Sample protocol for EE6032/ED5012 Project.

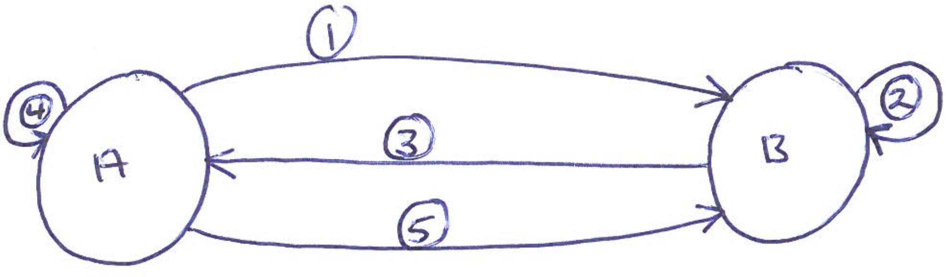
Need: 1) Mutually Generated Session Key.

2) Data Confidentiality

Data Integrity

Digital Signature of Key Generating components.

Assume Two Entities:



Notes:

1) A initiates the Session

Steps:

1) $A \rightarrow B : A, B, \{\overset{\text{challenge}}{PassA}, \overset{I}{\{H(PassA)\}}_{\overset{DS}{K_a^{-1}}}\}_{\overset{C}{K_b}}$

2) $B : K_{ab} = H(PassA \,\|\, PassB)$

3) $B \rightarrow A : B, A, \{\overset{\text{challenge}}{PassB}, \overbrace{\{PassA\}_{K_{ab}}}^{\text{Response}}, \{\overbrace{H(PassB, \{PassA\}_{K_{ab}})}^{I}\}_{\overset{DS}{K_b^{-1}}}\}_{\overset{C}{K_a}}$

④ $A : K_{ab} = H(PassA \,\|\, PassB)$

⑤ $A \rightarrow B : A, B, \overbrace{\{PassB\}_{K_{ab}}}^{\text{Response}}$

Note: H(M) can also be Sent.

* Now all communications uses Session Key i.e. $\{M\}_{K_{ab}}$