Championnat de protocole - Équipe REX

Hugo Finelle - Marcus Reis de Morais - Bastien Robert

October 8, 2020

Voici le protocole proposé par la team REX. A répond à B, lors du dernier message, uniquement si le haché de la clé K_{ab} envoyé par B est le même que celui calculé par A de son côté. Si B ne reçoit pas son nonce au début du message envoyé par A chiffré par la clé K_{ab}, il ne valide pas la connection et jette la clé K_{ab}.

$A \rightarrow B : \{A, K_{ab}\}_{pub(B)}$
$B \rightarrow A : B, \{h(K_{ab}), Nb\}_{pub(A)}$
$A \rightarrow B : \{Nb, K\}_{K_{ab}}$

Le coût total est de 176. (54 + 59 + 63)