

Dolev-Yao Derivations

$$\begin{array}{c}
 \frac{}{M \vdash k_1} (Axiom) \quad \frac{\frac{}{M \vdash \{m_1\}_{k_1}} (Axiom) \quad \frac{}{M \vdash k_1} (Axiom)}{M \vdash m_1} (DecSym) \quad \frac{}{M \vdash m_2} (Axiom)}{M \vdash \langle m_1, m_2 \rangle} (Compose) \\
 \hline
 M \vdash \{\langle m_1, m_2 \rangle\}_{k_1} (Compose)
 \end{array}$$

Strands

