Byzantine broadcast in $n$ parties, to corrupt/malicious/Byzantine.

Agreement: No two honest generals take different actions.

Termination: Every honest general eventually either attacks or retreats.

Validity: If commander is honest, then output commander's order.
Dolev-Strong Protocol: (1983)

Intuition:
- If some honest party receives a value, share it with all honest parties.
- Eventually, one honest party learns $x$
  \[\downarrow\]
  all honest parties learn $x$.

Round 1: Commander (sender) sends value $v$ to all parties.

Round 2: If I receive a value from the commander, then I send it to all parties.

Commit: If I receive exactly one value $v$, then output $v$.

output $\top$.

Round 1:

\[\begin{array}{c}
\text{K} \\
\text{V} \\
\text{V}'
\end{array}\]
Round 2:
\[ v, v' \]
\[ \_ \_ \]
\[ \_ \_ \]
\[ \_ \_ \]

Attack 2:

Round 1:
\[ \_ \]
\[ \_ \]
\[ \_ \]
\[ \_ \]

Solution:
Round 2: Do not consider commander's value.

If \( \leq 1 \) Byzantine:

\[ M \geq 2 \] Byzantine parties.

Round 1:
\[ \_ \]
\[ \_ \]
\[ \_ \]
\[ \_ \]

No messages.
Round 2: {R, S, T} nothing.

We can tolerate Byzantine faults.