Description du protocole

$A \rightarrow S : A, \{B, Na\}_{K_{SA}}$
$S \rightarrow A : \{N_a\}_{K_{SB}}$
$A \rightarrow B : \{N_a\}_{K_{SB}}$
$B \rightarrow A : h(N_a, B)$

Secret : N_a

Explications

1. A exprime au serveur S son souhait d'échanger un secret frais N_a avec B. Il chiffre B, N_a avec la clé symétrique préalablement partagée avec le serveur K_{SA}.
2. S répond à A en lui envoyant le secret N_a chiffrée avec la clé symétrique K_{SB}.
3. A transfert le secret chiffrée à B
4. B déchiffre la secret et répond à A avec un hash du secret et de son identité.

Coût

$1 + (10 + (50 + 1 + 1) + 1) = 64$
$10 + 1 + 1 = 12$
$10 + 1 + 1 = 7$
$5 + 1 + 1 = 7$
TOTAL : 95