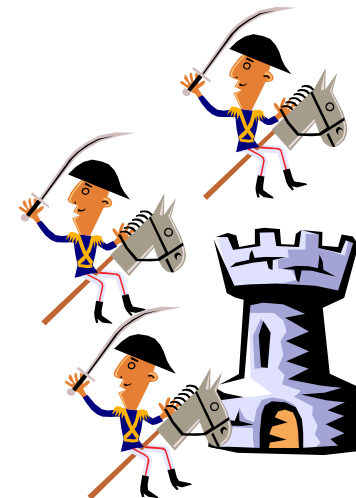
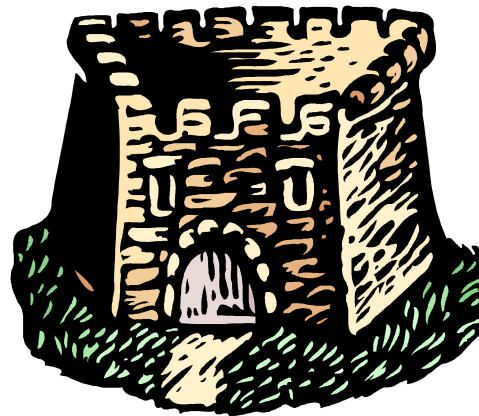
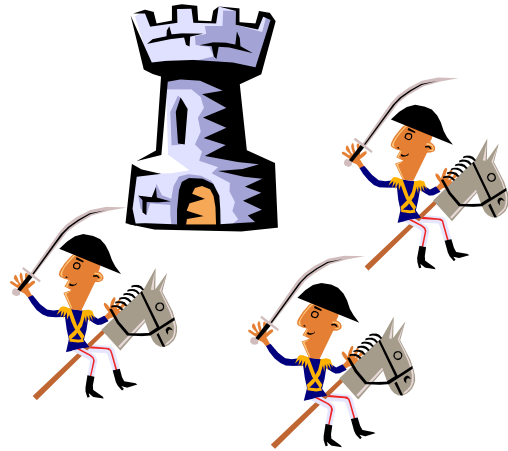


Intro To The Byzantine **Generals Problem**

Leslie Lamport, Robert Shostak, Marshall
Pease



Byzantine Generals Problem



BGP – the Generals

- Loyal Generals
 - Behave according to the algorithm
 - **They decide upon the same plan**
 - Every loyal general must obtain the same $v(1) \dots v(n)$
 - **A small number of traitors shouldn't be able to force a bad decision**
 - If the i^{th} general is loyal $v(i)$ must be used by all (loyal) generals
- Traitorous Generals
 - Try to influence the final decision
 - Send any info they want



Byzantine Generals Problem (formalism)

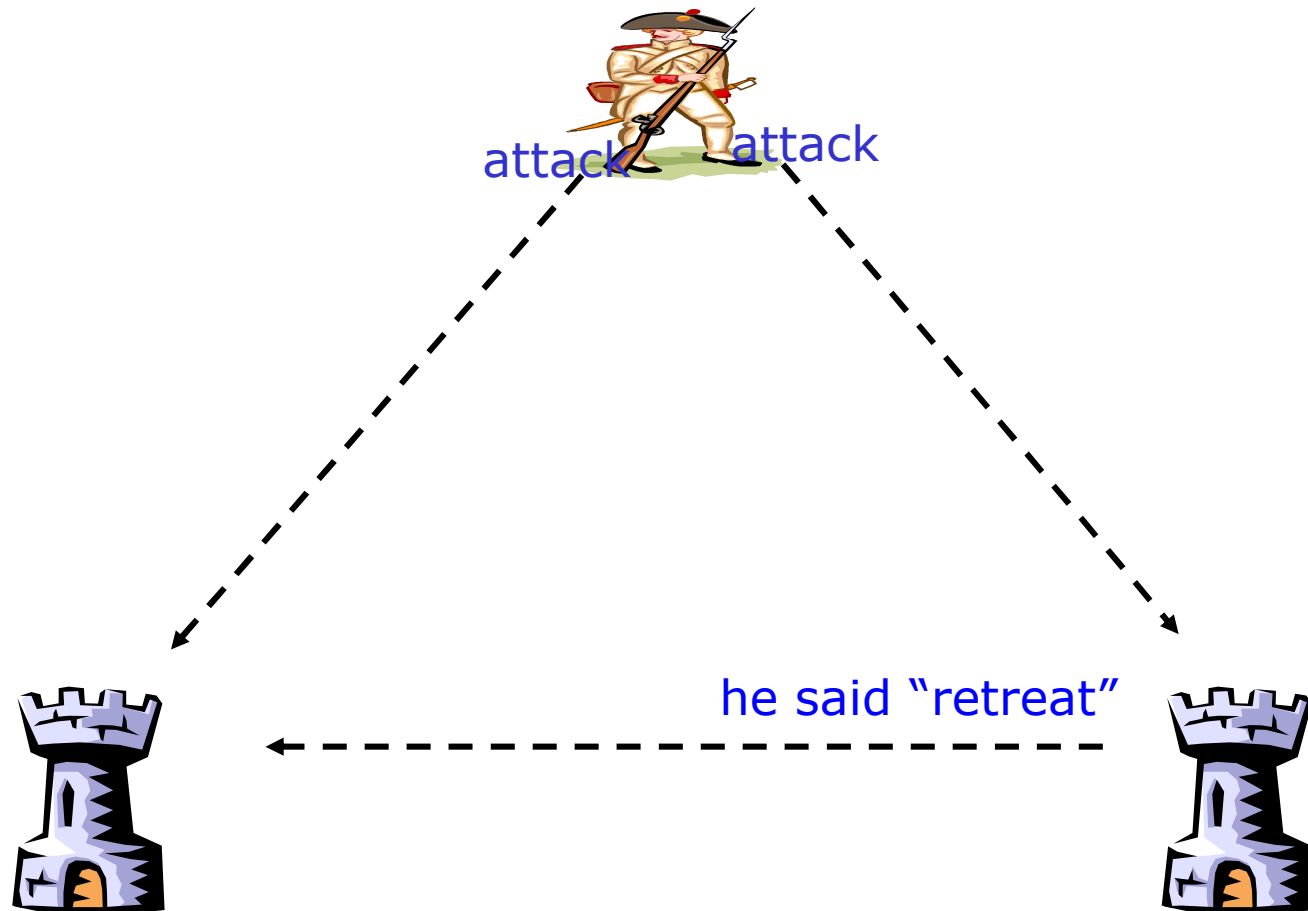
- 0 .. N-1 processes in a complete graph
- Process 0 needs to send a value v to all others such that
 - (IC1) If process 0 is non faulty then any non faulty process i receives v
 - (IC2) If processes i and j are non faulty, they receive the same value
- Note: 0 is non faulty, then $IC1 \Rightarrow IC2$



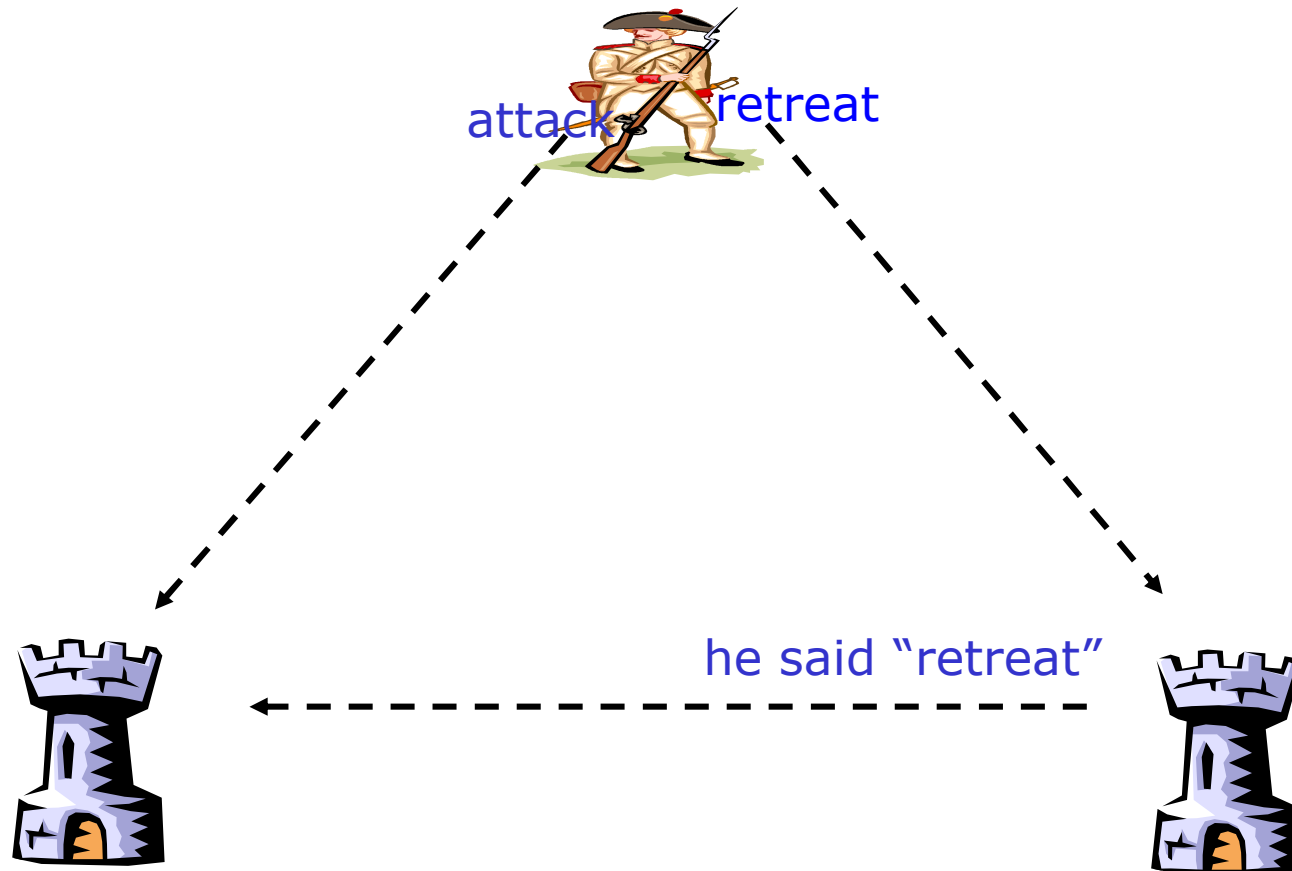
Impossibility Results – Oral Msg

- Oral message – the content is entirely under the control of the sender
- No solution if more than $1/3$ of the generals are traitorous

Traitorous Lieutenant



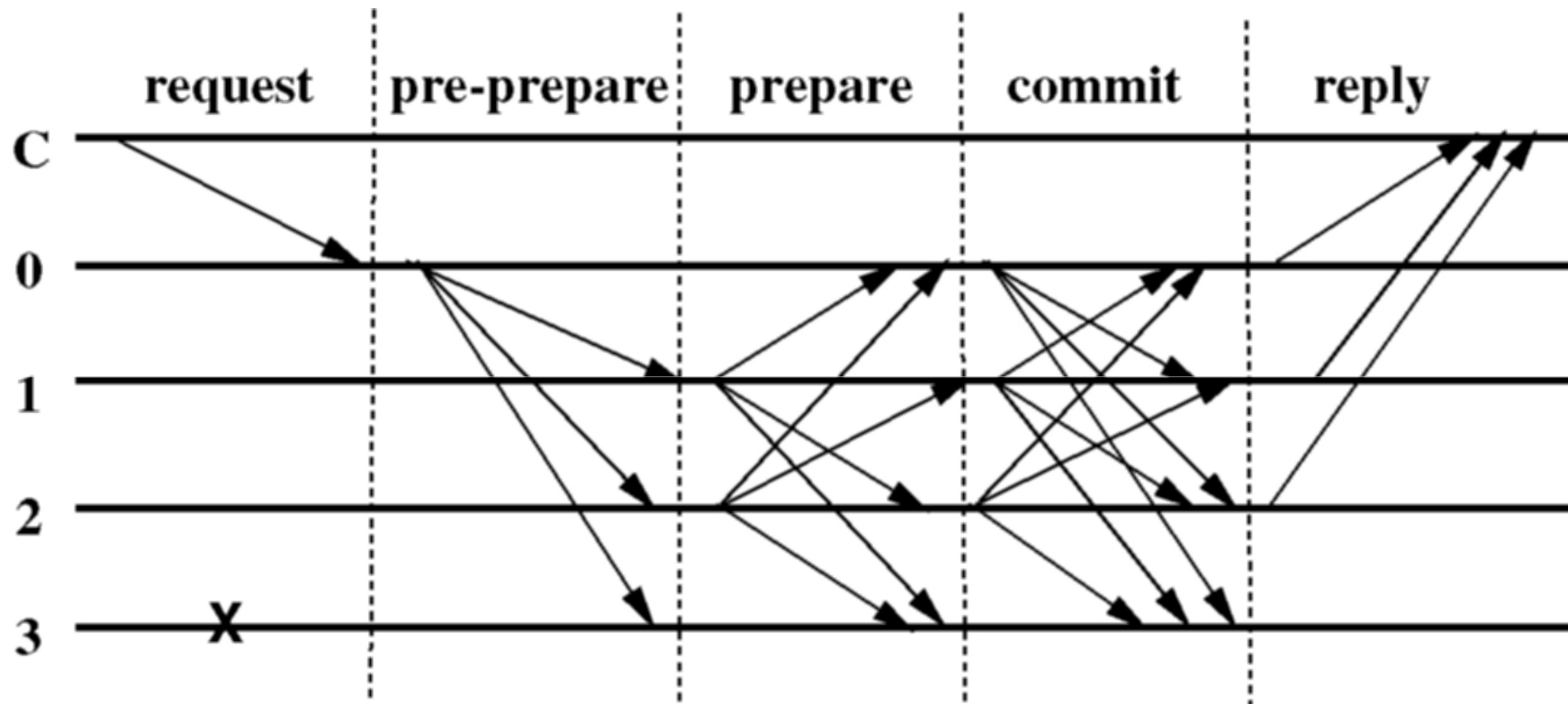
Traitorous General



Impossibility Results – Generalization

- No solution with fewer than **$3m+1$** generals for **m** traitors
- Proof by contradiction: reduce the problem to the 3 generals problem
 - Assume **$3m$** (let's call them Albanians) or fewer generals can cope with m traitors
 - Build the solution with Byzantine generals

An Actual Protocol



- Note: Relatively high overhead