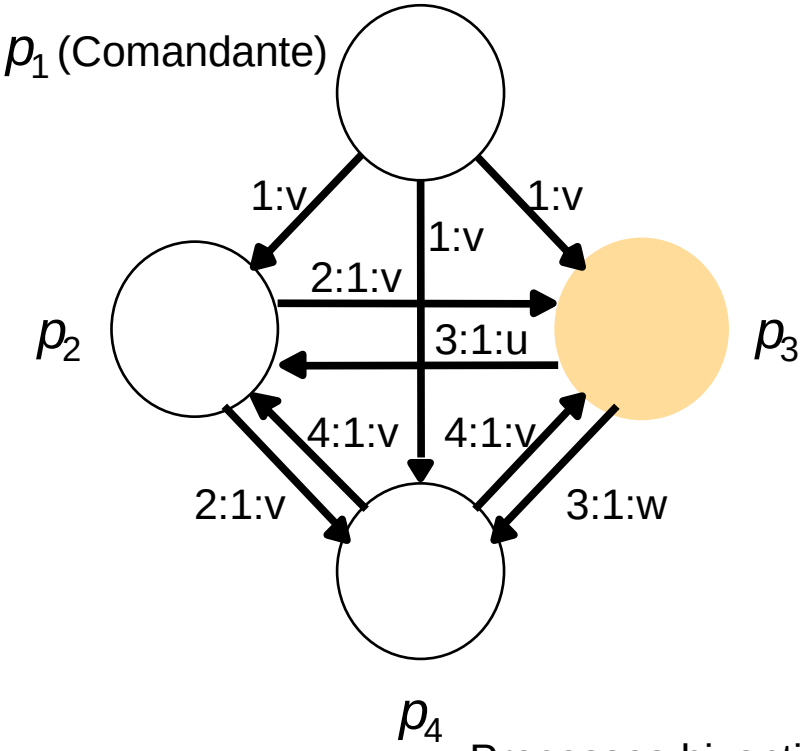
- Uma solução pode ser obtida com 3 generais caso estes adicionem uma assinatura única em suas mensagens

# Falhas Bizantinas: “Mensagens orais”




Processos bizantinos aparecem em laranja

# Falhas Bizantinas: “Mensagens orais”



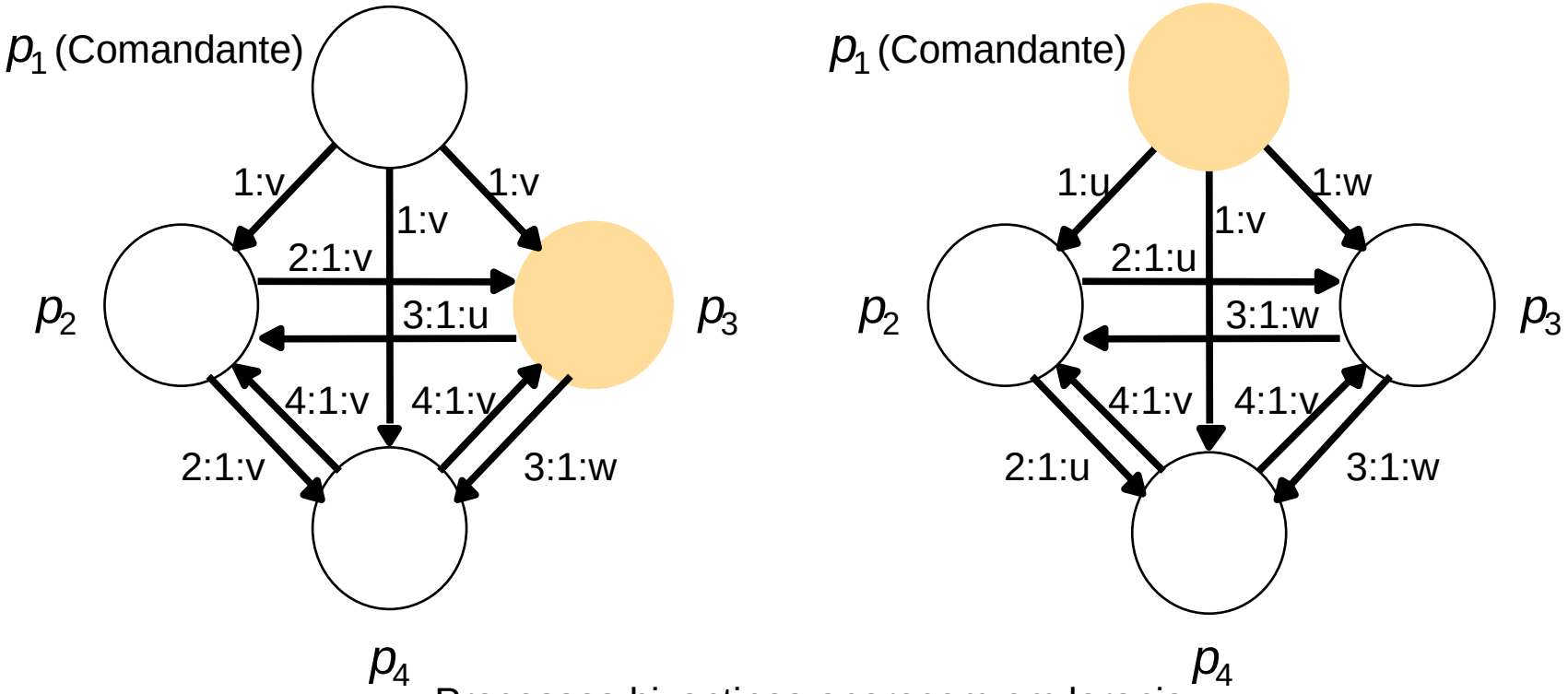

Processos bizantinos aparecem em laranja

**Tenente bizantino**

De acordo com a maioria, P2 decide por : maioria(v, u, v) = v

De acordo com a maioria, P4 decide por : maioria(v, v, w) = v

# Falhas Bizantinas: “Mensagens orais”




Processos bizantinos aparecem em laranja

**Tenente bizantino**

De acordo com a maioria, P2 decide por : maioria(v, u, v) = v

De acordo com a maioria, P4 decide por : maioria(v, v, w) = v

**Comandante bizantino**

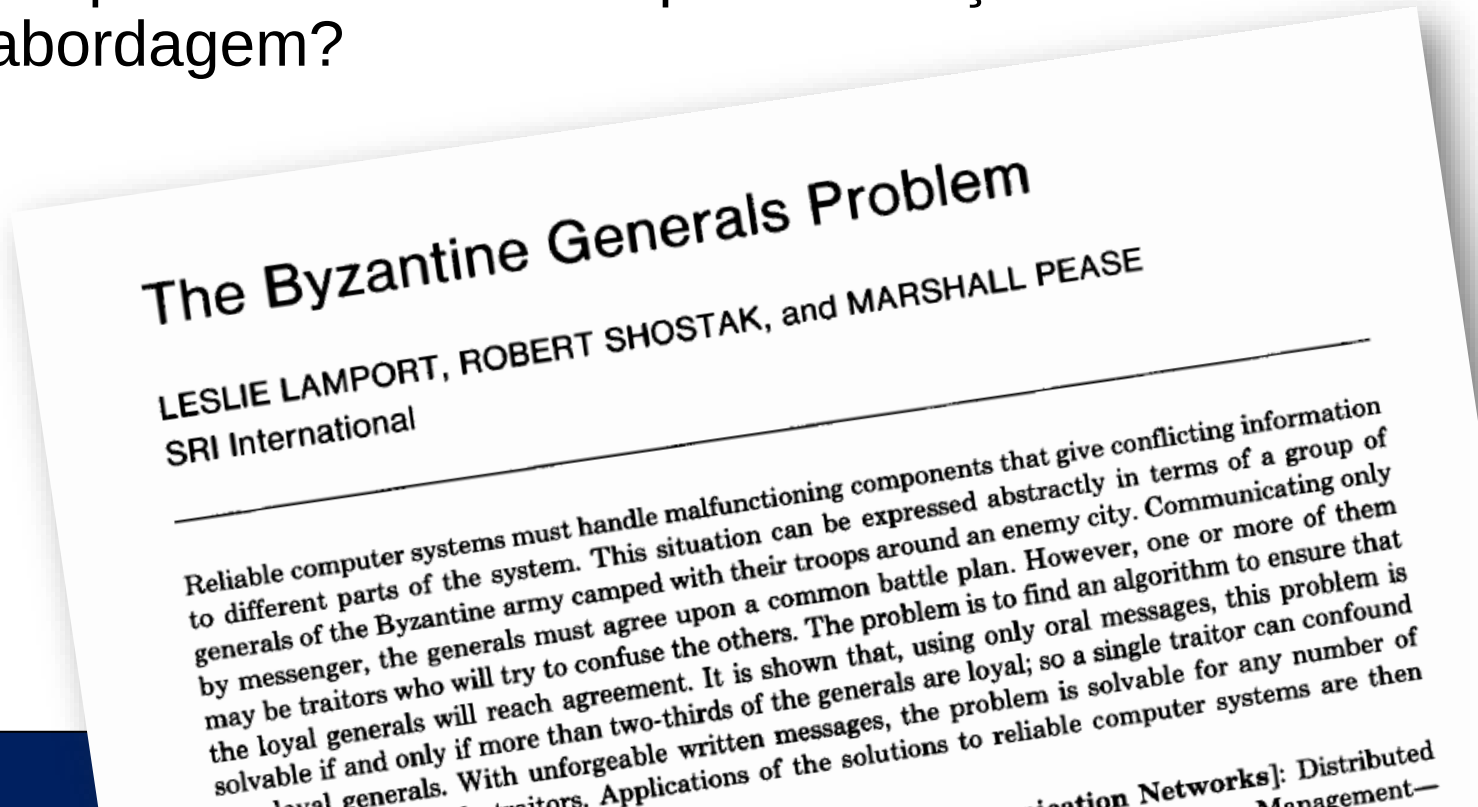
Não há uma maioria, P2 decide por : maioria(u, w, v) = ⊥

Não há uma maioria, P4 decide por : maioria(v, u, w) = ⊥

# Falhas Bizantinas: “Mensagens assinadas”

- Faça a leitura do artigo original
*“L. Lamport, R. Shostak, M. Pease. The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems. Vol. 4, No. 3, July 1982.*

- Qual a diferença na solução com mensagens assinadas?
- O número de participantes necessários para alcançar o consenso diminui com esta abordagem?



The Byzantine Generals Problem

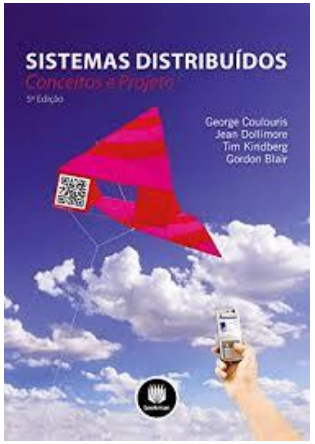
LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE
SRI International

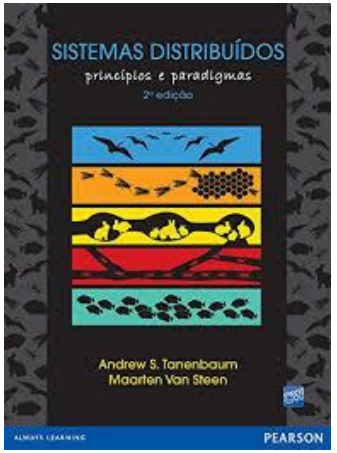
Reliable computer systems must handle malfunctioning components that give conflicting information to different parts of the system. This situation can be expressed abstractly in terms of a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement. It is shown that, using only oral messages, this problem is solvable if and only if more than two-thirds of the generals are loyal; so a single traitor can confound

# Referências

Parte destes slides são baseadas em material de aula dos livros:


- *Coulouris, George; Dollimore, Jean; Kindberg, Tim; Blair, Gordon. Sistemas Distribuídos: Conceitos e Projetos. Bookman; 5ª edição. 2013. ISBN: 8582600534*
- *Tanenbaum, Andrew S.; Van Steen, Maarten. Sistemas Distribuídos: Princípios e Paradigmas. 2007. Pearson Universidades; 2ª edição. ISBN: 8576051427*


- *Imagens e clip arts diversos:*
  *https://free-icon-rainbow.com/*
  *https://www.gratispng.com/*