Process Calculi and Security
AVISPA

Carlos Alberto Olarte
caolarte@atlas.puj.edu.co

31st August 2006

1 Workshop

Given the following protocol definition:

$$\begin{array}{lcl} A \rightarrow B & : & \{\{m, A, B\}_S, S\}_B \\ B \rightarrow S & : & \{n, \{m, A, B\}_S\}_S \\ S \rightarrow B & : & \{A, n, \{m, n, B\}_A\}_B \\ B \rightarrow A & : & \{m, n, B\}_A \\ A \rightarrow S & : & \{m, n\}_B \end{array}$$

where A, B and S are participants and m and n secrets generated by A and B respectively, the idea is to model the protocol in the spi-calculus or SPL.