Protocole

Clément Bidault, Loïc Cardinaël, Elise Klein

Notre protocole se décrit comme suit :

$$
\begin{aligned}
A &\rightarrow B : \{A, N_a\}_{pub(B)} \\
B &\rightarrow A : \{\{B, N_b\}_{h(N_a)}\}_{pub(A)} \\
A &\rightarrow B : \{\{K_{ab}\}_{h(N_b)}\}_{pub(B)} \\
B &\rightarrow A : \{N_a\}_{\{\{N_b\}_{K_{ab}}\}}
\end{aligned}
$$

Connaissances initiales : Au début du protocole on suppose que A et B connaissent les clé publiques *pub(C)* de tout agent C.

Valeurs générées au cours du protocole : Les agents A et B connaissent une fonction de hachage commune h qu'ils utiliseront pour hacher leurs nonces. Les nonces Na et Nb sont générés à chaque nouvelle conversation.

Description du protocole :

1. A entame la conversation en envoyant à B son nom et un nonce généré spécialement pour cette conversation, le tout chiffré avec la clé publique de B.
2. B répond en envoyant son nom et un deuxième nonce généré par lui et unique à cette conversation, le tout chiffré par le hash du premier nonce, puis chiffré par la clé publique de A.
3. A envoie alors la clé secrète chiffrée par le hash du deuxième nonce, puis chiffré par la clé publique de B.
4. Enfin, B renvoie le premier nonce chiffré par le deuxième nonce, puis chiffré par la clé secrète. A vérifie que c'est bien le premier nonce qu'il a envoyé en (1) et que c'est bien la clé qu'il a généré en (3) qui a été utilisée. Si oui, il considère que la communication s'est bien passée.

Propriétés de sécurité :

— *Authentification :* Lorsque B reçoit le message du serveur il sait que c'est Alice qui lui parle, et quand Alice envoie la clé à B, elle est sûre que B a reçu la clé.
— *Confidentialité :* Les 2 agents sont seuls à connaître K.

Poids du protocole : 166

— Règle 1 : $1 + 1 + 50 + 1 + 1 = 54$
— Règle 2 : $10 + 50 + 1 + 1 + 1 + 1 + 5 + 1 = 70$
— Règle 3 : $10 + 1 + 1 + 1 + 5 + 1 = 19$
— Règle 4 : $10 + 1 + 10 + 1 + 1 = 23$