Proposed Protocol

[redacted]

1 Protocol description

		Cost
$A \rightarrow S:$	$\{B, K_A\}_{symkey(A,S)}$	63
$S \rightarrow B:$	$\{K_A\}_{symkey(B,S)}$	12
$B \rightarrow A:$	$\{A, N_B\}_{K_A}$	63
$A \rightarrow B:$	$\{N_B\}_{pub(B)}$	3
Total cost:		141

2 Informal description

Initial knowledge Each agent A has a public key $pub(A)$ and a symmetric key $symkey(A, S)$. The identity and the public key of each agent are known by every other agent. The symmetric key $symkey(A, S)$ is known only to A and a trusted server S.

Data generated during the protocol When an agent in role A executes the protocol, he or she generates a fresh nonce (session key) K_A. Similarly, when an agent in role B executes the protocol, he or she generates a fresh nonce N_B.

Protocol execution We illustrate the execution of the protocol with two agends Alice and Bob. Alice assumes role A and generates a fresh session key K_A. She sends then $\{B, K_A\}_{symkey(A,S)}$ to the server. The server, after receiving this message, sends to Bob the message $\{K_A\}_{symkey(B,S)}$. Bob then sends to Alice the message $\{A, N_B\}_{K_A}$ to confirm that the key was the one Alice generated. Alice confirms by sending $\{N_B\}_{pub(B)}$ to Bob.

Security properties

- K_A remains known only to the server, Alice, and Bob.
- After Alice finishes an execution of the protocol in role A, apparently with Bob in role B, then Bob was executing the protocol in role B and Alice and Bob agree on the value of K_A.