Championnat de protocole - Équipe REX - Protocole CHI1 v2

Hugo Finelle - Marcus Reis de Morais - Bastien Robert

October 13, 2020

Connaissances initiales : Au début du protocole, chaque agent A connait la clé publique des autres agents. Il connait aussi sa clé privée.

Description du protocole : Voici le protocole proposé par la team REX.

- Dans un premier temps A commence une connexion avec B en lui envoyant son identité ainsi que la clé symmétrique Kab.
- B lui répond en envoyant le haché de la clé, son identité et un nonce.
- 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}.

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

Poids du protocole : Le coût total est de 126. (54 + 60 + 12)